Annual BSA Program Training Manual

Summary: 31 CFR 1020.210

The Bank Secrecy Act (BSA) was originally passed by Congress in 1970. The act is intended to safeguard U.S. financial institutions from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. It has been amended several times since then, including provisions in Title III of the USA PATRIOT Act which were passed after September 11, 2001. The purpose of the BSA is to help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of the U.S. or deposited into financial institutions. Another overarching goal is to aid in the investigation of money laundering, tax evasion, international terrorism and other criminal activity. Banks are considered to be the key to deterring this type of criminal activity, since access to the financial system generally starts with a bank transaction.

Banks are expected to recognize this responsibility and to develop practices to identify and respond to possible money laundering and/or anti-laundering activities.

The Bank Secrecy Act ("BSA") calls for a BSA program that encompasses five pillars:

- Written Program with a system of Internal Controls;
- Independent Testing;
- BSA Officer;
- Training; and
- Customer Due Diligence.

Scope: 31 CFR 1010.200

BSA compliance relates to all domestic offices and branches of US financial institutions and US branches of foreign banks.

Board Responsibilities: FFIEC Exam Manual

The Board has oversight of the entire BSA program. Importantly, the Board is responsible for ensuring that senior management, the BSA officer and staff are "capable, qualified and properly motivated" to handle the BSA program, comply with the requirements and manage BSA Risk. This includes providing adequate resources to ensure that these needs are met and that the Board has set a tone within the bank that BSA compliance is both expected and a top priority. The Board is also in charge of directing Senior Management to reinforce the tone set by the board and to ensure that the requirements in the bank's BSA program are carried out by employees.

Therefore, the duties related to BSA are ongoing and should be reviewed at periodic intervals. The Board is to review reports related to testing results and then utilize those reports to identify areas of concern, weaknesses, and places where the program can be improved. The Board should engage in the annual training that all other employees engage

in. Additionally, the Board has the responsibility to review any reports related to updates or issues with the current training program. Finally, the Board should ensure that the internal controls put in place by the written BSA program are effective and meeting the goals of compliance set out by the board.

An active, involved and knowledgeable Board is critical for successful implementation of the BSA/AML/OFAC compliance program. Without a general understanding of the requirements of BSA/AML/OFAC, the Board cannot adequately provide BSA/AML/OFAC oversight; approve BSA/AML/OFAC policies, procedures, and processes; or allocate sufficient BSA/AML/OFAC resources. BSA is now a part of the CAMELS rating system under "Management" and therefore, is part of the overall safety and soundness composite rating. BSA was moved from "Compliance" to signify the increasing importance of this regulation resulting from some large bank infractions in New York City relating to money laundering and other questionable international dealings. A 12 CFR 21.21 (BSA) violation is means for a Cease and Desist Order, and often results in civil money penalties being imposed on the Board.

Risk Based Program

Risk assessments are the best way for an organization to determine risk associated with their products and services. A strong risk assessment approach is crucial for an organization to be certain their daily activities will not expose them to unknown or unaccounted risks. Timing of the risk assessment process is crucial. Risk assessments should be performed prior to implementing a new product or service or making changes to an existing product or service. This ensures that the bank has the ability to evaluate all potential issues and mitigate any concerns prior to implementation.

Risk assessments are the living, breathing documents that ensure appropriate policies are in place, appropriate mitigating controls are in place, and that the bank is able to manage oversight of each area to ensure risk levels remain at a tolerable level for the organization. An organization with a strong risk assessment process will be able to take all the risk assessments completed for the organization and quickly determine the bank's enterprise risk. Enterprise risk is determined by averaging the risk from each assessment across the organization. If risk levels are higher than the desired level, the bank can begin to make the appropriate changes to bring the risk level to an acceptable level.

Process

The risk assessment process involves evaluating the risks that threaten to impact the bank. Basic risk categories may be consistent bank-wide; however, the likelihood and anticipated impact may be unique for each branch and each product and service. Therefore, an effective risk assessment process will give the bank the ability to reveal potential risk and give the bank an opportunity to reduce the probability and/or impact of the identified risk.

Primary Risk Factors

Primary risk factors are universal across organizations and must be considered when formulating an effective risk assessment. Those primary risk factors are: Natural Threats; Human Threats; and Technical Threats.

Potential Threats

When developing a risk assessment process, the bank must determine the potential threats and vulnerability of the bank. Examples of potential threats and vulnerabilities include:

- Types of products/services offered
- Customer base
- Location of bank and branches
- Employee training/knowledge/experience
- System capabilities

- Economy/market conditions

Inherent Risk

Inherent risk is the risk that an activity poses if no controls or other mitigating factors are in place. This is also known as "gross risk" which gives a risk rating without netting out risk mitigation. As with the possibility of an incident occurring, the bank should consider inherent risk based on the possible worst-case scenario. This, of course, means that inherent risk is generally going to be higher due to the lack of controls. It is imperative to do this evaluation because inherent risk is the baseline to determine the strength of controls needed to ensure an occurrence does not take place. After determining the inherent risk of an occurrence, the bank will rate the inherent risk as Low, Moderate, or High.

Mitigating Controls

After evaluating inherent risk, the next step is to look at what mitigating controls are available to lessen the potential threats. Mitigating controls are those processed that help identify, quantify, and mitigate risks that impact that bank. Mitigating controls are measures put in place to lessen potential threats. There are three main mitigating controls to consider:

- Policies
- Systems and Staff
- Bank Oversight

Main Pillars/Components of BSA Program: FFIEC BSA Exam Manual

BSA Officer

The Board must designate a qualified person(s) responsible for overseeing the day-to-day compliance with BSA/AML/OFAC regulations. The Board of Directors must approve a BSA Officer annually. The Bank's BSA Officer must be provided the tools and training to effectively manage the BSA program. The BSA Officer must also possess the authority sufficient to manage the BSA/AML Program pursuant to the bank's risk profile. A common issue with choosing a BSA officer is that Board's sometime choose anyone but the guidance clearly indicates that the designated BSA officer should be experienced and understands all the BSA requirements and regulations. The guidance very clearly states that simply having a BSA officer isn't enough to meet this pillar requirement – they must have the know-how, authority, and importantly, for smaller institutions, the time to complete all these BSA duties. In addition, this is not a position that can simply be moved to a single person and stop there. The BSA officer *must* have documented lines of communication that allows that person to report to the Board of Directors and senior management on a regular and as needed basis.

Written Program

The written program should be revisited and revised annually based on the results of the Bank's BSA/AML/OFAC Risk Assessment. The board is required to ensure that the written program is approved annually and is strong enough to ensure compliance with BSA, mitigate BSA risk and monitor for compliance. This approval must be noted in the board minutes. The written program should be commensurate with the size and complexity of the Bank. The internal controls prescribed in policy and procedures should be based upon the Bank's risk assessment and the size and complexity of the Bank. Those policies and procedures should include compliance reporting and record keeping.

EXAMPLE: The same employee who completes the CTR should not submit the CTR. The CTR should be reviewed and approved by another member of personnel before submission.

EXAMPLE: Accounts designated high risk should not be periodically reviewed by its account officer. Reviews should be conducted by an independent party within the bank who does not have a relationship with the account holder.

Risk Assessments

As the BSA program is required to be risk-based, that necessarily requires a BSA risk assessment. BSA risk assessments must take into account:

- Products and services
- Customers and entities
- Geographies served

Internal Controls

The purpose of the written program is to address both the BSA requirements and how the bank intends to meet those requirements. As noted, the Board of Directors is ultimately responsible for setting the tone for BSA compliance within the bank and by their direction, senior management is in charge of making sure the program is actually implemented. This program is required to be tailored so it should not just be a recitation of the bank requirements. An adequate discussion of written controls within the bank's written program will discuss items tailored to the bank such as which of the banks services/locations/products are at risk for money laundering and how the bank has tailored their program to address those risks.

Internal controls work both ways in that they require that the board and senior management regularly get reports related to the effectiveness of the BSA program – including any issues and mitigating action – as well as allow for the Board and Senior Management to set forth initiatives related to BSA requirements. The internal control portion of the rule overlaps with the BSA officer portion of the rule as the person who is appointed for day-to-day compliance (the BSA officer) is also part of the system of internal controls. Similarly, internal controls also includes pillar items like ensuring employees are trained on BSA requirements and having customer due diligence policies, procedures and processes.

Part of the internal controls is ensuring the BSA program runs smoothly regardless of transitions in directors, bank leadership or the BSA officer. The program must, of course, be up-to-date and accurate and therefore, incorporate all reporting requirements, recordkeeping requirements and changes to any of those rules. Similarly, monitoring is a critically important part of the internal controls portion of this rule. The program should identify things like:

- Required reports and documentation
- Reportable CTR Transactions (and exemptions)
- Reportable suspicious activity
- How the bank supervises employees who are in charge of reportable transactions, exemptions and timely reporting

Finally, the bank needs to ensure, along with supervising responsible employees, that BSA requirements and responsibilities are actually part of documented job descriptions and included in employee evaluations for performance. There are often times questions about what's "required" for BSA and it's worth noting that the internal controls portion of the written program needs to include how the bank will set for a system of dual controls and how the bank will ensure to segregate employee duties so that there's another layer of monitoring and evaluation.

Independent Testing

Comprehensive independent testing must be conducted at least annually. Testing should be risk-based and therefore, tailored to the bank's risk profile. That includes a decision of whether annual testing is enough to ensure an effective BSA program. Findings and management responses should be communicated with the Board in a timely manner. A tracking program should be developed to document follow-up to audit findings and report progress to the Board.

"Independent" doesn't necessarily mean external. Yes, an external audit will meet this requirement but the bank can also use an independent internal audit by having audit report directly to the Board of Directors in lieu of the BSA Officer or senior management. The testing is meant to evaluate the effectiveness of the bank's entire program in addition to the program meeting the compliance requirements of the BSA. Independent testing should include testing of the bank's risk assessment – is the risk assessment actually appropriate so that it sets the correct risk basis for the rest of the BSA program? The independent testing also needs to include a review of the whether the bank is complying with the BSA reporting requirements and, of course, the five year record retention requirements.

The testing should cover all five pillars. This means that the independent test should include a review of whether the BSA training is done and, just as importantly, whether the BSA training is up-to-date and adequate. For example, a review of the 2018 training should include all the guidance and updates related to beneficial ownership before and after implementation.

Testing of the bank's BSA program also needs to include how the bank – namely senior management- responds to any known issues. It also includes a review of the adequacy of the bank's monitoring of suspicious activity. Finally, it should include a review of how accurate and effective the bank's monitoring system is (including model validation of automated systems).

Training

The bank must ensure that all personnel as well as the Board are trained in applicable aspects of BSA. Each and every member of Bank personnel (including the Board) has to receive BSA/AML/OFAC training annually. New employees should receive training prior to on-boarding during an orientation. Training should include regulatory requirements and the Bank's internal BSA/AML policies, procedures, and processes. Training should be specific to each employee's job description which means that BSA training for lending should differ from front line teller which should differ for back-of-house employees, etc. Be aware that the training and testing materials, the dates of training sessions, and attendance records should be maintained by the bank as a record of BSA compliance. Board of Directors and senior management need to be trained on major changes to BSA. Training should be ongoing and include any BSA requirement changes. All training needs to be documented.

Customer Due Diligence: 31 CFR 1020.210(b) (5)

The bank is specifically required to have risk-based procedures for conducting ongoing customer due diligence. This mandates that the bank has to understand the purpose for the customer engaging in a relationship with the bank, conducting ongoing monitoring, report suspicious activity and update the customer's information, as needed. This portion of the rule also requires the collection of beneficial ownership information. Risk considerations should include the products or services, the customer, anticipated and actual account activity, and the geographic area where business is being done.

Beneficial Ownership: 31 CFR 1010.230; 1020.210

On May 11, 2016, FinCEN issued its Final Rule relating to Customer Due Diligence including the specific requirements for identifying and verifying the identity of beneficial owners of legal entity customers. The rule was effective May 11, 2018 and is codified at 31 CFR 1010.230. The beneficial ownership requirements comprise the fifth pillar of BSA. The rule includes definitions and exclusions as to who qualifies as a legal entity customer and the account types that require collection of beneficial owner information. The beneficial owner requirements track with the standard CIP requirements. Additionally, the regulation reiterates that there are core elements for customer due diligence and adds a requirement for risk-based due diligence within the bank's Anti-Money Laundering (AML) program. Those core elements include things like written policies, procedures, risk assessments, training and independent testing.

Coverage

The Beneficial Ownership Rule applies when an account (of any type) is opened by a new or existing "legal entity" customer. While the regulation and rule itself, is very short and simple, the practical applications have been anything but. Thus, it is important to understand every step of determining coverage under the rule including using this six-step process:

Six-Step Test

Step	Question	Citation
Step 1	Is this a new "account" per the CIP definition?	31 CFR 1020.100
Step 2	Who is my customer? (fiduciary accounts, etc. – who signs the contract and not "who does this account benefit?").	31 CFR 1020.100
Step 3	Is the customer a non-natural person? If No, 100% exempt from beneficial ownership requirements	31 CFR 1010.230(e)
Step 4	Is the non-natural person a general partnership or required to register as a business with the Sec. of State or similar agency? If no, 100% exempt from beneficial ownership requirements. If yes, the customer is a legal entity customer, thus the Beneficial Ownership Rule s apply.	31 CFR 1010.230(e)
Step 5	Is the legal entity excluded from the definition of legal entity customer (e.g., is the customer a governmental unit)? If yes, they are 100% exempt from the rule.	31 CFR 1010.230(e)(2)
Step 6	Is the legal entity a nonprofit? If yes, they are exempt from the ownership prong only. If no, comply with all parts of the rule.	31 CFR 1010.230(e)(3)

Accounts:

The Beneficial Ownership Rule differs from CIP in one major away. The difference is that beneficial owner information must be collected every time a legal entity customer opens a new account. Information collection is not based on the legal entity being a new customer. Every time a legal entity opens a new account the beneficial ownership information is needed (with a couple exceptions), even if the entity has banked with the bank for 20 years.

Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act, FAQs - April 28, 2005:

"An "account" is defined in the CIP rule as "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account or other extension of credit." An account also includes "a relationship established to provide a safety deposit box or other safekeeping services or to provide cash management, custodian, or trust services." An account does not include "products and services for which a formal banking relationship is not generally established with a person, such as check cashing, wire transfer, or the sale of a check or money order." For CIP purposes, an account does not include any account that the bank acquires, or accounts opened, to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974."

Requirements

Identify: 31 CFR 1010.230(b)(1)

The rule first requires the bank to identify who the beneficial owners of a legal entity customer are. There are two "prongs" of beneficial ownership, the ownership prong and control prong. Every legal entity customer will need to identify at least one natural person and can identify up to five natural persons. It is up to the bank to set the threshold of ownership if they want to collect information on more owners (for example, all controlling owners or owners with 10% interests) pursuant to the bank's due diligence processes.

Ownership	Control
0 to 4 natural persons	1 person
Natural person who owns at least 25% of the entity – directly or indirectly	Natural person who controls or manages the entity.
Can rely on customer information (unless there is evidence the information is incorrect)	Can rely on customer information (unless there is evidence the information is incorrect)

Ownership

First, the bank needs to figure out if anyone owns at least 25% of the business. For example, for sole member LLC, you're going to have one person who owns 100% of the company and you need to get his/her verification documents. On the other hand, a company that is owned by 10 people, all owing at least 10% of the company, would not have any named beneficial owners under this rule. In addition, the rule looks at both direct and indirect ownership.

Indirect Ownership

A legal entity that is owned by another legal entity will still have to be evaluated to see if any natural person owns enough of the legal entity or entities that own your customer to qualify as a beneficial owner. Any natural person who has at least 25% ownership of the legal entity customer will be identified.

Control

In addition to your owners, you also need one person who has the ability to control or manage the business. For example, a CEO, CFO or COO. It doesn't matter who it is, as long as they can control the company. You can also rely on the information the customer is giving you in regard to this role.

Non-Profits

Non-profit legal entities are only required to collect information related to the control prong. However, many people have been confused about the requirement to collect this information. The non-profit must first be a covered legal entity under the rule. A club or unincorporated association or other group that is not a general partnership nor required to register with the state as a business, is not a legal entity and are fully exempt from the rule. Therefore, no information needs to be taken related to either prong.

Verification: 31 CFR 1010.230(b)(2)

The Beneficial Ownership Rule requires that banks identify who the beneficial owners of a legal entity customer are and then, verify the identity of those owners much like CIP. The bank will collect information that is very similar to CIP information. The minimum requirements are:

- Name and title of the individual
- Name and address of the business or personal address
- Date of birth; and
- Social Security Numbers for US citizens or Social Security Number, Passport Number and Country of Issuance, or other similar identification number for non-citizens

Another big difference from the CIP requirements is that unlike CIP, you can accept copies of verification documents instead of the actual ID. So this means, the person opening the account can come prepared with that information. Just like the ownership information, the bank is allowed to rely on the customer's information, in good faith.

CIP

One of the most important take-aways from the CDD Beneficial Ownership Rule, is that while it is like CIP, it is not CIP. CIP is based on customer relationship and is looking at the customer for information. This means for opening accounts in-person, the bank is doing CIP on the person in front of them or the entity for whom the person is in front of them opening the account for. There is no requirement that the signer of the beneficial ownership certification be a listed beneficial owner. The bank may not ever meet with a listed beneficial owner nor have any contact with that beneficial owner nor is such interaction required.

Model Certification Form: Appendix A

The bank may (but is not required to) rely on the model certification form to meet the requirements of the Final Rule. The model certification form is found in Appendix A to 1010.230. The Certification needs to be filled out by the natural person who has authority to open the account (the "account opener"). The model form requests that all the beneficial owners provide their name, address, date of birth and social security number (or passport number if there is no social security number). The instructions are helpful to the customer (and the bank) as they give a simplified explanation of who is considered a beneficial owner. The account opener will list their name and title and the name and address of the legal entity who is the accountholder. The account opener must certify that all the information provided on the form is accurate to the best of their knowledge, as required by the rule. The certification is needed even if account opener is not considered a "beneficial owner" for this requirement.

Suspicious Activity Report: 31 CFR 1020.321; FFIEC SAR

The purpose of the Bank Secrecy Act is to combat money laundering and the financing of drug trafficking. There are two ways a bank does this: first, by refusing to bank customers who are suspected of or are known to have committed such crimes; and second, by compiling information which is utilized by FinCEN and law enforcement agencies to detect patterns and evidence of illicit activities. The Suspicious Activity Report (SAR) is an important part of FinCEN's ability to assist law enforcement to detect and combat these crimes. After going through due diligence and investigation steps, if the bank determines suspicious activity has occurred the SAR must be filed within certain thresholds. As with the monitoring considerations, when a bank must file a SAR on a suspect, it should also decide whether more action is needed and take steps to:

- Start a law enforcement investigation
- Support existing law enforcement investigations
- Remove/penalize insiders involved in crime

The Suspicious Activity Report is required for criminal violations detected by the bank based on certain thresholds. Filing is required if there is a "reasonable" suspicion that a violation of law has occurred. This is based on a "normal person" standard and therefore, the bank should have set standards. A transaction includes essentially any activity to, though, or by the bank including:

- Deposits
- Withdrawals
- Account Transfers
- Currency Exchanges
- Loans
- Stock purchases
- Certificates of Deposits
- Purchase or Sale of monetary instruments

Confidentiality: 31 CFR 1020.320(e)

One of the most critical requirements in this rule is that SARs must be kept confidential. This is true even if a SAR is not filed - meaning that the bank's decision to *not* file a SAR is also considered confidential under this rule. The bank is required to have internal controls that allow for these items to be kept confidential. The only time the bank can disclose the existence of a SAR is to comply with the BSA requirements. At no point can the suspect involved with the transaction be notified of the SAR detection or filing.

If the bank is subpoenaed or has a legitimate requirement from FinCEN or law enforcement, the bank can provide additional information. Otherwise, the bank cannot provide the SAR itself or disclose that a SAR has been filed. The bank can disclose a SAR to the bank holding company but only as far as needed for the holding company to comply with the SAR requirements.

Board Reporting

The Board must be notified that a SAR has been filed. There is no specific format to complete this requirement. For example, there's no requirement to present the board with full copies of the SAR and supporting documentation. Of course, if there is a board member or BSA committee member that has a SAR filed on them, the bank cannot disclose that to them. Navigating these sorts of issues causes a lot of difficulties and it is best practice to anticipate and mitigate these sorts of issues upfront in the bank's policies and procedures.

Filing Thresholds: 31 CFR 1020.320(a)(2); 31 CFR 1020.320(c)

Activity	Threshold
Known Suspect	$5,000
Money Laundering or Illegal Activity Designed to Evade BSA	$5,000
Unknown Suspect	$25,000
Bank Insider	$0

The aggregate threshold for reporting suspicious activity is $5,000 when the suspect is known, $25,000 where is no suspect and any amount if the suspect is a bank insider. If the suspicious activity requires immediate attention, the bank can and should notify the appropriate law enforcement authority. Additionally, even if the suspicious activity doesn't meet the threshold, the bank can but doesn't have to report it. C/A often gets asked if the bank is allowed to report – for example, where there has been a $10,000 counterfeit check but there is no suspect – the bank can still report it. The safe harbor for reporting SAR information still applies regardless of whether the report is mandatory or voluntary. In addition, it's worth noting that a SAR is not required for a robbery at the bank that has already been reported to the appropriate law enforcement agencies.

Timing: 31 CFR 1020.320(b)(3)

SARs have specific timing requirements and must be filed within 30 calendar days after the initial detection of facts that may constitute a basis for filing a SAR. It's important to note that "initial detection" doesn't mean when the bank's automated system red flags an item or when an employee submits the item for review. The term "initial detection" is based on when the bank determines that the activity is suspicious.

The bank is allowed to delay filing for an additional 30 calendar days if that time is needed to identify a suspect. As noted above, the bank can and should contact law enforcement and their regulator if a suspected violation requires immediate attention.

Continuing SARs:

The bank is required to continuing monitoring individuals, accounts and transactions after a SAR is filed. If there is continuing suspicious activity, the bank must file a continuing SAR after a 90-day review timeframe. The bank has 30

days after that 90-day review for continuing activity to submit the continuing SAR (for a total of 120 days since the last SAR was filed).

Currency Transaction Report: FFIEC Exam Manual: 31 CFR 1010.310

Currency Transaction Reports (CTR) capture aggregated cash transactions of over $10,000 in a single business day. It is one of many BSA records that must be kept by the bank and one of a few that need to be filed with FinCEN. This type of information is utilized as supporting information for FinCEN and, assists the bank in monitoring whether such transactions rise to the level of being "suspicious" and requiring a SAR.

Report Requirements: 31 CFR 1010.312

CTRs are only required where cash in or cash out exceeds $10,000. It's important to note that unlike SARs, there's not an optional threshold. However, if the amount of cash in or out is exactly $10,000 or $9,999 – it might be suspicious. Also, unlike a SAR, the CTR is not confidential. The bank is allowed to explain to a customer that they are collecting their information. However, if they refuse to continue with the transaction because of this, that may be suspicious activity that needs to be recorded on a SAR. When the bank has a transaction over $10,000, identification is required because the bank will need to record specific information for the CTR. The bank must retain a record of the individual's account number and social security number or Tax ID number.

Transactor or Beneficiary

A CTR must be filed when amounts of cash over $10,000 are deposited or withdrawn when it's either done by the same person or done for the same person. This sometimes can be confusing because a non-customer, for example, can come in as a runner for their employer, have a reportable transaction, and then the bank needs to get information about both their employer (beneficiary) and the runner (transactor) because the transaction is over $10,000. It can also be difficult to tell when transactions are for benefit of someone else. Part of this can be resolved by including it in the banks' procedures that tellers need to ask questions about reportable transactions and part of this is based on a good faith interpretation of the transaction.

Aggregation: 31 CFR 1010.313

When determining whether there is a reportable transaction, the bank needs to include deposits or withdrawals included at all branches and any other deposit/withdrawal taking locations. Cash taken or deposited during a single business day (so, including night drop boxes, etc.) count for determining whether there is a reportable transaction/are reportable transactions. A common topic is the difference between aggregation and multiple transactions. Multiple transactions relate to when there is more than one transaction in a day. Aggregated transactions relate to when there are multiple transactions that trigger a CTR but none of those transactions, by themselves, are over $10,000 and therefore, a CTR is required because the amounts added together is over $10,000 in a single business day. Another important note is that the amounts in and amounts out are not used to come up with a total. For example, if someone deposits $15,000 and they withdraw $5,000 and therefore, end up with exactly $10,000, a CTR is still required because the cash in is over $15,000.

Multi-Party Accounts

Joint accounts cause a bit of heart burn because there are different rules depending on whether the transaction is a deposit or a withdrawal. If a transaction of over $10,000 is deposited into a joint account, the bank will have to report the person making the deposit (transactor) but also, the joint owner as a person whom the deposit benefits. On the other hand, if there is a withdrawal over $10,000 from a joint account, unless the bank has reason to know that the

transaction is on behalf of another owner, the CTR will only be filed as being done by the person making the withdrawal for their own benefit.

On business accounts, when different people are making reportable deposits to the same business account, the transactors will be listed as depositing for the benefit of another (the company) and the company will be listed the beneficiary of the transaction. Again, this may require that the bank get information for non-customers or people who are otherwise not involved but it is necessary in order to properly fill out the CTR.

Structured: 31 CFR 1010.314

Structured transactions are transactions were the deposits are broken up into smaller amounts in order to evade CTR identification requirements. This type of activity is considered suspicious and as it will involve amounts over $5,000, the bank needs to file a SAR on structured transactions.

Back-filing: FFIEC Exam Manual

Should the bank miss a transaction or find out that someone they thought was exempt never was, the bank needs to start reporting CTRs going forward. In addition, the guidance specifically dictates that the bank should contact FinCEN directly to determine whether back-filing is necessary.

Exemptions: FFIEC Exam Manual

Some customer transactions over $10,000 are exempt from the requirement to file a SAR. There are two different types of exemptions and also business types that are ineligible for exemption even if a Phase II exemption would otherwise apply.

Phase I Exempt	Phase II Exempt	Ineligible
Financial Institutions	Transaction Account Customers +	Lawyers
Government Entities	2+ Months +	Accountant
Entities That Trade on a Stock Exchange	5 or More Transactions +	Doctors
Subsidiaries of the above Entities	Over $10,000 +	Auctioneers
	Not Ineligible	Boat, Bus, Plane Charters
		Casinos/ Gaming
		Real Estate Broker
		Investment Bankers
		Title Insurance
		Real Estate Closers

		Trade Union

Phase I

Entities that are phase I exempt include:

- Financial Institutions
- Government Entities
- Entities that trade stock exchange and their subsidiaries.

As a note, a subsidiary qualifies if they are owned at least 51% by the exempted entity. A common question is how to tell if an entity meets these requirements and the simple answer is: ask. As part of the bank policy, the bank can require verifying information for this exemption – for example, proof that an entity was set up as a government entity pursuant to federal, state of local law. For companies that trade on the NASDAQ or New York Stock Exchange and/or their subsidiaries the bank can ask for:

- Officer's Certificate
- IRS form 851
- SEC Form 10-k

The bank can also determine if an entity is "publicly traded" by doing simple things like checking the newspaper, looking at a common listing stock guide, stock websites, etc. Phase I exemptions for government entities and financial institutions are automatic and do not require filing a DOEP form (*See*: below)

Phase II

Phase II exemptions are allowed for businesses that have maintained a transaction account at the bank for a least two months and have at least 5 transactions over $10,000 in a year. Of course, if the business type is ineligible for exemption, this Phase II exemption will not apply. In the case of businesses that engage in both eligible and ineligible business, there is a 50% threshold of the eligible business for companies that engage in exempt and nonexempt businesses.

Ineligible for Exemption

There are certain which are ineligible for a Phase II exemption. An ineligible business is defined as a business engaged primarily in one or more of the activities below:

- Serving as a financial institution or as agents for a financial institution of any type.
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- Practicing law, accounting, or medicine.
- Auctioning of goods.
- Chartering or operation of ships, buses, or aircraft.
- Operating a pawn brokerage.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks).
- Engaging in investment advisory services or investment banking services.
- Operating a real estate brokerage.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Engaging in any other activity that may, from time to time, be specified by FinCEN, such as marijuana-related businesses.

Designation of Exempt Person (DOEP)

For Phase II exemptions the bank must file a Designation of Exempt Person Report within 30 days of the exemption. This report only needs to be filed once for each Phase II exemption and each Phase I exempted entity. Again, there is no requirement to file DOEPs for banks or government entities. The bank must still do their due diligence as far as ensuring that these parties are exempt. If a party is no longer exempt, the bank can file a revocation of the DOEP or simply file a CTR for the next reportable transaction.

Ongoing Responsibilities

For each of the exempted entities, an annual review is required. Annual Review: Required once per year - "year" is not defined, but once every 12 months is the conservative approach (versus once per calendar year). Review that the customer makes at least five of the CTR transactions and does not engage in ineligible businesses.

Revocation

If no longer exempt, you can file a revocation of the DOEP or simply file a CTR for the next reportable transaction.

Record Retention

As with other BSA requirements, the record retention requirement is five years. That five-year record retention includes the report and the retention period starts on the date that the report was made.

The amount and account number(s) entered in Item 21 "Cash in amount…" or Item 22 "Cash out amount…" will be the amount and account number(s) associated with the specific locations. The initial Part I section on the entity home office/headquarters will show the total amount and all account numbers involved in Item 21 or 22. When there are multiple DBA names involved in a transaction, Item 8 "Alternate Name" should be left blank in the entity office Part I section. When the entity home office address is the same as the transaction location, only a home office Part I section should be completed.

Information Sharing Between Law Enforcement and Financial Institutions (Section 314(a))

In 2002, final regulations (31 CRR 103.100) and 31CFR 103.110) which implement section 314 of the USA Patriot Act became effective. The regulations established procedures which allowed for information sharing in an effort to deter money laundering and terrorist activity. In 2010, the regulations were amended by FinCEN allowing state, local, and certain foreign law enforcement agencies access to the information sharing program.

A federal, state, local, or foreign law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions. In soliciting this information from FinCEN, the law enforcement agencies must provide a written certification attesting that there is credible evidence of involvement or reasonably suspected involvement in terrorist activity or money laundering for each individual, entity, or organization in which they are seeking information. Law enforcement agencies must also provide FinCEN with information such date of birth and address so financial institutions can differentiate between similar names and their customers. Once FinCEN receives this information, a request for information will be sent to financial institutions. FinCEN then makes suspect information available to the financial services community by posting it every two weeks to its secure website.

Search Requirements

FinCEN will send information requests to financial institutions every two weeks, or more frequently if an emergency request is transmitted. These requests will be sent to a designated point of contact(s). Financial institution are then expected to conduct a one-time search of their records to identify any accounts or transactions of a named suspect. Unless otherwise instructed, financial institutions must search their records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. Financial institutions must search their records and report any positive matches to FinCEN within 14 days.

If the financial institution identifies a match, they must be reported the match to FinCEN. No additional information should be provided. If no match is identified, the financial institution has no further obligations other than to maintain documentation of receiving and searching their records.

You **must do** a one-time search of the following records:

- Deposit account records to determine if a named subject is or was (within the last 12 months) an account holder;
- Loan records to determine whether a named subject is or was (within the last 12 months) a borrower;
- Safe deposit box records to determine whether a named subject maintains or maintained (within the last 12 months) or has had authorized access to, a safe deposit box. You are obligated to search safe deposit records, however, ONLY if the records are searchable electronically;
- Trust department records for current accounts and accounts closed within the last 12 months to determine whether a named subject matches the name in which an account is titled;
- Records of accounts to purchase, sell, lend, hold, or maintain custody of securities to determine whether a named subject is or was (within the last 12 months) an account holder;
- Records of commodity futures, options, or other derivatives accounts to determine if a named subject is or was (within the last 12 months) an account holder;
- Funds transfer records maintained pursuant to the Bank Secrecy Act (for the past 6 months) to determine whether a named subject was an originator/transmitter of funds for outgoing funds transfers, or a beneficiary/recipient of a funds transfer for incoming transfers; and
- Records of the sale of monetary instruments maintained pursuant to the Bank Secrecy Act (for the last 6 months) to determine whether a named subject purchased a monetary instrument.

You **are not required** to search any other record, including the following:

- Checks processed to determine whether a named subject was a payee on a check;
- Monetary instruments issued by the Bank to determine if the named subject was a payee on the instrument;
- Signature cards to determine if a named subject is a signer on an account; and
- Reports filed (such as CTRs and SARs) that you previously filed with FinCEN.

Confidentiality

A financial institution may not disclose to any person, other than to FinCEN, their primary regulator, or the law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information. One thing to note regarding the confidentiality of these requests is that financial institutions are permitted to provide the 314(a) subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the necessary steps are taken through the use of an agreement or procedures, to ensure that the third-party safeguards and maintains the confidentiality of the information.

Financial institutions are strongly discouraged from using the 314(a) subject list as the sole basis for establishing or maintain an account. One thing to keep in mind with the 314(a) subject lists is that unlike the OFAC lists, these lists are not permanent "watch list". In fact, these lists are generally related to a one-time inquiry and the names do not correspond to convicted or indicted individuals. The lists are not updated or corrected if an investigation is corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. FinCEN also advises that inclusion on a section 314(a) subject list should not be the sole factor used for determining whether to file a SAR. Financial institutions should follow their normal SAR procedures in making such a determination.

Documentation

Banks must maintain documentation that all required searches were performed. This documentation may be printed or stored on a search self-verification document from the Web-based 314(a) SISS for each 314(a) subject list transmission. If the bank prints and maintains copies, the information should be appropriately secured and protected to maintain confidentiality.

Examples of documentation:

- Copies of section 314(a) requests.
- A log that records the tracking numbers and includes a sign-off column.
- Copies of SISS-generated search self-verification documents.
- If appropriate, request documentation from FinCEN regarding the bank's history of accessing the SISS.
- For positive matches, copies of the form returned to FinCEN (e.g., SISS-generated Subject Response Lists) and the supporting documentation should be retained.

Ensuring Compliance

The bank's policies and procedures should address 314(a) requests. This includes ensuring that there are internal controls and procedures in place for receiving, searching, and documenting the bank's compliance with the requests. At a minimum, the bank's procedures should:

- Designate a point of contact for receiving information requests;
- Ensure that the confidentiality of requested information is safeguarded;
- Establish a process for responding to FinCEN's requests; and
- Establish a process for determining if and when a SAR should be filed.

Voluntary Information Sharing - 314(b) of the USA Patriot Act

Section 314(b) of the USA Patriot Act, providing specific protections from liability, encourages financial institutions and associations of financial institutions located within the United States to share information in an effort to identify and report activities which may involve terrorist activity or money laundering. Sharing information for these purposes is voluntary and requirements must be met in order to do so.

Requirements

Financial institutions must make a determination whether to participate in voluntary information sharing. If the bank elects not to participate, no action is required. That being noted, the bank may not share information with other financial institutions or associations of financial institutions who have elected to share.

If the financial elects to voluntarily share information, they must file a notification form with FinCEN, providing an effective date for the sharing of information. The notice to share information is only effective for one year therefore, notification must be updated annually. A financial institution must also take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to FinCEN. FinCEN provides participating financial institutions with access to a list of other participating financial institutions and their related contact information. The bank should also establish a process for sending and receiving information sharing requests.

Safe Harbor

For a financial institution to be afforded safe harbor from liability, they must notify FinCEN of their intent to engage in information sharing and have established procedures in place to protect the security and confidentiality of the information. Failure to comply with the these requirements may result in the loss of safe harbor protections and a violation of privacy laws or other laws and regulations. Safe harbor will not extend to sharing of information across international borders as 314(b) only applies to financial institutions located within the United States.

Confidentiality

If a financial institution receives information from another financial institution or associations of financial institutions, they should limit use of the information and maintain its security and confidentiality. Information received from other financial institutions or associations of financial institutions should only be used to identify and, where appropriate, report on money laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA compliance. Financial institutions should develop procedures to ensure confidentiality similar to those established for complying with section 501 of the Gramm–Leach–Bliley Act (15 USC 6801) which provide protection of its customers' nonpublic personal information.

Section 314(b) does not authorize financial institutions to share a SAR, nor does it allow financial institutions to disclose the existence or nonexistence of a SAR. If a financial institution shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying transaction and customer information. A financial institution may use information such information to determine whether to file a SAR, but the intention to prepare or file a SAR cannot be shared with other financial institutions. Financial institutions should establish a process for determining when and if a SAR should be filed and they should follow their normal SAR procedures in making such a determination.

Documents

The bank should file a notification form with FinCEN which provides an effective date for the sharing of information that is within the previous 12 months and should maintain documentation of this notification. A financial institution should also maintain documentation of the information shared and received.

Ensuring Compliance

The bank's policies and procedures should address the sharing and receiving of information under 314(b) of the USA PATRIOT Act. This includes ensuring that there are internal controls and procedures in place for sharing information and receiving information. At a minimum, the bank's procedures should:

- Designate a point of contact for receiving and providing information.
- Ensure the safeguarding and confidentiality of information received and information requested.
- Establish a process for sending and responding to requests, including ensuring that other parties with whom the financial institution intends to share information (including affiliates) have filed the proper notice.
- Establish procedures for determining whether and when a SAR should be filed.

Annual BSA Program Training FAQ – Questions

Question 1: What are the steps to take as the bank prepares for a BSA/AML risk assessment?

_____
_____
_____
_____
_____

Question 2: If a customer is at the teller line making a withdrawal that triggers a CTR and they are accompanied by a family member not on the account, should that family member be listed as a transactor or benefactor on the CTR?

_____
_____
_____
_____
_____

Question 3: If we are filing a SAR on a customer who has a joint account and has been putting money into that joint account, do we need to include the joint owner on the SAR? The joint owner has never been present when the suspicious activity has taken place.

_____
_____
_____
_____
_____

Question 4: Are estate accounts included in the Beneficial Ownership rule?

_____
_____
_____
_____
_____

Question 5: We are working on our BSA Customer Base Risk Assessment. We are listing a customer with his name DBA "this" restaurant. Do I need to list his personal accounts or just his business account that I feel is high risk.

BSA Program Overview FAQ - Answers

ANSWER 1:

The bank's general risk management principles used enterprise-wide should be applied when assessing and managing BSA/AML risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. There are many effective methods and formats used in completing a BSA/AML risk assessment, but in general the process should include a planning and conducting risk assessment phase.

The planning phase will be key to ensure the bank's overall risk management practices align with the BSA/AML strategy. A risk centric planning process combines the fundamental elements of strategic planning and enterprise risk management programs to truly sync the bank's objectives and strategic plans. This will allow the bank to leverage its already established risk principles, side-step any potential problems and allow the bank to continue on its successfully course.

During the conducting the risk assessment phase, the bank will assess those risk established during the planning phase. Typically, a bank will assess the following:

- Impact
- Likelihood
- Mitigation

It's important to implement a consistent rating system, such as a low, moderate, high scale or possibly assigning a numeric value (i.e.- 1-3) to each. Whichever assessment rating system the bank utilizes ensure it aligns with the bank's overall risk rating strategy, if possible.

ANSWER 2:

This isn't really addressed in the regulation or guidance. While not directly on point, if the Bank has knowledge that the transaction was being conducted on behalf of the family member, based on the below FAQ there may be an argument that the Bank would list the family member's information. However, because this is FAQ is addressing withdrawals from a joint account there is an argument that the FAQ does not apply to when it is just a family member present at the Bank with the customer.

Reference:
https://www.fincen.gov/frequently-asked-questions-regarding-fincen-currency-transaction-report-ctr

24. How do I properly complete Part I on the FinCEN CTR for withdrawals from a joint account? What amounts do we show in Item 22 for each Part I? For example, John and Jane Smith have a joint account together. During one business day, John Smith withdrew $12,000 from the account.

Since John Smith made a withdrawal from the joint account in excess of $10,000, then the financial institution would list Jane Smith's information only if it has knowledge that the transaction was also being conducted on her behalf. If the financial institution does not have knowledge that the withdrawal was conducted on behalf of Jane Smith, then it would neither be required to nor prohibited from listing Jane Smith in a second Part I.

Therefore, if the financial institution does not have knowledge that the withdrawal was conducted on behalf of Jane Smith, the financial institution would complete a Part I on John Smith. For Item 2 of Part I, the financial institution would

check 2a "Person conducting transaction on own behalf" and complete the applicable information for John Smith. Item 22 for Part I on John Smith would be completed by entering $12,000 and providing the account number affected.

However, if the financial institution does have knowledge the withdrawal was completed on behalf of both John Smith and Jane Smith, the financial institution must complete two Part Is. In completing a Part I on John Smith, the financial institution would check 2a "Person conducting transaction on own behalf" and complete the applicable information for John Smith. In completing a Part I on Jane Smith, the financial institution would check 2c "Person on whose behalf transaction was conducted" and complete the applicable information for Jane Smith. Item 22 for each Part I would be completed similarly by entering $12,000 and providing the account number affected."

ANSWER 3:

As the joint owner is not the transactor nor does the bank have information that the transactions are on behalf of the joint owner, there is no need to specifically list them on the SAR as a subject. This is because Part I requires the bank to list persons who are involved in the suspicious activity. This being said, the bank is allowed to list both owners.

ANSWER 4:

They are not. This is because they are not legal entities. Thus, an estate account would not need beneficial ownership information collected on it.

Reference:
https://www.fdic.gov/regulations/laws/rules/8000-1400.html#fdic8000fra1010.230

31 CFR § 1010.230A(e)(1):
"(e) Legal entity customer. For the purposes of this section:
(1) Legal entity customer means a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account."

ANSWER 5:

Typically, you would do the restaurant account. Here, while It's not specifically provided for in the BSA guidance, I can see the argument for including all of his accounts since the restaurant is operated as a sole prop and is not its own legal entity and thus a separate customer.