

SECTION 3 – THE BANK SECRECY ACT

Prepared by: Thomas C. Leduc

Section 3 – The Bank Secrecy Act

General Overview

We've all heard the expression "Crime doesn't pay." Indeed, when a perpetrator of crimes is apprehended, indicted, convicted, and sentenced, that lesson is learned the hard way. Sad but true, however, is the fact that — at least until the bad guys are apprehended — some crime *does* pay. Or, perhaps more accurately, crime reaps payments. And crime doesn't usually accept credit cards — it takes its payment largely in cold, hard cash. Whether the crime is blackmail, drug dealing, tax evasion, illegal gambling, loan sharking, embezzlement, or a wide range of other types of activity that our laws have defined as criminal, the successful criminal eventually winds up with a pile of currency.

But that currency can present a problem. In order to put this money to work, it must eventually re-enter into circulation – "laundering" the illegally obtained funds into legitimate funds.

Because of the banking system's large — if unwanted — role in allowing criminals to launder their money, Congress has passed a collection of laws referred to as the "Bank Secrecy Act." In an effort to provide assistance to law enforcement, "banks" are required to keep certain records and file certain reports regarding currency and other transactions.

The Bank Secrecy Act is perhaps misnamed. It applies to much more than just "banks" — as that term is commonly used — and it has more to do with divulging secrets than keeping them.

In this section, we will briefly discuss the various laws that make up the Bank Secrecy Act (BSA). Next we will turn our attention to the NCUA regulation that generally mandates BSA compliance for all federally insured credit unions. Finally, we will discuss the particular recordkeeping and reporting requirements that are at the heart of BSA compliance.

Many of the various statutes and regulations that financial institutions must comply with are created with consumer protection in mind. The BSA is not, however, about consumer protection — it is a law enforcement tool. Violations of the various Bank Secrecy Act laws and regulations can expose credit unions to both civil and criminal penalties.

The laws that form “Bank Secrecy Act” compliance

Although terms like “Bank Secrecy Act” or “BSA” are frequently used in connection with the compliance duties of financial institutions, they do not usually refer to a single statute. The following is a list of the laws and regulations that come into play when discussing BSA compliance.

- Antidrug Abuse Act of 1986;
- Money Laundering Control Act of 1986;
- Bank Secrecy Act of 1970;
- Currency and Foreign Transactions Reporting Act;
- NCUA Rules and Regulations Part 748.2;
- Financial Recordkeeping and Reporting of Currency and Foreign Transactions rules; and
- Title III of the USA PATRIOT Act.

Antidrug Abuse Act of 1986

This law was enacted to help federal law enforcement’s efforts to thwart illicit drug crops, to stop international drug trafficking, to improve the enforcement of the antidrug laws already on the books, and to establish more effective drug abuse and prevention programs.

Money Laundering Control Act of 1986

The Money Laundering Control Act — part of the Antidrug Abuse Act of 1986 — made money laundering a federal crime. It created three new criminal offenses for money laundering activities by, through, or to a financial institution. These offenses are:

- Knowingly helping to launder money from criminal activity.
- Knowingly engaging (including by being willfully blind) in a transaction of more than \$10,000 that involves property from criminal activity.
- Structuring transactions to avoid BSA reporting.

To be convicted of money laundering through a credit union, the crime must involve an amount greater than \$10,000.

Bank Secrecy Act of 1970

Perhaps best known among these various statutes is the Bank Secrecy Act of 1970. This is the federal statute that mandates, among other things, that financial institutions maintain certain records about their members’ and customers’

transactions, and report certain currency transactions in amounts greater than \$10,000.

The Currency and Foreign Transactions Reporting Act

This law requires that persons file a Report of International Transportation of Currency or Monetary Instruments (Customs Form 4790) whenever they send or receive more than \$10,000 in currency or monetary instruments out of, or into, the U.S. This statute rarely directly effects credit unions.

NCUA Rules and Regulations Section 748.2

Although the original Bank Secrecy Act of 1970 applied to credit unions, there were no rules specific to credit unions until 1986. At that time NCUA adopted a regulation that specifically provided BSA compliance requirements for federally insured credit unions.

NCUA Rules and Regulations Section 748.2 requires all federally insured credit unions to develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements in the Bank Secrecy Act. NCUA requires that credit unions' compliance programs adhere to the requirements in 31 CFR 103 — the BSA regulations adopted by the U.S. Treasury Department. Each credit union must have a written plan that has been approved by their board of directors.

NCUA requires that each credit union's formal BSA compliance plan must:

- Provide for a system of internal controls to ensure ongoing compliance.
- Provide for independent testing for compliance to be conducted by credit union personnel or outside parties.
- Designate an individual responsible for coordinating and monitoring day-to-day compliance.
- Provide training for appropriate personnel.

The Financial Recordkeeping and Reporting of Currency and Foreign Transactions

This Treasury Department regulation is contained in Part 103 of Title 31 of the Code of Federal Regulations (31 CFR 103) and outlines the basic BSA reporting and recordkeeping requirements.

It was enacted to implement the requirements of the Bank Secrecy Act of 1970. The main requirements for credit unions include:

- Filing a Currency Transaction Report (CTR) for transaction in currency in amounts greater than \$10,000.

- Filing a Suspicious Activity Report (SAR) when a transaction appears suspicious in nature.
- Keeping records of the sale of bank checks, cashier's checks, money orders, or traveler's checks for \$3,000 to \$10,000 in currency, and
- Penalties for noncompliance with the requirements.

The Treasury broadly defines the term “bank” to include all credit unions — both state and federally chartered. Throughout the remainder of this section, references to rules regarding BSA compliance will be to the regulations in 31 CFR 103.

The USA PATRIOT Act

Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 of the USA PATRIOT Act amends the Bank Secrecy Act and targets money laundering issues. One provision of this law requires financial institutions – including credit unions – to have minimum standards to verify the identity of members when opening accounts. Another requirement is that financial institutions have antimoney-laundering programs in place. NCUA regulations already require federally insured credit unions to have a compliance program similar to the anti-money-laundering programs required by this act.

The USA PATRIOT Act also requires a financial institution to search its records when a request is received from FinCEN to determine:

- If the financial institution maintains or has maintained accounts for the individuals or organizations named in the request.
- If the financial institution has engaged in transactions with the individuals or organizations listed on the request.

Reporting Requirements

A number of different reporting requirements are included in the BSA regulations. For credit unions, the Currency Transaction Report (IRS Form 104, or CTR) is the most familiar. The CTR is, for credit unions, the centerpiece of compliance with the BSA. Other required reports include Suspicious Activity Reports and Reports of International Transportation of Currency or Monetary Instruments.

Currency Transaction Reports

The Currency Transaction Report (CTR) is used to track large cash transactions. In general, a credit union must complete and submit a CTR each time it takes a

Figure 3-1

CTR or No CTR?
<p>Q. A member deposits a check made out to cash for \$15,000 into her credit union account. Must a CTR be filed?</p> <p>A. No. A check — even one made payable to cash — is not currency.</p>
<p>Q. A member deposits \$10,000 worth of \$100 bills into his credit union account. Must a CTR be filed?</p> <p>A. No. Although the transaction is in currency, it does not exceed \$10,000.</p>
<p>Q. A member withdraws \$9,000 in currency in the morning. Later that day, a teller discovers the same member withdrew \$3,000 in currency that same day at another branch of the same credit union. Must a CTR be filed?</p> <p>A. Yes. Same-day withdrawals are aggregated.</p>
<p>Q. A member deposits \$9,000 in currency into his credit union account in the morning. Later that day, a teller discovers that the same member withdrew \$3,000 in currency that same day at another branch of the same credit union. Must a CTR be filed?</p> <p>A. No. Same-day deposits and withdrawals are not aggregated with each other (although same-day multiple withdrawals are aggregated and same-day multiple deposits are aggregated among themselves).</p>

deposit, gives a withdrawal, or exchanges currency, if the transaction involves currency of more than \$10,000.

In addition, multiple same-day transactions completed at any branch of a credit union must be treated as a single transaction if the credit union has knowledge that those transactions are by or on behalf of the same individual. If those multiple transactions result in total cash into or cash out of the credit union, in excess of \$10,000, a CTR must be filed.

Two points to keep in mind:

- 1) No CTR is required unless the transaction or transactions amount to more than \$10,000 in currency coming into or going out of the credit union. There is no need to file a CTR for a cash deposit of exactly \$10,000. Figure 3-1 provides different scenarios illustrating when a CTR is or is not needed.
- 2) The transaction must be in currency to be reportable. BSA defines currency as the coin and paper money of the U.S., as well as the coin and paper money designated as legal tender of any other country. Some examples include U.S.

revision notes, Federal Reserve notes, and official foreign notes that are customarily used and accepted as a medium of exchange in a foreign country.

Reportable CTR transactions must be filed by the credit union within 15 days following the date of the transaction (25 days if filed magnetically or electronically). A copy of the CTR with instructions is available at http://www.fincen.gov/reg_bsaforms.html#finform1041. A copy of the form with instructions is also reproduced in Appendix 3-A of this section.

Proper identification required

Under the BSA regulations, credit unions are required to verify and record the name and address of any member presenting a transaction that will be reportable on a CTR. The identity, account number, and Social Security, or taxpayer identification number of the person on whose behalf a reportable transaction is made must also be included. If the individual claims to be an alien or a nonresident of the U.S., the credit union must verify his or her identification by reviewing a passport, alien identification card, or other official document evidencing nationality or residence.

Exemptions

Recognizing that not all transactions involving more than \$10,000 in currency are likely to have value in assisting law enforcement officials investigating potential criminal activity, the BSA regulations allow credit unions to exempt certain transactions from the general reporting requirements. A credit union is not required to file a CTR for a transaction completed by an exempt person, provided the transaction falls within the exempt person's stated limits.

revision There are two categories (Phase I and Phase II) of potential "exempt persons" listed in the BSA regulations. See 103.22(d)(2). Under the Phase I designation, transactions in currency by credit unions/banks, governmental departments or agencies and public or listed companies and their subsidiaries are exempt from reporting. Phase II designees are exempt from reporting transactions in currency made by smaller businesses (such as non-listed businesses and payroll customers) that meet specific criteria as laid out in FinCEN's guidance (Advisory No. 10, "Reformed CTR Exemption Process: Questions & Answers" October 1998).

FinCEN identifies five categories of Phase I exempt persons:

- A credit union or bank (domestic operations only).
- A department or agency of the U.S., any states, or political subdivision of a state.
- Any entity exercising governmental authority within the United States.

- Any entity (other than a credit union or bank) whose common stock is listed on the New York, American or Nasdaq stock exchanges (with some exceptions).
- Any subsidiary (other than a credit union or bank) of any “listed entity” that is organized under U.S. law and at least 51 percent of its stock is owned by the listed entity.

FinCEN identifies two categories of Phase II exempt persons:

- A business – other than a publicly listed corporation or subsidiary as listed above – that has maintained a transaction account with the credit union for at least 12 months; frequently engages in transactions in currency with the credit union in excess of \$10,000; and is organized or incorporated under the law of the U.S. or a state. See, § 103.22 (referred to in the regulation as “non listed businesses”).
- A person or business that has maintained a transaction account with the credit union for at least 12 months; operates a firm that regularly **withdraws** more than \$10,000 in order to pay its employees in currency; and is incorporated or organized under the laws of the U.S. or a state. Exemption only applies to payroll withdrawals. See, § 103.22 (referred to in the regulation as “payroll customers”).

CTR Exemption Renewal

revision

The credit union must document information supporting a Phase I exemption designation and that documentation must be reviewed and verified at least once per year. With respect to Phase II exemption designations (“non-listed businesses” and “payroll customers”), the designation must be **renewed** every two years by filing the Designation of Exempt Person form each March 15th. This report is due by March 15th of the second calendar year following the year in which the member was first designated as an “exempt person,” then each March 15th thereafter. Under the biennial renewal process, the credit union must: (i) include information regarding a change of control over the Phase II exempt designee known to the credit union (or which should have been known) and (ii) certify that the credit union has applied its suspicious activity monitoring process to the currency transactions of the “exempt person” at least annually. A copy of this form is available at your local IRS forms office or via BSA Direct E-filing at <http://bsaefiling.fincen.treas.gov/index.jsp>

A number of businesses are ineligible under BSA regulations to receive “exempt person” status. A business is ineligible if it is engaged in one or more of the following activities:

- Service as a nonbank financial institution or an agent of a nonbank financial

institution (examples of financial institutions that are not banks include securities brokers, check cashers, sellers of traveler's checks, or telegraph companies that wire funds).

- Purchase or sale to customers of motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- The practice of law, accountancy, or medicine.
- The auctioning of goods.
- The chartering or operation of ships, buses, or aircraft.
- Gaming of any kind except licensed parimutuel betting at race tracks.
- Investment advisory services or investment banking services.
- Real estate brokerage.
- Pawn brokerage.
- Title insurance and real estate closing.
- Trade union activities.
- Any other activities that may be specified by the Financial Crimes Enforcement Network (FinCEN) – the division of the U.S. Treasury charged with BSA enforcement.

The procedure to designate a member as an “exempt person” was substantially revised in 1998. A credit union must now report to FinCen each member who is considered an “exempt person.” To designate a member as exempt, the credit union must file FinCEN form 110 called the “Designation of Exempt Person” form. This designation must be completed within 30 days of the first otherwise reportable transaction between the credit union and the “exempt person.”

Note: Prior to the 1998 rule change, credit unions had different requirements for granting and recording exemptions.

Remember, although a credit union might designate a member as an “exempt person” under these rules, it must still file Suspicious Activity Reports when circumstances dictate. Also, FinCEN can revoke the status of a member as an “exempt” person upon written notice.

Geographic targeting

From time to time, FinCEN may determine that there are reasonable grounds for requiring additional recordkeeping and/or reporting requirements under the BSA regulations within a certain geographical area. In these cases, the Secretary of the Treasury may issue an order requiring any domestic financial institution or group of financial institutions in a geographic area to file CTRs for specially

described dollar thresholds. For example, the Secretary could issue an order for all financial institutions in a given area to file CTRs for cash transactions exceeding, say, \$6,000 in currency, as opposed to the usual \$10,000.

A special order of this nature is directed to the chief executive officer (CEO) of an affected credit union. It clearly describes the types of transactions that must be reported, including the following:

- Dollar amount of transactions that must be reported.
- Types of transactions that must be reported.
- Appropriate form to use to file the report.
- Address for filing the report.
- Starting and ending dates for the special reporting.
- Name of a Treasury official to contact for additional information or questions.
- Amount of time the special reports and records of those reports must be retained.

These special orders are not effective for 60 days, but can be renewed in exactly the same way as the original special order was issued. Unless directed otherwise, a credit union can continue to use the exemptions it has already granted members.

Suspicious Activity Reports

In 1996, FinCEN developed a new form, the Suspicious Activity Report (SAR). Credit unions and other financial institutions are required to use this form to report transactions that indicate possible illegal activity. An SAR must be filed for any transaction that involves or aggregates more than \$5,000 if the credit union knows, suspects, or has reason to suspect that the transaction:

- Involves funds from illegal activities, or is intended to hide funds or assets from illegal activities, as part of a plan to violate or evade any federal law or regulation or to avoid any CTR requirement.
- Is designed to evade any requirements of any regulations established under the Bank Secrecy Act.
- Has no business or apparent lawful purpose, or is not the type of activity the member would normally engage in, and the credit union knows of no reasonable explanation for the transaction after examining the available facts.

In addition to the rules regarding SAR filing, the NCUA requires that credit unions file an SAR in the following situations:

- Whenever any known or suspected criminal violation has been committed



AUDIT CHECKLIST

against a credit union, regardless of the amount of money involved, if the credit union believes the violation was committed by an “insider” — for example, a director, officer, employee, agent, or other institution-affiliated party.

- Whenever any known or suspected criminal violation, involving \$5,000 or more, has been committed against a credit union and a possible suspect (who is not an insider) can be identified.
- Whenever any known or suspected criminal violation, involving \$25,000 or more, has been committed against a credit union regardless of whether or not any suspects have been identified.
- Whenever there are transactions aggregating \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.

An SAR must generally be filed within 30 days of the time in which the credit union is aware of the facts that might constitute a basis for filing the form. If no suspect was identified at the time the credit union first discovered the facts which might lead to the filing of an SAR, the filing can be delayed up to an additional 30 days. See, § 103.18(b) (3).

The SAR must be filed with FinCEN. Credit unions should not file supporting documentation with the SAR. Instead, credit unions must maintain records of all supporting documentation related to a filed SAR (along with a copy of the SAR) for a period of at least five years from the filing date.

FinCEN has revised the SAR a few times in an effort to make the form more user friendly. Additionally, new software has been created to assist in the preparation and filing of the SAR form. A copy of the SAR as well as any new software updates are available via the Internet at www.fincen.gov/reg_bsaforms.html. SAR forms are also available at your local IRS forms office.

It is important to note that a credit union need not file an SAR for a robbery or burglary committed or attempted, as long as that robbery or burglary is reported to appropriate local law enforcement authorities. When completing the SAR, be sure to indicate if the criminal activity involves identity theft, pretext calling, or computer intrusion.

A credit union that files an SAR may not notify any person involved in the transaction about the filing. And, if an individual inquires about whether an SAR has been filed, the credit union is required to report the inquiry to FinCEN.

Filing a Suspicious Activity Report is a serious matter. Credit unions should carefully consider the information provided to federal law enforcement agencies, bearing in mind the protections afforded individuals through the Right to Financial Privacy Act. When in doubt, consult your manager or compliance department prior to filing an SAR.

Report of International Transportation of Currency or Monetary Instruments

BSA regulations also require that a Report of International Transportation of Currency or Monetary Instruments (Customs Form 4790) be filed whenever a person sends or receives more than \$10,000 in currency or monetary instruments (checks, money orders, traveler's checks and so on) into or out of the U.S. Credit unions are very seldom required to file this particular report.

A credit union must file a Form 4790:

- When the credit union physically transports, mails, or ships currency and/or monetary instruments in excess of \$10,000 at one time into, or out of, the U.S.;
or
- When the credit union receives currency and/or monetary instruments in excess of \$10,000 at one time, which has been transported, mailed, or shipped to it by a member from a location outside the U.S.

Note that a credit union is not considered to have "received" the currency or monetary instruments if the member deposits it into his credit union account, even if the credit union knows that the currency or instruments were received or transported from a place outside the U.S. In such a case, the member would have the duty to file the report, assuming the member was the person who transported, shipped, or received the currency and monetary instruments. The credit union has no obligation to inform the member of this duty to file the report, but FinCEN asks that the credit union do so.

IRS Form 90-22.1

Credit unions that have financial account relationships outside the U.S. that exceed \$10,000 are required to file an annual IRS Form 90-22-1. Credit unions that have such foreign accounts should call the IRS at 1-800-829-3676 for more information about this form.

Filing Forms Electronically

The Financial Crimes Enforcement Network (FinCEN) provides credit unions access to the BSA Direct E-Filing system, which now replaces the Patriot Act Communication System or (PACS). The system supports secure electronic filing of Bank Secrecy Act (BSA) forms (single or batched) such as Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs) and Designation of Exempt Person forms (DEP) over the Internet in encrypted form. In addition, institutions can use this system to send secure messages to FinCEN and receive responses, when appropriate. Finally, FinCEN can use the BSA E-Filing system to issue

advisories and BSA E-Filing system updates to the user community.

Institutions that are not equipped to use the E-Filing system can continue to file magnetic tape or paper reports. For additional questions, credit unions can contact the BSA E-Filing Help Desk at 1-888-827-2778 (option 6) or BSAEFilingHelp@notes.tcs.treas.gov. The BSA Direct E-Filing homepage can be found at <http://bsaefiling.fincen.treas.gov/index.jsp>.



RECORD RETENTION

Recordkeeping Requirements

Part of the initial motivation behind the various BSA statutes and regulations was the fact that, until the original Bank Secrecy Act was passed in 1970, law enforcement officials were frequently frustrated in their attempts to convict perpetrators of financial crimes due to the lax recordkeeping practices of many banks. So, a great deal of the BSA compliance burden lies in its recordkeeping requirements. A number of specific records that must be retained by financial institutions are listed in the regulations. All of these records must be retained for five years. The good news, from the standpoint of compliance burdens, is that these types of records are now commonplace for financial institutions. Each of the specific recordkeeping requirements will be discussed. Credit unions must retain either the original, a microfilm, or other copy of these records for at least five years.

Filed Reports

Records of all BSA-related reports — Currency Transaction Reports, Suspicious Activity Reports, or Reports of International Transportation of Currency or Monetary Instruments — must be retained for at least five years.

Certain Credit Extensions

Credit unions must maintain records of each extension of credit in amounts exceeding \$10,000, unless the credit is secured by real property. These records must be retained for five years and must include the name and address of the borrower, the amount of the loan, the nature or purpose of the loan, and the date of the loan.

Certain Transfers of Currency or Monetary Instruments

Credit unions must also maintain records of each advice, request, or instruction that is received or given regarding any transaction involving the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than \$10,000 to or from any person, account, or place outside the U.S. Even if the advice, request, or instruction is later cancelled, the credit union

must maintain the records. In addition, records of any advice, request, or instruction given to another financial institution must be retained. The retention period for these is five years.

Records Regarding a Geographic Targeting Order

As was discussed earlier, there may be instances when the Secretary of Treasury will require a financial institution or a group of financial institutions within a geographic area to maintain special records regarding currency transactions. The BSA regulations require that any such records — including any CTRs filed under the order — must be retained for as long as is specified in the order. This record retention period may not exceed five years.

Sales of Certain Monetary Instruments in Amounts Between \$3,000 and \$10,000

If a credit union sells a draft, cashier's check, teller's check, money order, or other monetary instrument to a person in an amount of \$3,000 to \$10,000, and the purchase is made in currency, certain records must be maintained. The specific requirements depend on whether a credit union sells such instruments to a member or a nonmember. These records must be retained for five years.

For sales to members, the record must include:

- The member's name.
- The date of the purchase.
- The type of instrument purchased.
- The dollar amount of the transaction.
- The serial number of each instrument purchased.

For sales to nonmembers, the record must include:

- the above information,
- the purchaser's address, Social Security number (or alien identification number), and
- the purchaser's date of birth.

Credit unions can implement policies to avoid some of these requirements. For instance, they can require a member who wishes to purchase one of these monetary instruments in cash to first deposit the cash into an account – completing the actual purchase of the instrument via a debit to that account. The U.S. Treasury clarified in 1994 that this is permissible, as long as the credit union's policy in this regard is in writing, includes formal written procedures for implementation, and applies to all deposit account holders without exception.

Note: when this recordkeeping requirement was first mandated by Congress in 1988, it included a requirement that credit unions and other financial institutions retain a centralized log containing records of these sales. In 1994, this centralized log requirement was eliminated.

Certain Wire Transfers

The BSA regulations mandate the retention of certain wire transfer records for a period of five years.

The following documents are exempt from these recordkeeping requirements:

- Records of wire transfers for less than \$3,000.
- Records of wire transfers governed by the Electronic Funds Transfer Act and Regulation E.
- Records of transfers made through an automated clearinghouse, automated teller machine, or point of sale system.

A credit union's recordkeeping requirements differ, depending on whether the credit union is the "originating bank" or the "beneficiary bank" in a wire transfer.

When a credit union acts as an originating bank, it executes a wire transfer on behalf of its member. In this case, the credit union must retain a record of:

- The originator's name and address.
- The amount, date, and payment instructions received.
- The beneficiary bank identification.
- The beneficiary's name and address, the beneficiary's account number, or any other identifiers if received with the payment order.

When a credit union serves as the beneficiary bank in a wire transfer, it is required to keep a copy of each payment order received. If the beneficiary is not an "established customer" of the credit union, the credit union must:

- Verify his or her name and address
- Retain a record of the means used to identify the person (for example, driver's license, passport, and so on).
- Retain a record of the originator's Social Security number, alien identification number, or employer identification number.

An "established customer" is a person with a credit union account or a person from whom the credit union has obtained a name, address, and taxpayer identification number and maintains a file of that information.

There are additional identity verification rules regarding individuals who are not

“established customers.” But because credit unions execute wire transfers almost exclusively for members or joint owners, these additional identity-verification procedures are not covered.

Records required under these rules must be retrievable by reference to the name and/or account number of the member who originated the transfer or the beneficiary of the transfer within a reasonable period of time.



RECORD RETENTION

Other Bank Secrecy Act Requirements

Credit unions are required to retain either the originals or copies of all of the following records for any account:

- The signature card.
- Each statement or other record for each deposit or share account showing each transaction made on the account.
- Each check, draft, or money order drawn on the credit union or issued and payable by it for more than \$100.
- Each debit of each member’s account in excess of \$100.
- Each check, draft, or transfer of credit of more than \$10,000 remitted or transferred to a person, account, or place outside of the U.S.
- Each check, draft, or transfer of credit for more than \$10,000 received directly from a bank, broker or dealer in foreign currency exchange outside the U.S.
- Each receipt of currency, other monetary instruments, investment securities, or checks and of each transfer of funds or credit of more than \$10,000 received on any one occasion from a bank, broker, or dealer in foreign currency exchange outside the U.S.
- Records in the ordinary course of business needed for the credit union to reconstruct a transaction (checking) account, trace a check in excess of \$100 deposited in such account through its domestic processing system, or supply a description of a deposited check in excess of \$100.
- A record containing the name, address, and TIN, if available, of the purchaser of each term share certificate, along with a description of the certificate, a notation of the method of payment, and the date of the transaction.
- A record containing the name, address, and TIN, if available, of any person presenting a term share certificate for payment, along with a description of the certificate and the date of the transaction.
- Each deposit slip or credit ticket reflecting a transaction, wire transfer deposit, or other direct deposit which exceeds \$100.

As with all other recordkeeping requirements under Bank Secrecy Act

regulations, account records must be maintained for at least five years. However, other regulations and state law may require longer retention times for certain records.

Information Sharing

The USA Patriot Act of 2001 encourages information sharing among financial institutions to identify and report activities that may involve terrorist acts or money laundering. Under 314(b), credit unions and associations of financial institutions may share information with other financial institutions after they file a notification with FinCEN and establish procedures to protect the security and confidentiality of the shared information.

If there are any suspicious transactions relating to money laundering or terrorist activity, credit unions may voluntarily report that information to law enforcement by completing the SAR and calling FinCEN's Financial Institution's Hotline for terrorist activity. Whereas 314(a) of the information sharing regulations also requires credit unions to expeditiously search their records when they receive a request from FinCEN. FinCEN contacts financial institutions on behalf of federal law enforcement agencies investigating money laundering or terrorist activity.

USA PATRIOT Act's Customer Identification Program Requirements

The USA PATRIOT Act of 2001 requires the U.S. Treasury Department to issue regulations providing minimum standards for financial institutions to identify and verify any person who opens an account.

CIP Requirements

Section 326 of the USA PATRIOT Act requires financial institutions to:

- Implement reasonable procedures to verify the identity of any person wanting to open an account, to the extent reasonable and practicable.
- Maintain records of the information used to verify the person's identity.
- Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.
- Provide the customer opening a new account with notice of the information collection requirement.

The aim of this rule is to protect the U.S. financial system from money

laundering and terrorist financing. According to the regulators, this rule will have the added benefit of helping to protect consumers against various forms of fraud, including the growing incidence of identity theft involving new accounts.

The regulation requires all financial institutions, including credit unions, to implement a “customer identification program” or “CIP” that requires a procedure to get identifying information from anyone opening an account and verify that information. The CIP procedures must enable the credit union to form a reasonable belief that it knows the true identity of the accountholder.

Credit unions must apply its CIP to each person that establishes a new account relationship with it. This includes not only members, but joint accountholders, co-borrowers and businesses.

Required Information

Credit unions are required to get at least four pieces of information from each new member/customer. At a minimum, the credit union must obtain the person’s:

1. Name
2. Date of birth (for an individual)
3. Address
 - Credit unions must get a residential or business street address so that there is a physical location at which someone could be contacted by a government investigator if the information is ever requested from the credit union. The credit union does not, however, have to keep this information current for CIP purposes.
 - If the prospective individual member or customer is unable to provide a residential or business street address, the credit union may accept an address of a friend or relative, or an Army Post Office (APO) or Fleet Post Office (FPO) box number.
 - The address for a business can be either the principal place of business, local office, or other physical location of the business.
 - The credit union, of course, can get additional addresses, such as a mailing address, to meet its own or the member’s needs.
4. Identification number
 - For a U.S. person, this means a Social Security number (SSN) for an individual or an employer identification number (EIN) for a business. The definition of U.S. person is a U.S. citizen or a business, partnership, or other legal entity that is established or organized under federal or state law.
 - For any non-U.S. person, which is simply any person or entity not

qualifying as a U.S. person, the credit union has more flexibility. It can obtain:

1. a Social Security number from a resident alien;
 2. an individual taxpayer identification number (ITIN);
 3. a passport number and the country of issuance;
 4. an alien identification card number; or
 5. a number and country of issuance on any other foreign government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard (perhaps a “similar safeguard” may be looking down the pike whereby technology readily exists to identify thumbprints or eye scans).
- If someone has applied for a taxpayer identification number, but has not yet received it, the credit union can still open an account as long as it confirms that the TIN application was filed before the member/customer opens an account and that the credit union gets the TIN within a reasonable period of time after the account is opened.

Member/Customer Due Diligence

Recently, NCUA, along with the joint banking agencies, released the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual. The manual is intended to provide comprehensive guidance to examiners and financial institutions regarding BSA/AML regulatory requirements and best practices.

According to the manual, financial institutions (including credit unions) are expected to develop and maintain member/customer due diligence policies. These policies would require credit unions to collect additional member information (beyond CIP requirements) during account opening, which would give the credit union an indication of the types of transactions a member is likely to engage in. The manual emphasizes the importance of such policies in aiding in the detection of unusual or suspicious activity and suggests that member/customer due diligence policies be applied to all members.

Identity Verification

Once the credit union gets all the required information from the member/customer, it must verify identity enough to establish a reasonable belief that it knows the true identity of the person.

There are two methods that credit unions can use to verify identity - documents or some nondocumentary methods. Documents are generally any unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. Once the

credit union verifies the member/customer through a document, it does not have to take steps to determine whether the document is valid (unless it's obviously fraudulent).

The credit union can also rely on nondocumentary methods of verifying the identity of its members/customers. Nondocumentary methods can be things like independently verifying the member's identity by comparing information provided by the member/customer with information obtained from a consumer reporting agency, public database, or other source, checking references with other financial institutions, or obtaining a financial statement.

Nondocumentary methods enable a credit union to form a reasonable belief that it knows the true identity of the member/customer by relying on something other than an unexpired government-issued identification. These terms can be tricky because nondocumentary methods can include things that would typically be called documents, like a financial statement. Just keep in mind that as a general rule for individuals, a documentary method of verification is relying on government-issued documents (like a driver's license or passport) while a nondocumentary method is relying on something that is not a government-issued document.

Checking Government Lists

Credit unions must have procedures in place for determining whether a member/customer appears on any list of known or suspected terrorists or terrorist organizations.

Record Retention

Credit unions are required to make and maintain a record of all the information they receive from their member. This includes the name, address, date of birth, and identification number. These records must be retained for five years after the date the account is closed.

A credit union's records must also include a description - not a copy - of any document the credit union relied on. This will be the information it records when verifying a member's identity and it must be kept for five years after the record is made. The credit union must keep:

- A description of any document that was relied on to verify the member's identity;
- Any identification number in the document;
- The place the document was issued; and
- The date of issuance and expiration, if any.

The credit union must also keep a description of the methods and the results of any measures that were taken to verify the member's identity and a description of

the resolution of any substantive discrepancy that was discovered when verifying the information. These records must also be kept for five years after the record is made.

Notice Requirements

A credit union must provide adequate notice to its members that it is requesting information to verify identities. An adequate notice generally describes the identification requirements of the rule and provides notice in a manner designed to make sure that a member views it, or is otherwise given notice, *before* opening an account.

This means that depending on the way the account is opened, the credit union posts the notice in the lobby or on its Web site, include the notice on its account application, or use any other form of written or oral notice. Sample language is provided in the regulation.

Penalties for Noncompliance

Credit unions (as corporate entities) and individuals (classified as “institution-affiliated parties”) can be subject to a wide range of penalties for BSA violations. For example, if a CTR is incomplete or inaccurate a credit union can be fined \$500. If it appears that a credit union has developed a pattern of negligent violations, the credit union can be fined up to \$50,000. If a CTR is not filed as required within 15 days of the completion of a currency transaction exceeding \$10,000, the credit union can be fined \$10,000 per day for each day the report is not filed. In addition, a credit union convicted of money-laundering crimes or willful evasion of currency transaction reporting laws can be put into receivership or conservatorship by the NCUA. State-chartered credit unions may lose their share insurance coverage.

“Institution-affiliated parties” (a term that includes credit union directors, officers, employees, agents, and in some situations, independent contractors like attorneys, appraisers, or accountants) can be suspended if they are charged with a violation of the BSA. They can be permanently removed if the Treasury Department finds that they intentionally violated the regulations or knew that another individual violated the regulations. Beyond suspension or removal, an individual actually convicted of a willful violation is subject to a civil fine in the amount of the transaction, with a minimum fine of \$25,000 and a maximum fine of \$100,000. Finally, individuals convicted of violating the BSA can face criminal penalties up to \$250,000 and/or imprisonment for up to five years, unless the amount of illegal activity involves more than \$100,000 in a 12-month period. In that case, the individual can be subject to a fine of up to \$500,000 and/or 10 years in prison.

The range of penalties for violating BSA requirements can be severe, pointing out why BSA compliance should be a top priority.

Appendix 3-A

IRS Form 4789 and Instructions

(also available at www.fincen.gov/fin104_ctr.pdf)

Multiple Persons

Complete applicable parts below if box 1b on page 1 is checked

Part I Person(s) Involved in Transaction(s)					
Section A--Person(s) on Whose Behalf Transaction(s) Is Conducted					
2 Individual's last name or entity's name			3 First name		4 Middle initial
5 Doing business as (DBA)				6 SSN or EIN 	
7 Address (number, street, and apt. or suite no.)				8 Date of birth _ / _ / _ MM DD YYYY	
9 City	10 State	11 ZIP code	12 Country code (if not U.S.)	13 Occupation, profession, or business	
14 If an individual, describe method used to verify identity: a <input type="checkbox"/> Driver's license/State I.D. b <input type="checkbox"/> Passport c <input type="checkbox"/> Alien registration d <input type="checkbox"/> Other _____ e Issued by: _____ f Number: _____					
Section B--Individual(s) Conducting Transaction(s) (if other than above).					
15 Individual's last name			16 First name		17 Middle initial
18 Address (number, street, and apt. or suite no.)				19 SSN 	
20 City	21 State	22 ZIP code	23 Country code (if not U.S.)	24 Date of birth _ / _ / _ MM DD YYYY	
25 If an individual, describe method used to verify identity: a <input type="checkbox"/> Driver's license/State I.D. b <input type="checkbox"/> Passport c <input type="checkbox"/> Alien registration d <input type="checkbox"/> Other _____ e Issued by: _____ f Number: _____					

Part I Person(s) Involved in Transaction(s)					
Section A--Person(s) on Whose Behalf Transaction(s) Is Conducted					
2 Individual's last name or entity's name			3 First name		4 Middle initial
5 Doing business as (DBA)				6 SSN or EIN 	
7 Address (number, street, and apt. or suite no.)				8 Date of birth _ / _ / _ MM DD YYYY	
9 City	10 State	11 ZIP code	12 Country code (if not U.S.)	13 Occupation, profession, or business	
14 If an individual, describe method used to verify identity: a <input type="checkbox"/> Driver's license/State I.D. b <input type="checkbox"/> Passport c <input type="checkbox"/> Alien registration d <input type="checkbox"/> Other _____ e Issued by: _____ f Number: _____					
Section B--Individual(s) Conducting Transaction(s) (if other than above).					
15 Individual's last name			16 First name		17 Middle initial
18 Address (number, street, and apt. or suite no.)				19 SSN 	
20 City	21 State	22 ZIP code	23 Country code (if not U.S.)	24 Date of birth _ / _ / _ MM DD YYYY	
25 If an individual, describe method used to verify identity: a <input type="checkbox"/> Driver's license/State I.D. b <input type="checkbox"/> Passport c <input type="checkbox"/> Alien registration d <input type="checkbox"/> Other _____ e Issued by: _____ f Number: _____					

Suspicious Transactions

This Currency Transaction Report (CTR) should NOT be filed for suspicious transactions involving \$10,000 or less in currency OR to note that a transaction of more than \$10,000 is suspicious. Any suspicious or unusual activity should be reported by a financial institution in the manner prescribed by its appropriate federal regulator or BSA examiner. (See the instructions for Item 37.) If a transaction is suspicious and in excess of \$10,000 in currency, then both a CTR and the appropriate Suspicious Activity Report form must be filed.

Should the suspicious activity require immediate attention, financial institutions should telephone 1-800-800-CTRS. An Internal Revenue Service (IRS) employee will direct the call to the local office of the IRS Criminal Investigation Division (CI). This toll-free number is operational Monday through Friday, from approximately 9:00 am to 6:00 pm Eastern Standard Time. If an emergency, consult directory assistance for the local IRS CID Office.

General Instructions

Who Must File. Each financial institution (other than a casino, which instead must file FinCEN Form 103, and the U.S. Postal Service for which there are separate rules) must file FinCEN Form 104 (formerly 4789) (CTR) for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency of more than \$10,000. Multiple transactions must be treated as a single transaction if the financial institution has knowledge that (1) they are by or on behalf of the same person, and (2) they result in either currency received (Cash In) or currency disbursed (Cash Out) by the financial institution totaling more than \$10,000 during any one business day. For a bank, a business day is the day on which transactions are routinely posted to customers' accounts, as normally communicated to depository customers. For all other financial institutions, a business day is a calendar day.

Generally, financial institutions are defined as banks, other types of depository institutions, brokers or dealers in securities, money transmitters, currency exchangers, check cashers, and issuers and sellers of money orders and traveler's checks. Should you have questions, see the definitions in 31 CFR Part 103.

When and Where To File. File this CTR by the 15th calendar day after the day of the transaction with the:

IRS Detroit Computing Center
ATTN: CTR
P.O. Box 33604
Detroit, MI 48232-5604

Keep a copy of each CTR for five years from the date filed.

A financial institution may apply to file the CTRs magnetically. To obtain an application to file magnetically, write to the:

IRS Detroit Computing Center
ATTN: CTR Magnetic Media Coordinator
P.O. Box 33604
Detroit, MI 48232-5604

Identification Requirements. All individuals (except employees of armored car services) conducting a reportable transaction(s) for themselves or for another person, must be identified by means of an official document(s). Acceptable forms of identification include a driver's license, military and military/dependent identification cards, passport, state issued identification card, cedular card (foreign), non-resident alien identification cards, or any other identification document

or documents, which contain name and preferably address and a photograph and are normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers.

Acceptable identification information obtained previously and maintained in the financial institution's records may be used. For example, if documents verifying an individual's identity were examined and recorded on a signature card when an account was opened, the financial institution may rely on that information. In completing the CTR, the financial institution must indicate on the form the method, type, and number of the identification. Statements such as "known customer" or "signature card on file" are not sufficient for form completion.

Penalties. Civil and criminal penalties are provided for failure to file a CTR or to supply information or for filing a false or fraudulent CTR. See 31 U.S.C. 5321, 5322 and 5324.

For purposes of this CTR, the terms below have the following meanings:

Currency. The coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money.

Person. An individual, corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture or other unincorporated organization or group.

Organization. Entity other than an individual.

Transaction in Currency. The physical transfer of currency from one person to another. This does not include a transfer of funds by means of bank check, bank draft, wire transfer or other written order that does not involve the physical transfer of currency.

Negotiable Instruments. All checks and drafts (including business, personal, bank, cashier's and third-party), money orders, and promissory notes. For purposes of this CTR, all traveler's checks shall also be considered negotiable instruments whether or not they are in bearer form.

Foreign exchange rates. If completing items 26a/27a, use the exchange rate in effect for the business day of the transaction. The source of the exchange rate that is used will be determined by the reporting institution.

Specific Instructions

Because of the limited space on the front and back of the CTR, it may be necessary to submit additional information on attached sheets. Submit this additional information on plain paper attached to the CTR. Be sure to put the individual's or entity's name and identifying number (items 2, 3, 4, and 6 of the CTR) on any additional sheets so that if it becomes separated, it may be associated with the CTR.

Item 1a. Amends Prior Report. If this CTR is being filed because it amends a report filed previously, check Item 1a. Staple a copy of the original CTR to the amended one, complete Part III fully and only those other entries which are being amended.

Item 1b. Multiple Persons. If this transaction is being conducted by more than one person or on behalf of more than one person, check Item 1b. Enter information in Part I for one of the persons and provide information on any other persons on the back of the CTR.

Item 1c. Multiple Transactions. If the financial institution has knowledge that there are multiple transactions, check Item 1c.

PART I - Person(s) Involved in Transaction(s)

Section A must be completed. If an individual conducts a transaction on his own behalf, complete Section A and leave Section "B" BLANK. If an individual conducts a transaction on his own behalf and on behalf of another person(s), complete Section "A" for each person and leave Section "B" BLANK. If an individual conducts a transaction on behalf of another person(s), complete Section "B" for the individual conducting the transaction, and complete Section "A" for each person on whose behalf the transaction is conducted of whom the financial institution has knowledge.

Section A. Person(s) on Whose Behalf Transaction(s) Is Conducted. See instructions above.

Items 2, 3, and 4. Individual/Organization Name. If the person on whose behalf the transaction(s) is conducted is an individual, put his/her last name in Item 2, first name in Item 3, and middle initial in Item 4. If there is no middle initial, leave item 4 BLANK. If the transaction is conducted on behalf of an entity, put its name in Item 2 and leave Items 3 and 4 BLANK.

Item 5. Doing Business As (DBA). If the financial institution has knowledge of a separate "doing business as" name, enter it in Item 5. For example, Smith Enterprise DBA MJ's Pizza.

Item 6. SSN/ITIN or EIN. Enter the Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) or Employer Identification Number (EIN) of the person or entity identified in Item 2. If none, write NONE.

Items 7, 9, 10, 11, and 12. Address. Enter the permanent address including ZIP Code of the person identified in Item 2. Use the U.S. Postal Service's two letter state abbreviation code. A P.O. Box should not be used by itself, and may only be used if there is no street address. If a P.O. Box is used, the name of the apartment or suite number, road or route number where the person resides must also be provided. If the address is outside the U.S., provide the street address, city, province or state, postal code (if known), and the two letter country code. For country code list go to www.fincen.gov/reg_bsaforms.html or telephone 1-800-949-2732 and select option number 5. If U.S., leave item 12 blank.

Item 8. Date of Birth. Enter the date of birth. Eight numerals must be inserted for each date. The first two will reflect the month, the second two the day, and the last four the year. A zero (0) should precede any single digit number. For example, if an individual's birth date is April 3 1948, Item 8 should read 04 03 1948.

Item 13. Occupation, Profession, or Business. Identify the occupation, profession, or business of the person on whose behalf the transaction was conducted. For example: secretary, shoe salesman, carpenter, attorney, housewife, restaurant, liquor store, etc. Do not use non-specific terms such as merchant, self-employed, businessman, etc.

Item 14. If an Individual, Describe Method Used To Verify Identity. If an individual conducts the transaction(s) on his/her own behalf, his/her identity must be verified by examination of an acceptable document (see **General Instructions**). For example, check box a if a driver's license is used to verify an individual's identity, and enter the state that issued the license and the number in items e and f. If the transaction is conducted by an individual on behalf of another individual not present or on behalf of an entity, enter N/A in Item 14.

Section B. Individual(s) Conducting Transaction(s) (if other than above). Financial institutions should enter as much information as is available.

However, there may be instances in which Items 15-25 may be left BLANK or incomplete. If Items 15-25 are left BLANK or incomplete, check one or more of the boxes provided to indicate the reasons.

Example: If there are multiple transactions that, if only when aggregated, the financial institution has knowledge the transactions exceed the reporting threshold, and therefore, did not identify the transactor(s), check box d for Multiple Transactions.

Items 15, 16, and 17. Individual's Name. Complete these items if an individual conducts a transaction(s) on behalf of another person. For example, if John Doe, an employee of XYZ Grocery Store, makes a deposit to the store's account, XYZ Grocery Store should be identified in Section A and John Doe should be identified in section B.

Items 18, 20, 21, 22, and 23. Address. Enter the permanent street address including ZIP Code of the individual. (See the instructions for Items 7 and 9 through 12.) Enter country code if not U.S. (Reference item 12).

Item 19. SSN/ITIN. If the individual has a Social Security Number, or Individual Taxpayer Identification Number, enter it in Item 19. If the individual does not have an SSN/ITIN, enter NONE.

Item 24. Date of Birth. Enter the individual's date of birth. (See the instructions for Item 8.)

Item 25. If an Individual, Describe Method Used To Verify Identity. Enter the method used to identify the individual's identity. (See **General Instructions** and the instructions for Item 14.)

PART II - Amount and Type of Transaction(s)

Complete Part II to identify the type of transaction(s) and the amount(s) involved.

Items 26 and 27. Total Cash In/Total Cash Out. In the spaces provided, enter the total amount of currency received (Total Cash In) or total currency disbursed (Total Cash Out) by the financial institution. If foreign currency is exchanged, use the U.S. dollar equivalent on the day of the transaction (See "Foreign exchange rates"), and complete item 26a or 27a, whichever is appropriate.

If less than a full dollar amount is involved, increase that figure to the next highest dollar. For example, if the currency totals \$20,000.05, show the total as \$20,001.00.

Items 26a and 27a. Foreign cash in/Foreign cash out. If foreign currency is exchanged, enter the amount of foreign currency in items 26a and 27a. Report country of origin in item 29.

Item 28. Date of Transaction. Insert eight numerals for each date. (See instructions for Item 8.)

Item 29. Foreign Country. If items 26a and/or 27a are completed indicating that foreign currency is involved, check Item 29 and identify the country. If multiple foreign currencies are involved, check box 36 and identify the additional country(s) and/or currency(s) involved.

Determining Whether Transactions Meet the Reporting Threshold.

Only cash transactions that, if alone or when aggregated, exceed \$10,000 should be reported on the CTR. Transactions shall not be offset against one another.

If there are both Cash In and Cash Out transactions that are reportable, the amounts should be considered separately and not aggregated. However, they may be reported on a single CTR.

If there is a currency exchange, it should be aggregated separately with each of the Cash In and Cash Out totals.

Example 1: A person deposits \$11,000 in currency to his savings account and withdraws \$3,000 in currency from his checking account. The CTR should be completed as follows:

Cash In \$11,000 and no entry for Cash Out. This is because the \$3,000 transaction does not meet the reporting threshold.

Example 2: A person deposits \$11,000 in currency to his savings account and withdraws \$12,000 in currency from his checking account. The CTR should be completed as follows:

Cash In \$11,000, Cash Out \$12,000. This is because there are two reportable transactions. However, one CTR may be filed to reflect both.

Example 3: A person deposits \$6,000 in currency to his savings account and withdraws \$4,000 in currency from his checking account. Further, he presents \$5,000 in currency to be exchanged for the equivalent in French Francs. The CTR should be completed as follows:

Cash In \$11,000 and no entry for Cash Out. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash In and Cash Out amounts. The result is a reportable \$11,000 Cash In transaction. The total Cash Out amount is \$9,000, which does not meet the reporting threshold. Therefore, it is not entered on the CTR.

Example 4: A person deposits \$6,000 in currency to his savings account and withdraws \$7,000 in currency from his checking account. Further, he presents \$5,000 in currency to be exchanged for the equivalent in French francs. The CTR should be completed as follows:

Cash In \$11,000, Cash Out \$12,000. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash In and Cash Out amounts. In this example, each of the Cash In and Cash Out totals exceed \$10,000 and must be reflected on the CTR.

Items 30-33. Check the appropriate item(s) to identify the following type of transaction(s):

- 30. Wire Transfer(s)
- 31. Negotiable Instrument(s) Purchased
- 32. Negotiable Instrument(s) Cashed
- 33. Currency Exchange(s)

Item 34. Deposits/Withdrawals. Check this item to identify deposits to or withdrawals from accounts, e.g. demand deposit accounts, savings accounts, time deposits, mutual fund accounts, or any other account held at the financial institution. Enter the account number(s) in item 35.

Item 35. Account Numbers Affected (if any). Enter the account numbers of any accounts affected by the transactions that are maintained at the financial institution conducting the transaction(s). If necessary, use additional sheets of paper to indicate all of the affected accounts.

Example 1: If a person cashes a check drawn on an account held at the financial institution, the CTR should be completed as follows:

Indicate negotiable instrument(s) cashed and provide the account number of the check.

If the transaction does not affect an account, make no entry.

Example 2: A person cashes a check drawn on another financial institution. In this instance, negotiable instrument(s) cashed would be indicated, but no account at the financial institution has been affected. Therefore, Item 35 should be left BLANK.

Item 36. Other (specify). If a transaction is not identified in Items 30-34, check Item 36 and provide an additional description. For example, a person presents a check to purchase "foreign currency." Also list multiple foreign currencies from item 29.

PART III - Financial Institution Where Transaction(s) Take Place

Item 37. Name of Financial Institution and Identity of Regulator or BSA Examiner. Enter the financial institution's full legal name and identify the regulator or BSA examiner, using the following codes:

Regulator or BSA Examiner	CODE
Comptroller of the Currency (OCC).....	1
Federal Deposit Insurance Corporation (FDIC).....	2
Federal Reserve System (FRS).....	3
Office of Thrift Supervision (OTS).....	4
National Credit Union Administration (NCUA).....	5
Securities and Exchange Commission (SEC).....	6
Internal Revenue Service (IRS).....	7
U.S. Postal Service (USPS).....	8
Commodity Futures Trading Commission (CFTC).....	9
State Regulator.....	10

Items 38, 40, 41, and 42. Address. Enter the street address, city, state, and ZIP Code of the financial institution where the transaction occurred. If there are multiple transactions, provide information of the office or branch where any one of the transactions has occurred.

Item 39. EIN or SSN. Enter the financial institution's EIN. If the financial institution does not have an EIN, enter the SSN of the financial institution's principal owner.

Item 43. Routing (MICR) Number. If a depository institution, enter the routing (Magnetic Ink Character Recognition (MICR)) number.

SIGNATURE

Items 44 and 45. Title and signature of Approving Official. The official who reviews and approves the CTR must indicate his/her title and sign the CTR.

Item 46. Date of Signature. The approving official must enter the date the CTR is signed. (See the instructions for Item 8.)

Item 47. Preparer's Name. Type or print the full name of the individual preparing the CTR. The preparer and the approving official may not necessarily be the same individual.

Items 48 and 49. Contact Person/Telephone Number. Type or print the name and telephone number of an individual to contact concerning questions about the CTR.

Paperwork Reduction Act Notice. The requested information is useful in criminal, tax, and regulatory investigations and proceedings. Financial institutions are required to provide the information under 31 U.S.C. 5313 and 31 CFR Part 103, commonly referred to as the Bank Secrecy Act (BSA). The BSA is administered by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). You are not required to provide the requested information unless a form displays a valid OMB control number.

The time needed to complete this form will vary depending on individual circumstances. The estimated average time is 19 minutes. If you have comments concerning the accuracy of this time estimate or suggestions for making this form simpler, you may write to the **Financial Crimes Enforcement Network, P. O. Box 39, Vienna, VA 22183. Do not send this form to this office. Instead, see When and Where to File in the instructions.**

Appendix 3-B

Suspicious Activity Report and Instructions

(also available at www.fincen.gov/reg_bsaforms.html)

<h1 style="margin: 0;">Suspicious Activity Report</h1> <p style="margin: 0;">July 2003 Previous editions will not be accepted after December 31, 2003</p>		<div style="border: 1px solid black; background-color: black; color: white; padding: 2px; text-align: center; width: 20px; margin: 0 auto;">1</div> <p style="margin: 0;">FRB: FR 2230 OMB No. 7100-0212 FDIC: 6710/06 OMB No. 3064-0077 OCC: 8010-9,8010-1 OMB No. 1557-0180 OTS: 1601 OMB No. 1550-0003 NCUA: 2362 OMB No. 3133-0094 TREASURY: TD F 90-22.47 OMB No. 1506-0001</p>
ALWAYS COMPLETE ENTIRE REPORT (see instructions)		
<p>1 Check box below only if correcting a prior report. <input type="checkbox"/> Corrects Prior Report (see instruction #3 under "How to Make a Report")</p>		
Part I Reporting Financial Institution Information		
2 Name of Financial Institution		3 EIN
4 Address of Financial Institution		5 Primary Federal Regulator
6 City	7 State	8 Zip Code
		a <input type="checkbox"/> Federal Reserve d <input type="checkbox"/> OCC b <input type="checkbox"/> FDIC e <input type="checkbox"/> OTS c <input type="checkbox"/> NCUA
9 Address of Branch Office(s) where activity occurred <input type="checkbox"/> Multiple Branches (include information in narrative, Part V)		
10 City	11 State	12 Zip Code
		13 If institution closed, date closed
		MM / DD / YYYY
14 Account number(s) affected, if any		
a _____	Closed? <input type="checkbox"/> Yes <input type="checkbox"/> No	c _____
b _____	Closed? <input type="checkbox"/> Yes <input type="checkbox"/> No	d _____
Part II Suspect Information <input type="checkbox"/> Suspect Information Unavailable		
15 Last Name or Name of Entity		16 First Name
		17 Middle
18 Address		19 SSN, EIN or TIN
20 City	21 State	22 Zip Code
		23 Country
24 Phone Number - Residence (include area code) ()		25 Phone Number - Work (include area code) ()
26 Occupation/Type of Business	27 Date of Birth	28 Admission/Confession?
	MM / DD / YYYY	a <input type="checkbox"/> Yes b <input type="checkbox"/> No
29 Forms of Identification for Suspect:		
a <input type="checkbox"/> Driver's License/State ID	b <input type="checkbox"/> Passport	c <input type="checkbox"/> Alien Registration
Number _____		d <input type="checkbox"/> Other _____
Issuing Authority _____		
30 Relationship to Financial Institution:		
a <input type="checkbox"/> Accountant	d <input type="checkbox"/> Attorney	g <input type="checkbox"/> Customer
b <input type="checkbox"/> Agent	e <input type="checkbox"/> Borrower	h <input type="checkbox"/> Director
c <input type="checkbox"/> Appraiser	f <input type="checkbox"/> Broker	i <input type="checkbox"/> Employee
		j <input type="checkbox"/> Officer
		k <input type="checkbox"/> Shareholder
		l <input type="checkbox"/> Other _____
31 Is the relationship an insider relationship? a <input type="checkbox"/> Yes b <input type="checkbox"/> No		
If Yes specify: c <input type="checkbox"/> Still employed at financial institution e <input type="checkbox"/> Terminated		
d <input type="checkbox"/> Suspended		f <input type="checkbox"/> Resigned
32 Date of Suspension, Termination, Resignation		
MM / DD / YYYY		

Part V Suspicious Activity Information Explanation/Description 3

Explanation/description of known or suspected violation of law or suspicious activity.

This section of the report is **critical**. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood. Provide below a chronological and **complete** account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account. **If necessary, continue the narrative on a duplicate of this page.**

- a **Describe** supporting documentation and retain for 5 years.
- b **Explain** who benefited, financially or otherwise, from the transaction, how much, and how.
- c **Retain** any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.
- d **Retain** any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.
- e **Retain** any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others.

- f **Indicate** where the possible violation took place (e.g., main office, branch, other).
- g **Indicate** whether the possible violation is an isolated incident or relates to other transactions.
- h **Indicate** whether there is any related litigation; if so, specify.
- i **Recommend** any further investigation that might assist law enforcement authorities.
- j **Indicate** whether any information has been excluded from this report; if so, why?
- k If you are correcting a previously filed report, describe the changes that are being made.

For Bank Secrecy Act/Structuring/Money Laundering reports, include the following additional information:

- l **Indicate** whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, letter of credit, domestic or international money order, stocks, bonds, traveler's checks, wire transfers sent or received, cash, etc.).
- m **Indicate** any account number that may be involved or affected.

Tips on SAR Form preparation and filing are available in the SAR Activity Review at www.fincen.gov/pub_reports.html

Paperwork Reduction Act Notice: The purpose of this form is to provide an effective and consistent means for financial institutions to notify appropriate law enforcement agencies of known or suspected criminal conduct or suspicious activities that take place at or were perpetrated against financial institutions. This report is required by law, pursuant to authority contained in the following statutes. Board of Governors of the Federal Reserve System: 12 U.S.C. 324, 334, 611a, 1844(b) and (c), 3105(c) (2) and 3106(a). Federal Deposit Insurance Corporation: 12 U.S.C. 93a, 1818, 1881-84, 3401-22. Office of the Comptroller of the Currency: 12 U.S.C. 93a, 1818, 1881-84, 3401-22. Office of Thrift Supervision: 12 U.S.C. 1463 and 1464. National Credit Union Administration: 12 U.S.C. 1766(a), 1786(q). Financial Crimes Enforcement Network: 31 U.S.C. 5318(g). Information collected on this report is confidential (5 U.S.C. 552(b)(7) and 552a(k)(2), and 31 U.S.C. 5318(g)). The Federal financial institutions' regulatory agencies and the U.S. Departments of Justice and Treasury may use and share the information. Public reporting and recordkeeping burden for this information collection is estimated to average 30 minutes per response, and includes time to gather and maintain data in the required report, review the instructions, and complete the information collection. Send comments regarding this burden estimate, including suggestions for reducing the burden, to the Office of Management and Budget, Paperwork Reduction Project, Washington, DC 20503 and, depending on your primary Federal regulatory agency, to Secretary, Board of Governors of the Federal Reserve System, Washington, DC 20551; or Assistant Executive Secretary, Federal Deposit Insurance Corporation, Washington, DC 20429; or Legislative and Regulatory Analysis Division, Office of the Comptroller of the Currency, Washington, DC 20219; or Office of Thrift Supervision, Enforcement Office, Washington, DC 20552; or National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314; or Office of the Director, Financial Crimes Enforcement Network, Department of the Treasury, 2070 Chain Bridge Road, Vienna, VA 22182. The agencies may not conduct or sponsor, and an organization (or a person) is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

Suspicious Activity Report Instructions
--

Safe Harbor Federal law (31 U.S.C. 5318(g)(3)) provides complete 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 this report's instructions or are filed on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "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".

Notification Prohibited Federal law (31 U.S.C. 5318(g)(2)) requires that a financial institution, and its directors, officers, employees and agents who, voluntarily or by means of a suspicious activity report, report suspected or known criminal violations or suspicious activities may not notify any person involved in the transaction that the transaction has been reported.

<p>In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the financial institution shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities in addition to filing a timely suspicious activity report.</p>
--

WHEN TO MAKE A REPORT:

1. All financial institutions operating in the United States, including insured banks, savings associations, savings association service corporations, credit unions, bank holding companies, nonbank subsidiaries of bank holding companies, Edge and Agreement corporations, and U.S. branches and agencies of foreign banks, are required to make this report following the discovery of:
 - a. **Insider abuse involving any amount.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, and the financial institution has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.
 - b. **Violations aggregating \$5,000 or more where a suspect can be identified.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution and involving or aggregating \$5,000 or more in funds or other assets, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, and the financial institution has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an "alias," then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported.
 - c. **Violations aggregating \$25,000 or more regardless of a potential suspect.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution and involving or aggregating \$25,000 or more in funds or other assets, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.
 - d. **Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.** Any transaction (which for purposes of this subsection means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, 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 financial institution, by whatever means effected) conducted or attempted by, at

or through the financial institution and involving or aggregating \$5,000 or more in funds or other assets, if the financial institution knows, suspects, or has reason to suspect that:

- i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;
- ii. The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or
- iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Bank Secrecy Act requires all financial institutions to file currency transaction reports (CTRs) in accordance with the Department of the Treasury's implementing regulations (31 CFR Part 103). These regulations require a financial institution to file a CTR whenever a currency transaction exceeds \$10,000. If a currency transaction exceeds \$10,000 and is suspicious, the institution must file both a CTR (reporting the currency transaction) and a suspicious activity report (reporting the suspicious or criminal aspects of the transaction). If a currency transaction equals or is below \$10,000 and is suspicious, the institution should only file a suspicious activity report.

2. **Computer Intrusion.** For purposes of this report, "computer intrusion" is defined as gaining access to a computer system of a financial institution to:

- a. Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
- b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
- c. Damage, disable or otherwise affect critical systems of the institution.

For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information.

- 3. A financial institution is required to file a suspicious activity report no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious activity report. If no suspect was identified on the date of detection of the incident requiring the filing, a financial institution may delay filing a suspicious activity report for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.
- 4. This suspicious activity report does not need to be filed for those robberies and burglaries that are reported to local authorities, or (except for savings associations and service corporations) for lost, missing, counterfeit, or stolen securities that are reported pursuant to the requirements of 17 CFR 240.17f-1.

HOW TO MAKE A REPORT:

- 1. Send each completed suspicious activity report to:

Detroit Computing Center, P.O. Box 33980, Detroit, MI 48232-0980

- 2. For items that do not apply or for which information is not available, leave blank.
- 3. If you are correcting a previously filed report, check the box at the top of the report (line 1). Complete the report in its entirety and include the corrected information in the applicable boxes. Then describe the changes that are being made in Part V (Description of Suspicious Activity), line k.
- 4. **Do not include any supporting documentation with the suspicious activity report.** Identify and retain a copy of the suspicious activity report and all original supporting documentation or business record equivalent for five (5) years from the date of the suspicious activity report. All supporting documentation must be made available to appropriate authorities upon request.
- 5. If more space is needed to report additional suspects, attach copies of page 1 to provide the additional information. If more space is needed to report additional branch addresses, include this information in the narrative, Part V.
- 6. Financial institutions are encouraged to provide copies of suspicious activity reports to state and local authorities, where appropriate.

The Bank Secrecy Act

Quiz/Study Guide

1. Which of the following requires a credit union to file a Currency Transaction Report (CTR)?
 - a. Mary comes to your teller window with a check made payable to herself for \$15,000 and deposits that check into her share account.
 - b. Max wants to deposit \$10,000 in cash in his share draft account.
 - c. Jane withdraws \$9,000 in cash in the morning at your main office and \$5,000 in cash at a branch in the afternoon.
 - d. Sue withdraws \$9,000 in cash from her account in the morning and then later that day deposits \$3,000 in cash into her account.

2. When are credit unions required to file a CTR for multiple same-day transactions?

3. What information must be gathered by the credit union when a transaction requires the completion of a CTR?

4. BSA provides seven categories of potential “exempt persons”. Three of these are banks; corporations listed in the New York Stock Exchange, NASDAQ, or the American Stock Exchange; and nonlisted businesses. List the other four categories.

5. From time to time, FinCEN may determine that circumstances warrant additional recordkeeping and reporting requirements under the BSA within a certain geographic area. What is this called?

6. When a credit union sells a cashier’s check, teller’s check, money order, or other similar monetary instrument to a member, what information must be recorded?

7. What four pieces of personal information must be collected from a member opening their first account with the credit union?

8. The credit union is only required to verify the new member's identity to the extent that it forms a "reasonable belief that it knows the true identity of the person.

True False

9. After the person's identity has been verified, are there any other requirements of the CIP rules?

Yes No

10. Posting a notice of the identity verification requirements in the credit union lobby is all the regulation requires.

True False

The Bank Secrecy Act

Answer Key

1. Scenario c. requires filing a CTR. **(Page 3-7)**
2. Multiple same-day transactions made at any of a credit union's offices must be reported on a CTR if they: 1) equal more than \$10,000 either into or out of an account and 2) are made by or for the same person. **(Page 3-7)**
3. The name and address of the person presenting the transaction must be verified and the name, address, account number, and Social Security number or taxpayer identification number of the member on whose behalf the transaction is being made must be gathered. **(Page 3-8)**
4. The other categories are: 1) a department or agency of the U.S., a state, or political subdivision of a state, 2) an entity established under U.S. law or state law, 3) a subsidiary of a company listed on the New York Stock Exchange, NASDAQ, or American Stock Exchange, and 4) payroll customers. **(Page 3-8)**
5. Geographic targeting. **(Page 3-10)**
6. The credit union must keep a record of: 1) the member's name, 2) the date of the purchase, 3) the type of instrument purchased, 4) the dollar amount of the transaction, and 5) the serial number of each instrument purchased. **(Page 3-15)**
7. The credit union must collect: 1. name, 2. date of birth (for an individual), 3. a residential or business street address, 4. identification number (SSN, EIN, ITIN, passport number or similar). **(Page 3-19)**
8. True **(Page 3-20)**
9. Yes, the name must be checked against government lists. **(Page 3-20)**
10. False, the notice must be placed or given so that members opening accounts through the various methods offered by the credit union see the notice prior to opening the account. **(Page 3-21)**

revision

