

Bank Secrecy Act/ Anti-Money Laundering Ledger

1st QTR 2005

FEDERAL RESERVE BANK
OF CHICAGO

THE EVOLUTION OF THE BANK SECRECY ACT (BSA): Technical Consistency, Analytical Turbulence for Banks

The events of 9/11 provided a wake-up call to leaders of many nations. A clear message was sounded calling on international cooperation to prevent future attacks. The key would be to squelch terrorist financing within the United States and abroad in order to thwart potential terrorist plots and cut off lines of support to terrorist groups. As chains of funding and financial transactions were analyzed, the paths repeatedly led to identified “weak links” in anti-money laundering (AML) efforts within and between nations. These weak links, whether they exist between nations or between financial institutions within a particular nation, provide a breeding ground for laundering funds from illicit activities and/or terrorist financing.

Laundering patterns and techniques remain quite consistent, regardless of the illicit activity (e.g., terrorist financing, drug trafficking, illegal arms trafficking, tax evasion). Requirements of regulations such as the BSA were historically established to detect potential laundering activities, and banks within the United States have long been required to report suspicious activity. While the United States had mechanisms in place within the banking system to assist in AML efforts prior to 9/11, after 9/11 it became more apparent that an expanded focus was necessary to properly utilize the tools at our disposal and to identify the movement of funds between various sectors of the financial services industry.

The passage of the USA PATRIOT Act in October 2001 subsequently set the stage for an entourage of financial services providers to join in BSA/AML compliance. The technical aspects of the BSA have not changed significantly for banks. The words on the regulatory page remain strikingly familiar. Yet, banks are finding it necessary to make considerable enhancements to existing systems and processes, including internal controls and suspicious activity monitoring capabilities. Why?

Over the years since the BSA was passed, the focus has shifted from a technical or checklist mentality to a forensic approach to compliance. This is particularly true in the area of suspicious activity monitoring. For example, banks are required to monitor and report suspicious activity through Suspicious Activity Report (SAR) filings. Traditionally, banks have filed SARs on activities such as embezzlement, insider abuse, and fraud. These types of activities do not simply appear “suspicious,” they appear to be illegal as well. Financial institutions are now expected to file SARs on “suspicious” (as the name implies) activities. Sounds simple enough, right? Unfortunately, financial institutions are stumbling upon significant weaknesses in the tools they have historically relied upon to identify and monitor suspicious activity.

Article continued on page 2:

We hope you enjoy this complimentary issue of the Bank Secrecy Act/Anti Money Laundering Ledger. In the future this publication will only be available on the Federal Reserve Bank of Chicago's website at:

http://www.chicagofed.org/other/email_notification.cfm. This free subscription service will send an e-mail directly to subscribers when new issues of the Bank Secrecy Act/Anti Money Laundering Ledger have been posted to the website.

In This Issue:

The Evolution of the Bank Secrecy Act (BSA)

A historical perspective on the BSA and the impact of the USA PATRIOT Act

Structuring

Defining structuring and the relationship to anti-money laundering

Monitoring Suspicious Activity

An overview of the challenges in monitoring for suspicious activity and examining bank systems

Frequently Asked Questions

Answers to some frequently asked questions about suspicious activity reports

One such weakness often surfaces as bank management attempts to wrestle with the identification of potentially suspicious transactions. How will unusual transactions or patterns of transactions be spotted? What reports are available from bank systems to allow them to effectively detect suspicious transactions and/or relationships? Once a comfort level is reached regarding the proper systems to enable the identification of unusual activities or transactions, the next potential weakness emerges. How will they know if the customer's activity or transactions are usual or unusual? The focus then shifts to account opening

procedures and the corresponding need to perform risk assessments on new customers. Consequently, many financial institutions are setting up profiles for accounts as they are opened. Information such as the intended use of the account and the level of activity anticipated by the customer is obtained at the time the account is established. Account opening information, coupled with transaction activity provides bank management with needed data when suspicious activity reviews are required.

As financial institutions step-up suspicious activity monitoring efforts, regulators and bank managers have discovered the obvious: "if you don't look, you won't find it." As a direct result of the passage of the USA PATRIOT Act, Congress is now looking, law enforcement is looking, regulators are looking, and the financial industry is looking!

STRUCTURING: The Buzz of BSA

The current "buzz" surrounding Bank Secrecy Act/Anti-Money Laundering (BSA/AML) is certain to be heard in connection with discussions of "structuring". What is "structuring"? The Bank Secrecy Act (BSA) defines structuring to include the following:

...a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the reporting requirements...

... "In any manner" includes, but is not limited to, the breaking down of a single sum of currency exceeding \$10,000 into smaller sums, including sums at or below \$10,000, or the conducting of a transaction, or series of currency transactions, including transactions at or below \$10,000. The transaction or transactions need not exceed the \$10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring within the meaning of this definition.

Financial institutions are required by the BSA and the Federal Reserve's Regulation H to file suspicious activity reports (SARs) if the institution knows, suspects, or has reason to suspect that a transaction:

- involves funds from illegal activities or is conducted to hide illicit funds or assets in a plan to violate or evade any law or regulation or to avoid transaction reporting requirements under federal law;
- is designed to evade any of the BSA regulations; or
- has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining available facts, including the background and transaction purpose.

Structuring, by definition, is aimed at evading Currency Transaction Report (CTR) filing requirements and is one of over 200 predicate crimes to money laundering. Structuring is often used as a primary means of introducing illegally gained funds into the financial system. The art of money laundering has typically included the structuring of transactions to avoid the attention of bankers and law enforcement and ultimately, detection of the true source of such funds.

More intricate forms of this type of structuring have gone mostly undetected in the financial services industry. Historically, structuring attempts were identified on an exception basis by tellers or other operational staff witnessing customers changing deposit amounts once CTR information was requested. Because of the increased emphasis on BSA

compliance after the passage of the USA PATRIOT Act, financial institutions are now expected to look beyond individual transactions to detect structuring that occurs over a period of time. This type of analysis may require changes in the types of reporting tools used by bank management and/or the methods used to deploy such tools for suspicious activity monitoring purposes.

As part of this process, an ongoing dialogue is required between bank personnel charged with daily monitoring for suspicious activity and other members of management responsible for specific customers and accounts (e.g. lending area or private banking, etc.). These dialogs should typically involve individuals from multiple functional areas/business lines within the institution so that management can gain an understanding of a customer's complete relationship in order to assess the risk associated with a particular customer or account. Moreover, examiners must also understand a customer's full relationship with the institution in order to conduct detailed transaction testing associated with current BSA/AML examinations and ultimately, to validate the effectiveness of banks' suspicious activity monitoring systems.

MONITORING SUSPICIOUS ACTIVITY:

Challenges of the Current Environment

The Bank Secrecy Act (BSA), as well as the Federal Reserve's Regulation H and Regulation Y, have required financial institutions to monitor for suspicious activity and make corresponding reports in the form of Suspicious Activity Report (SAR) filings. So why has this topic become so nebulous to so many within the banking industry? While the concept has not changed, the degree of monitoring and the expected methods used by institutions to monitor for suspicious activity are considerably more elaborate. Even the smallest community banks are affected by the shift in emphasis initiated by passage of the USA PATRIOT Act. However, the monitoring tools historically used by smaller community banks may continue to be a sufficient starting point under the new regime, assuming they are utilized appropriately. Larger, more complex community banks and large banking organizations are faced with a more difficult challenge of first assessing the usefulness of existing monitoring tools and reports, making appropriate changes, and then ensuring effective implementation.

Depending on various factors such as the size and inherent risk of the organization, financial institutions may employ different approaches to determining suspicious activity. The first line of inquiry has typically been to look at cash transactions. As such, cash transaction reports have been, and continue to be, a necessary part of monitoring for suspicious activity. Small community banks may use a daily cash report that identifies cash transactions over a certain threshold (e.g., typically ranges from \$3,000-8,000) and aggregates them by tax identification number. A daily report may be manageable for smaller institutions and can oftentimes be used as a starting point in identifying potentially suspicious cash transactions. The larger the institution, the more unwieldy a daily report becomes. A daily review, however, will not provide management with the information necessary to identify suspicious activity such as structuring. Therefore, daily cash transactions must then be

reviewed over a period of time (e.g., at least monthly) to detect instances or a pattern of structuring. Some institutions have allowed for this type of analysis by logging daily cash transactions into an Excel spreadsheet for ongoing monitoring. Other institutions have turned to vendors to gain access to standardized reports that aggregate the cash transactions automatically over a specified period of time. Aside from vendor reports, a wide array of application software programs are also used by larger institutions to allow for a more sophisticated monitoring system.

Ultimately, the goal is to deploy a monitoring system that is most effective and efficient for the size and complexity of the organization. Management must balance the cost of human resource time required for implementation of manual systems (e.g., daily reports and manual logging) with the hard costs of acquiring automated solutions.

If cash transactions are the first line of inquiry, what are the subsequent lines? Once an institution has identified any instance of potentially suspicious activity, a full review should be conducted. A comprehensive review for suspicious activity encompasses a customer's entire relationship with the organization. Accordingly, management should consider all available information as part of the review. At a minimum, the following should be considered, as applicable:

- Historical transaction information, both cash and non-cash equivalents
- Known related/linking accounts and the corresponding transaction histories
- Account opening information or account profile information
- Wire transfers
- Purchases of monetary instruments
- Loan relationships (e.g., loan file information)

- Other relationships or services utilized
- Comparison of account/customer activity with that of like businesses
- Public information/databases

One can quickly see the challenges associated with aggregating and compiling information from diverse sources. Regardless of the identification methods and tools used to monitor for suspicious activity, bank management and examiners will be required to assess the level of BSA/AML risk within accounts to verify that appropriate filings are made.

Publisher

Julie Williams (312) 322-4032

Editor

John Trapani (312) 322-5922

BSA / AML Group of Supervision and Regulation, 14th Floor
Federal Reserve Bank of Chicago
P.O. Box 834
Chicago, Illinois 60690-0834

FREQUENTLY ASKED QUESTIONS:¹

Suspicious Activity Reports

Q. What are examples of some common patterns of suspicious activity?

A. Some examples of common patterns are: (1.) transactions designed to avoid reporting and recordkeeping requirements; (2.) transactions that are not commensurate with the stated business type and/or are unexpected in comparison to volumes of similar businesses operating in the same locale; (3.) unusually large numbers and/or volumes of wire transfers or repetitive wire transfer patterns; (4.) suspected shell entities; (5.) bulk cash and monetary instrument transactions; (6.) transactions conducted in bursts of activities within a short period of time; and (7.) parties and businesses that do not meet the standards of anti-money laundering oversight programs (e.g., unregistered or unlicensed businesses).

Q. What is the critical information an organization should communicate in a suspicious activity report (SAR) narrative?

A. A SAR narrative should identify the five essential elements of information—*who? what? when? where? and why?*—of the suspicious activity being reported, as well as the method of operation (or *how?*). (1.) Who is conducting the suspicious activity? (2.) What instruments or mechanisms are being used to facilitate the

suspect transaction(s)? (3.) When did the suspicious activity take place? (4.) Where did the suspicious activity take place? (5.) Why does the filer think the activity is suspicious? (6.) How did the suspicious activity occur—in a concise, accurate, and logical manner, describe how the suspect transaction or patterns of transactions was committed. (For additional direction, please refer to FinCEN's November 2003 Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative.)

Q. If an organization files a SAR on a customer's activity and the customer continues to conduct similar activity, does the organization have to file another SAR?

A. As a general rule of thumb, organizations should report continuing suspicious activity by filing a SAR every 90 days. This will serve the purposes of notifying law enforcement of the continuing nature of the activity, as well as provide a reminder to the organization to determine if other actions may be appropriate, such as terminating its relationship with the customer.

Q. If an organization files a SAR and receives contact from a law enforcement agency indicating that the agency does not intend to investigate the matter reported on the SAR, is it necessary to continue to file a SAR if the same activity continues?

A. The 90 day "rule of thumb" remains applicable. Even if law enforcement has declined to investigate or there is knowledge that an investigation has begun, the filing of SARs on continuing suspicious activity provides useful information to law enforcement and other supervisory authorities. Moreover, information contained in the SAR that one law enforcement agency declines to investigate may be of interest to other law enforcement agencies or supervisory authorities.

Q. Does an organization have to close a customer's account if it has filed a SAR on the account?

A. A filing of a SAR, on its own, should not be the basis for terminating a customer relationship. Rather, a determination should be made with the knowledge of the facts giving rise to the SAR filing and other available information that could tend to impact such a decision. However, banking organizations should have their SAR-related policies address the procedures for monitoring ongoing activity and when to consider closing an account.

Author Julie Williams is the Team Leader of the Federal Reserve Bank of Chicago's BSA/AML Risk Specialist Unit. The views expressed are the author's and do not necessarily represent the views of management of the Federal Reserve Bank of Chicago or the Federal Reserve System.

FEDERAL RESERVE BANK
OF CHICAGO

P.O. Box 834

Chicago, Illinois 60690-0834

RETURN SERVICE REQUESTED