

SUBJECT: BSA: Suspicious Activity Reports

Executive Summary	1	SAR completion and filing	7
Reportable activity	2	Cases requiring immediate attention	8
Reporting thresholds	2	Board of directors notification	8
Computer intrusion	3	Prohibition on SAR disclosure	9
Robberies and burglaries	3	SAR sharing with an affiliate	9
Marijuana-related businesses	3	Record retention	9
SARs and money services businesses (MSBs)	3	Providing supporting documentation to law enforcement	9
Reporting elder financial abuse	4	Safe harbor	9
Policies and procedures to monitor for suspicious activity	4	Accounts and services	10
Identification of unusual activity	5	Exhibit A - Filing suspicious activity reports on marijuana-related businesses	11
Managing alerts	7		
SAR decision making process	7		

INTRODUCTION

This release applies to all credit unions. It describes the requirements for filing a Suspicious Activity Report (SAR), as required by the Bank Secrecy Act (BSA). Additional BSA requirements are provided in *ii Release No. 0071, "Bank Secrecy Act," ii Release No. 0159, "BSA: Customer Identification Program and Customer Due Diligence,"* and *ii Release No. 0187 – BSA: Money Services Businesses.*

EXECUTIVE SUMMARY

Under NCUA regulations, a credit union must file a Suspicious Activity Report if it knows, suspects or has reason to suspect that any crime or any suspicious transaction related to money laundering or a violation of the BSA has occurred in the following circumstances:

- Criminal violations involving insider abuse in any amount;
- Criminal violations aggregating \$5,000 or more where a suspect can be identified;
- Criminal violations aggregating \$25,000 or more regardless of potential suspects;
- Transactions aggregating \$5,000 or more conducted or attempted by, at, or through the credit union, that involve potential money laundering or violations of the BSA if the credit union knows, suspects, or has reason to suspect:
 - The transaction(s) involves funds derived from illegal activities or is intended to hide or disguise funds or assets derived from illegal activities;
 - The transaction(s) is designed to evade any requirements of the BSA regulations; or
 - The transaction(s) has no business or apparent lawful purpose or is not the sort in which the particular member/customer would normally be expected to engage, 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; and
- Computer intrusions, defined as gaining access to a computer system to: remove, steal, procure or otherwise affect funds or critical information of the credit union or its members/customers; or damage, disable or otherwise affect critical systems of the credit union. It does not mean attempted intrusions of websites or other non-critical information systems that do not provide access to the credit union's or members' financial or other critical information.

A credit union must file a SAR with the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) generally within 30 calendar days after the initial detection of facts that may constitute a basis for filing a SAR. For violations requiring urgent attention, such as ongoing activity, a credit union is also required to immediately notify appropriate law enforcement and as necessary the credit union's primary regulator.

All financial institutions, including credit unions, must electronically file (e-file) BSA reports, including SARs, using FinCEN's online BSA E-Filing System. [FinCEN maintains a set of frequently asked questions about SARs, which includes guidance on completing SAR forms and electronic filing instructions.](#) Credit unions can also call the FinCEN Regulatory Help Line at (800) 949-2732 for questions regarding SARs.

A credit union must promptly notify its board of directors, or a committee designated by the board, of any SAR that is filed. In the rare instance when the suspect of the SAR is an individual in the organization, such as the president, a director or a member of the designated committee that reviews SARs, the credit union must take care not to notify the suspect, but other board or committee members must be notified.

No director, officer, employee, or agent of a credit union that reports a suspicious transaction may notify any person involved in the transaction that it has been reported. This means that any person subpoenaed or otherwise asked to disclose a SAR or the information contained in a SAR, must decline unless the request is from FinCEN, law enforcement, or a federal credit union regulator. FinCEN and the NCUA should be notified of any such request.

The credit union's Bank Secrecy Act & Anti-Money Laundering (BSA/AML) policy must provide for internal controls for the credit union to identify, research and report suspicious activity. See *ii Release No. 0071* for The League's Sample BSA/AML Policy. The credit union should assign adequate staff to the process. Personnel should have appropriate experience and get ongoing training to maintain their expertise. They should also have access to sufficient internal and external tools to allow them to properly research activities and formulate conclusions, taking into account the credit union's overall risk profile and the volume of transactions.

A credit union must maintain documentation to support the specific reasons for filing or not filing a SAR and a copy of any SAR that it files for five years from the date of the report.

REPORTABLE ACTIVITY

Each federally insured credit union is required by Part 748.1(c) of the NCUA Rules & Regulations to file a SAR if it knows, suspects, or has reason to suspect any crime or any suspicious transaction related to money laundering or a violation of the BSA has occurred.

Reporting thresholds

- **Criminal violations involving insider abuse in any amount.** File a SAR regardless of the dollar amount involved in the violation if the credit union has a substantial basis for identifying one of its directors, officers, employees, agents or other credit union-affiliated parties as having committed or aided in the commission of a criminal act.
- **Criminal violations aggregating \$5,000 or more where a suspect can be identified.** File a SAR if the credit union has a substantial basis for identifying a possible suspect or group of suspects in violations aggregating \$5,000 or more. In case of aliases, supply information that is available regarding the true identity as well as the alias identity. This includes drivers' license or social security numbers, addresses, and telephone numbers.
- **Criminal violations aggregating \$25,000 or more regardless of a potential suspect.** If there is no substantial basis for identifying a possible suspect or group of suspects, the reporting threshold is \$25,000.
- **Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.** File a SAR for a BSA violation involving \$5,000 or more in funds or other assets conducted or attempted by, at, or through the credit union. This includes transactions where the credit union knows, suspects, or has reason to suspect that:
 - The transaction(s) involves funds from illegal activities or is intended to hide/disguise funds from illegal activities, including attempts to hide the ownership, nature, source, location or control of funds;
 - The transaction(s) is designed to evade any requirements of the BSA regulations; or
 - The transaction(s) has no business or apparent lawful purpose or is not the sort in which the particular member/customer would normally be expected to engage, 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, share certificate or other monetary instrument; or any other payment, transfer, or delivery by, through, or to a credit union.

Keep in mind that the BSA requires the filing of a Currency Transaction Report (CTR) when a currency transaction exceeds \$10,000. If a currency transaction exceeds \$10,000 and is suspicious, then file both the CTR (reporting the currency transaction) and the SAR (reporting the suspicious or criminal aspects of the transaction). If a currency transaction is below \$10,000 and is suspicious, then file the SAR only. For more information about CTRs, see The League's *ii Release No. 071*.

Computer intrusion

"Computer intrusion" is among the crimes to be reported on a SAR. This is defined as gaining access to a computer system of a financial institution to:

- Remove, steal, procure or otherwise affect funds of the credit union or its members/customers;
- Remove, steal, procure or otherwise affect critical information of the credit union including member/customer account information; or
- Damage, disable or otherwise affect critical systems of the credit union.

Computer intrusion does not mean attempted intrusions of websites or other non-critical information systems that do not provide access to the credit union's or members' financial or other critical information.

Credit unions must have a written information security program. It must address how the credit union will respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member. In addition, all federally insured credit unions must notify the NCUA as soon as possible, and no later than 72 hours, after the credit union reasonably believes it has experienced a "reportable cyber incident" or received a notification from a third party regarding such an incident. For more information, see The League's *ii Release No. 0155, "NCUA Guidelines for Safeguarding Member Information & Reporting of Unauthorized Access."*

Robberies and burglaries

A SAR does not need to be filed for robberies or burglaries that are reported to local authorities.

Also, a SAR does not need to be completed for lost, missing, counterfeit, or stolen securities if the credit union files a report pursuant to the reporting requirements of Securities and Exchange Commission regulations.

Marijuana-related businesses

If the credit union serves marijuana-related businesses, see special guidance from FinCEN in *FIN-2014-G001 BSA Expectations Regarding Marijuana-Related Businesses (February 14, 2014)*. A portion of that guidance is reprinted in *Exhibit A - Filing suspicious activity reports on marijuana-related businesses* in this release. See the full text of *FIN-2014-G001* for FinCEN's due diligence considerations and red flags for financial institutions serving marijuana-related businesses. The special guidance is necessary because production, sale, and possession of marijuana, even medical marijuana is a crime under federal law, regardless of whether it is legal under state law.

Make no mistake: marijuana is currently illegal under Wisconsin law - including medical marijuana.

Hemp and CBD can be legal - if the current requirements under state and federal law are met. If the credit union services hemp or CBD businesses, it is advisable to be prepared (policies, training, and procedures) to comply with FinCEN's marijuana-related business guidance. The credit union could encounter products that don't qualify as legal hemp or CBD, so are viewed as marijuana under state and/or federal laws. Due diligence is required.

SARs and money services businesses (MSBs)

Money services business (MSB) is a term used by financial regulators to describe a business that isn't a bank or credit union but that provides some bank-like services, including currency dealers or exchangers, check cashers, issuers or sellers of traveler's checks or money orders, money transmitters, and providers or sellers of prepaid access.

Regulators have special BSA/AML compliance expectations for credit unions serving MSBs. Those expectations include adequate and ongoing suspicious activity monitoring, since some MSBs can present heightened risks.

Based on the credit union's assessment of the risks of its particular MSB members, monitoring should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time. Account activity would typically include deposits or withdrawals of currency, deposits of checks, or funds transfers. The mere

existence of variances does not necessarily mean that a problem exists, but may be an indication that additional review is needed. Furthermore, risk-based monitoring generally does not include “real-time” monitoring of all transactions flowing through the account of a MSB, such as a review of the payee or drawer of every deposited check.

While many MSBs provide services to individual customers, some MSBs provide services to other MSBs. This added layer of anonymity between the credit union and the originator of the transaction could pose additional complexity in identifying suspicious activity to the credit union. In addition, MSBs providing services to other MSBs can result in a much higher dollar amount and volume of activity, which can make it harder to identify suspicious activity or trends.

Federal regulators have provided examples of potential suspicious activity within MSB accounts, generally involving significant unexplained variations in transaction size, nature, or frequency through the account. For details, see The League’s *ii Release No. 0187 – BSA: Money Services Businesses*.

Reporting elder financial abuse

Credit unions and other financial institutions can be the “first line of defense” against financial abuse of the elderly and other adults who are at risk. Often, credit unions are quick to suspect elder financial exploitation based on staff’s familiarity with elderly members.

When credit union staff suspects elder financial abuse, Wisconsin law allows them to notify law enforcement or county adult protective service agencies. [Wisconsin law also allows a credit union to contact relatives and certain other parties \(including contacts that a member may authorize in advance\) for help when it suspects financial exploitation of a “vulnerable adult” \(meaning someone at least 65 years old or an “adult at risk”\).](#) The federal Senior Safe Act similarly allows credit unions and certain employees to report such abuse, and it encourages credit unions to train staff on recognizing and responding appropriately when elder financial abuse is suspected. Both the state and federal laws provide protections from liability for reporting suspected abuse. (At the federal level, the protection only applies if staff has had appropriate training.) For details, see The League’s *ii Release No. 0174 – Reporting Financial Abuse*. It includes a list of potential “red flags” that may signal possible financial abuse.

Credit unions should also file SARs in addition to (but not instead of) notifying authorities of suspected elder financial abuse. *The CFPB has reported* that “Financial institutions are filing an increasing number of [elder financial exploitation] SARs, but in most cases the SARs do not indicate that financial institutions are reporting elder financial exploitation to law enforcement or adult protective services. This is a missed opportunity to increase investigation and prosecution, and to make it more likely that victims will receive appropriate services.”

The SAR form includes a checkbox where filers can flag the activity as “elder financial exploitation.” Be sure to check that box when appropriate.

The *CFPB has recommended* filing Suspicious Activity Reports for any suspected elder financial abuse, regardless of the amount at stake. “If the transaction amounts are below the mandatory filing threshold, consider filing SARs anyway. ... Voluntary reporting may help deter continued financial abuse by the same perpetrator, and may help law enforcement with ongoing investigations and prosecution.”

POLICIES AND PROCEDURES TO MONITOR FOR SUSPICIOUS ACTIVITY

Your credit union’s Bank Secrecy Act & Anti-Money Laundering (BSA/AML) policy must provide for internal controls for the credit union to identify, research and report suspicious activity. See *ii Release No. 0071* for The League’s Sample BSA/AML Policy.

BSA compliance is generally “risk-based,” meaning that each credit union has to assess the level of risk it faces for suspicious activity and put together appropriate policies and procedures to meet that level of risk. The sophistication of the credit union’s monitoring systems should be dictated by the credit union’s assessment of risk, with particular emphasis on transaction volumes and higher-risk products, services, customers, and geographic locations. See *ii Release No. 0071* for more information on risk assessment.

The credit union should assign adequate staff to identify, research, and report suspicious activities. Personnel should have appropriate experience and get ongoing training to maintain their expertise.

There are four key components of an effective monitoring and reporting system:

- Identification of unusual activity;

- Managing alerts;
- SAR decision making; and
- SAR completion and filing.

Identification of unusual activity

Credit unions use a number of methods to identify potentially suspicious activity, including activity identified by employees during day-to-day operations, law enforcement inquiries or information sharing requests, transaction and automated monitoring system output, or any combination of these.

Employee identification

Employees may observe unusual activity as part of day-to-day operations. Policies, procedures and training should stress the importance of identifying potentially suspicious activity and reporting it to appropriate personnel for further research.

Law enforcement inquiries and requests

Law enforcement inquiries and requests can include criminal subpoenas, FinCEN information sharing requests (also called section 314(a) requests) and national security letters (NSLs). Due to their sensitive nature, NSLs are addressed separately in the next section. See *ii Release No. 0071* for details on 314(a) requests.

Merely receiving a law enforcement inquiry does not, by itself, require the credit union to file a SAR. Still, a law enforcement inquiry may be relevant to a credit union's overall risk assessment of its customer.

Credit unions should establish policies and procedures 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.

Due to the confidentiality of grand jury proceedings, related SARs should not reference a grand jury subpoena. The SAR should reference only those facts that support a finding of unusual or suspicious activities identified by the credit union.

National security letters

NSLs are written investigative demands that may be issued by the local FBI or other federal governmental authorities in counterintelligence and counterterrorism investigations.

NSLs are highly confidential. No credit union, or officer, employee or agent of the credit union, can disclose to anyone that a governmental authority has sought or obtained access to records through an NSL. Credit unions that receive NSLs must ensure that procedures are in place for processing and maintaining the confidentiality of the letters.

If a credit union files a SAR after receiving an NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts that support a finding of unusual or suspicious activities identified by the credit union.

Questions regarding NSLs should be directed to the credit union's local FBI field office.

Customer due diligence (CDD)

Credit unions must have written, risk-based procedures for conducting CDD as part of their BSA/AML compliance programs. Compliance is mandatory as of May 11, 2018. (Prior to 2018, FinCEN did not explicitly require credit unions or other covered financial institutions to engage in CDD, though regulators and examiners expected it and said it was “implicitly required” by BSA suspicious activity reporting obligations.)

Among other things, CDD helps credit unions understand the nature and purpose of member/customer relationships to develop a risk profile, monitor for suspicious transactions, and conduct “enhanced due diligence” on higher-risk members/customers. According to the federal regulators’ *BSA/AML Examination Manual*, the objective of CDD is for the credit union to predict “with relative certainty” the kinds of transactions a member is likely to conduct, in order to help spot suspicious transactions, including transactions that are not of the sort the member would be normally expected to engage in. To do this, you will need to rely on the “customer profile” information you gather at account opening, which should help you to understand what level of normal activity to expect for the member’s occupation or business operations.

Manual transaction monitoring

Having a manual transaction monitoring system means reviewing reports generated by the credit union's management information systems (MIS) or by vendor systems. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, and non-sufficient funds reports. Some credit union's MIS are supplemented by vendor systems designed to identify reportable currency transactions and to maintain funds transfer records. Many vendor systems also include filters for identifying unusual activity.

The manual transaction monitoring process may involve reviewing daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used depends on the credit union's BSA/AML risk profile. The reports should appropriately cover its higher-risk products, services, customers, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Management should select appropriate thresholds to detect unusual activity and periodically evaluate whether the filtering criteria is appropriate for their credit union. In addition, the credit union's monitoring systems should be independently reviewed for reasonableness of filtering criteria.

Typical manual transaction monitoring reports are Currency Transaction Reports, Funds Transfer Records, and Monetary Instrument Records. Each is discussed below.

- *Currency transaction reports.* The BSA requires the reporting of large currency transactions on CTRs. Most vendors offer reports to help credit unions with filing CTRs and identifying suspicious currency activity. Currency activity reports can generally be filtered using various parameters, for example:

- Currency transactions aggregated by customer name, tax identification number, or customer information file number.

It is also important to aggregate transactions based on the identity of the person making the transaction, not just by the name(s) or tax identification number(s) of the account owner(s). For example, if an authorized signer on a business account deposits \$6,000 in cash into that account and another \$6,000 into his/her personal account, those transactions should trigger a CTR or SAR. Similarly, if a power of attorney agent or guardian for a member withdraws cash from that member's account and from the agent's or guardian's own account, those transactions should trigger a CTR or SAR. Credit unions should consult their data processing system vendors to determine whether/how they can aggregate transactions in this way.

- Currency activity including multiple transactions greater than \$10,000.
- Currency activity (single and multiple transactions) below the \$10,000 reporting requirement (e.g., between \$7,000 and \$10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., \$3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., \$30,000).

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, will help a credit union identify and evaluate unusual currency transactions.

- *Funds transfer records.* The BSA requires credit unions to maintain records of funds transfer in amounts of \$3,000 or more. Periodic review of this information can help credit unions identify patterns of unusual activity.

Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions. Each credit union should establish its own filtering criteria for both individuals and businesses.

A periodic review of the funds transfer records in credit unions with few funds transfers is usually sufficient to identify unusual activity. For credit unions with more significant funds transfer activity, using a spreadsheet or vendor software is an efficient way to spot unusual patterns.

- *Monetary instrument records.* The BSA requires credit unions to keep records of certain monetary instrument sales. Such records can help the credit union identify possible currency structuring through the purchase of cashier's checks, official credit union checks, money orders, or traveler's checks in amounts of \$3,000 to \$10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees.

Automated account monitoring

Credit unions that are large, operate in many locations, or have a large volume of higher-risk customers typically use automated account-monitoring systems. These systems use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the credit union's core data processing system.

System parameters and filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of customer. Parameters and filters should be tested through a review of specific higher-risk customers, products and services before implementation to identify any gaps (common money laundering techniques, including cash structuring or frauds) that may not have been addressed.

The authority to establish or change system parameters and filtering criteria should be clearly defined and should generally require the approval of the BSA compliance officer or senior management. Controls should ensure limited access to the monitoring system.

Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the credit union's risks. Management should also periodically evaluate the filtering criteria and thresholds established to ensure that they are still effective. In addition, the credit union's monitoring system should be independently validated and reviewed for reasonableness of filtering criteria.

Managing alerts

Credit unions should have policies, procedures, and processes in place for referring unusual activity from all areas of the credit union to the personnel responsible for evaluating and reporting suspicious activity. There should be a clear and defined escalation process from initial detection to the end of the investigation.

Staff should have sufficient internal and external tools to properly research activities and formulate conclusions. Internal research tools include access to account systems and account information, including Customer Due Diligence (CDD) and enhanced due diligence (EDD) information. See *ii Release No. 0159* for more information on Customer Due Diligence. External research tools may include widely available Internet media search tools, as well as those accessible by subscription.

Identifying underlying crime

Credit unions are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes. However, credit unions are not obligated to confirm the underlying crime (e.g., terrorist financing, tax evasion, money laundering, and various types of fraud). Investigation of criminal activity 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.

SAR decision making process

After thorough research and analysis has been completed, findings are typically forwarded to an individual or committee with the authority to make the final SAR filing decision. Credit unions will find it helpful to document SAR decisions, including the specific reasons(s) for filing or not filing a SAR. The decision to file a SAR is an inherently subjective judgment. Examiners will focus on whether the credit union has an effective SAR decision-making process and may review individual SAR decisions as a way to test the effectiveness of the overall SAR monitoring, reporting and decision-making process.

SAR completion and filing

Appropriate policies, procedures and processes should be in place to ensure SARs are complete and accurate, the narrative provides a sufficient description of the activity as well as the basis for filing and reports are filed in a timely manner.

SARs must be filed electronically, using *FinCEN's online BSA E-Filing System*.

A SAR must be filed no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified, a credit union may delay filing for an additional 30 calendar days to identify a suspect.

Credit unions may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the

credit union, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity. Whenever possible, a prompt review of the transaction or the account is helpful. In any event, the review should be done in a reasonable period of time.

SAR quality

The importance of accurate SAR information cannot be overstated. Inaccurate information on the SAR form, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. A thorough and complete narrative may make the difference in whether law enforcement clearly understands the described conduct and its possible criminal nature. Failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

FinCEN maintains a set of *frequently asked questions* about SARs, which includes guidance on completing SAR forms and *electronic filing instructions*. Credit unions can also call the FinCEN Regulatory Help Line at (800) 949-2732 for questions regarding SARs.

SAR filing on continuing activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This is accomplished by a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the NCUA.

FinCEN's guidance permits credit unions to file SARs for continuing activity after a 90 day review, with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Credit unions may also file SARs on continuing activity earlier than the 120 day deadline if the credit union believes the activity warrants earlier review by law enforcement. This practice will notify law enforcement of the continuing nature of the activity, and remind the credit union that it should continue to review the suspicious activity to determine whether other actions may be appropriate (like deciding that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing).

The credit union's policies, procedures, and processes may address repeat SAR filings. The procedures may include:

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

CASES REQUIRING IMMEDIATE ATTENTION

For violations requiring immediate attention, such as when a reportable violation is ongoing, a credit union is required to immediately notify, by telephone, an appropriate law enforcement authority and as necessary the credit union's primary regulator, in addition to filing a timely SAR.

An appropriate law enforcement authority would generally be the local office of the IRS 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.

Credit unions should be aware that law enforcement might have an interest in ensuring that certain accounts remain open notwithstanding suspicious activity in connection with those accounts. If a law enforcement agency requests that a credit union maintain a particular account, the credit union should ask for a written request. Refer to "Requests by Law Enforcement for Financial Institutions to Maintain Accounts," June 13, 2007, at www.fincen.gov for further guidance. Ultimately, the decision to maintain or close an account should be made by a credit union in accordance with this own standards and guidelines.

BOARD OF DIRECTORS NOTIFICATION

A credit union must promptly notify its board of directors, or a committee designated by the board, of any SAR that is filed. The NCUA's Regulatory Alert 06-RA-07 indicates notification must be at least monthly. Notification at the monthly board meeting is adequate, unless the seriousness of an activity merits immediate reporting.

The credit union may provide actual copies of SARs to the board of directors or a board committee, or it could provide summaries, tables of SARs filed for specific violation types, or other forms of notification. America's Credit Unions says

that the best approach is simply to notify the board that a SAR has been filed, whether the SAR involved a member or employee, what dollar amount might be involved, and other general information about the circumstances that led to the SAR. This approach protects the credit union from SAR details being circulated. Such gossip could violate federal law, since SAR filings must be kept confidential.

In the rare instance when the suspect of the SAR is an individual in the organization, such as the president, a director or a member of the designated committee that reviews SARs, the credit union must not notify the suspect. Deviations to established policies and procedures to avoid notification to a subject of the SAR should be documented and appropriate uninformed senior organizational personnel should be so advised. Refer to “The SAR Activity Review—Trends, Tips & Issues, Issue 2, June 2001” available at www.fincen.gov for further guidance.

PROHIBITION ON SAR DISCLOSURE

No credit union, and no director, officer, employee, or agent of a credit union, that reports a suspicious transaction may notify any person involved in the transaction that it has been reported. This means that any person subpoenaed or otherwise asked to disclose a SAR or the information contained in a SAR, must decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed except when such disclosure is requested by FinCEN or appropriate law enforcement or federal credit union regulator.

FinCEN and the NCUA must be notified of any such request and of the credit union's response. Furthermore, FinCEN and the NCUA take the position that credit unions' internal controls for the filing of SARs should minimize the risks of disclosure.

SAR sharing with an affiliate

FinCEN has stated that a depository institution that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, as defined in FIN-2010-G006, provided the affiliate is subject to a SAR regulation. The sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a SAR rule. Therefore, such sharing within the depository institution's corporate organizational structure is consistent with the purposes of the BSA. As is the case with sharing SARs with head offices and controlling companies, there may be circumstances under which a depository institution, its affiliate, or both entities would be liable for direct or indirect disclosure by the affiliate of a SAR or any information that would reveal the existence of a SAR. Therefore, the depository institution, as part of its internal controls, should have policies and procedures in place to ensure that its affiliates protect the confidentiality of the SAR.

RECORD RETENTION

A credit union must maintain documentation to support the specific reasons for filing or not filing a SAR and a copy of any SAR that it files for five years from the date of the report. Supporting documentation is considered a part of the filed report even though it should not be actually filed with the submitted report.

Providing supporting documentation to law enforcement

Credit unions must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking 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 federal banking agency. For more information, see FinCEN's 2007 guidance titled, “*Suspicious Activity Report Supporting Documentation*” (Fin-2007-G003).

SAFE HARBOR

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 that 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 credit union is protected from liability for any disclosure in the report, or for failure to disclose the existence of the report, or both. This protection applies if the report is filed pursuant to NCUA rules or is filed on a voluntary basis.

ACCOUNTS AND SERVICES

The credit union cannot close a member's account or restrict services simply because a SAR has been filed. According to the NCUA Examiner's Guide:

“Since a credit union member has a fundamental right to maintain a share account and participate in elections, the credit union cannot deny someone credit union membership because it has identified suspicious activity.

However, the credit union may wish to consider limiting access to certain services. To do so, the credit union must have established its policy in writing and notified its members of the policies in advance.”

If an employee is the subject of a SAR, the credit union may need to consider reassigning or terminating the services of the employee, according to America's Credit Unions. However, the credit union should seek advice from its legal counsel in these situations.

* * * * *

League publications are designed to provide accurate information with regard to the subject matter covered, with the understanding that The League does not render legal services. If you have general questions regarding this release, please call The League at (608) 540-4050 if local or (800) 242-0833. For specific legal advice, please consult your credit union's attorney.

Legal Affairs Department

PEG/jb

© 2025 Wisconsin Credit Union League

EXHIBITS

A. Filing suspicious activity reports on marijuana-related businesses

EXHIBIT A - FILING SUSPICIOUS ACTIVITY REPORTS ON MARIJUANA-RELATED BUSINESSES

Former U.S. Department of Justice Deputy Attorney General James M. Cole issued a memorandum (the “Cole Memo”) to all United States Attorneys providing updated guidance to federal prosecutors concerning marijuana enforcement under the federal Controlled Substances Act. The Cole Memo guidance applied to all of DOJ’s federal enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states. The Cole memo was repealed by the DOJ in 2018. But the Treasury Department’s FinCEN preserves application of the Cole Memo Priorities in its guidance to financial institutions serving marijuana-related businesses.

The Cole Memo priorities are:

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

The guidance below is from FIN-2014-6001 BSA Expectations Regarding Marijuana-related businesses.

Filing suspicious activity reports on marijuana-related businesses

The obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity. A financial institution is required to file a SAR if, consistent with FinCEN regulations, the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution:

- (i) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity;
- (ii) is designed to evade regulations promulgated under the BSA, or
- (iii) lacks a business or apparent lawful purpose. (Financial institutions shall file with FinCEN, to the extent and in the manner required, a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a SAR with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations.)

Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity.

Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN’s suspicious activity reporting requirements and related thresholds.

One of the BSA’s purposes is to require financial institutions to file reports that are highly useful in criminal investigations and proceedings. The guidance below furthers this objective by assisting financial institutions in determining how to file a SAR that facilitates law enforcement’s access to information pertinent to a priority.

“Marijuana Limited” SAR filings

A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a “Marijuana Limited” SAR. The content of this SAR should be limited to the following information:

- (i) identifying information of the subject and related parties;
- (ii) addresses of the subject and related parties;
- (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv) the fact that no additional suspicious activity has been identified. Financial institutions should use the term “MARIJUANA LIMITED” in the narrative section.

A financial institution should follow FinCEN’s existing guidance on the timing of filing continuing activity reports for the same activity initially reported on a “Marijuana Limited” SAR. The continuing activity report may contain the same limited content as the initial SAR, plus details about the amount of deposits, withdrawals, and transfers in the account since the last SAR. However, if, in the course of conducting customer due diligence (including ongoing monitoring for red flags), the financial institution detects changes in activity that potentially implicate one of the Cole Memo priorities or violate state law, the financial institution should file a “Marijuana Priority” SAR.

“Marijuana Priority” SAR filings

A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a “Marijuana Priority” SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include:

- (i) identifying information of the subject and related parties;
- (ii) addresses of the subject and related parties;
- (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and
- (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity.

Financial institutions should use the term “MARIJUANA PRIORITY” in the narrative section to help law enforcement distinguish these SARs.

“Marijuana Termination” SAR filings

If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should file a SAR and note in the narrative the basis for the termination. Financial institutions should use the term “MARIJUANA TERMINATION” in the narrative section. To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity. See FinCEN’s *Section 314(b) Fact Sheet* for more information.

Red flags to distinguish priority SARs

The following red flags indicate that a marijuana-related business may be engaged in activity that implicates one of the Cole Memo priorities or violates state law. These red flags indicate only possible signs of such activity, and also do not constitute an exhaustive list. It is thus important to view any red flag(s) in the context of other indicators and facts, such as the financial institution’s knowledge about the underlying parties obtained through its customer due diligence. Further, the presence of any of these red flags in a given transaction or business arrangement may indicate a need for additional due diligence, which could include seeking information from other involved financial institutions under Section 314(b). These red flags are based primarily upon schemes and typologies described in SARs or identified by our law enforcement and regulatory partners, and may be updated in future guidance.

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
 - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
 - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
 - The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
 - The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
 - The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.
 - Deposits apparently structured to avoid Currency Transaction Report (“CTR”) requirements.
 - Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
 - Deposits by third parties with no apparent connection to the accountholder.
 - Excessive commingling of funds with the personal account of the business’s owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
 - Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
 - Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
 - A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.
- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of significant outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a “consulting,” “holding,” or “management” company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.

- A marijuana-related business's proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).