Financial Institutions Outreach Initiative

Report on Outreach to Large Depository Institutions
October 2009

FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Institutions Outreach Initiative

Report on Outreach to Large Depository Institutions

October 2009

Table of Contents

Executive Summary 1

Introduction 3

Bank Secrecy Act/Anti-Money Laundering Programs 4

Risk Assessment and Due Diligence 6

SAR Filings and Account Closure Procedures 7

Fraud-Related SARs 9

Fraud vs. Money Laundering 10

Currency Transaction Reports and the Exemption Process 12

Transactional Monitoring and Alert Review 14

Peer Groups 14

Alerts 14

Typologies and Manual Monitoring 15

Evaluation of Transaction Monitoring Tools 15

Bank Referrals 16

Investigations 17

Case Management 17

Money Services Businesses 19

Training 20

314(a) 21

314(b) 22

Financial Intelligence Units 23

Partnerships with Law Enforcement 24

Independent Testing (Audit) 24

Issues Raised by the Banks 26

SAR Sharing 26

Regulatory Observations 27

Information Technology 27

Civil Money Penalties 27

The 30-Day Clock 28
SAR Acknowledgements 29
Compliance Challenges 29
Standardized Country Risk Ratings 30
Requests for Guidance 30
Conclusion 31

Executive Summary

The Financial Crimes Enforcement Network (FinCEN) is engaged in a variety of initiatives to ensure that our mission as administrator of the Bank Secrecy Act (BSA) is carried out in the most efficient and effective manner possible. This outreach will also assist in FinCEN's ongoing work with the financial industry as financial institutions strive to comply with their responsibility to report certain financial information and suspicious activities to FinCEN, as well as our responsibility to ensure this useful information is made available to law enforcement, as appropriate. In furtherance of these goals, FinCEN initiated an outreach effort in 2008 with representatives from a variety of industries that fall under BSA regulatory requirements, beginning with large depository institutions.

The purpose of this report is to share information FinCEN gathered over the past year as part of its outreach initiative to large depository institutions. However, information contained in this report about specific practices and procedures obtained by FinCEN during the course of the outreach initiative does not imply FinCEN's approval of those practices, nor does it mean that FinCEN requires any institution to follow these examples. These findings alone do not change FinCEN's regulations or guidance.

Among the key findings, FinCEN learned that many larger depository institutions have account closure policies in place relating to suspicious activity report (SAR) filings. Generally, once a bank files a second SAR on a customer's activity, the account is closely monitored and may be closed, depending on law enforcement interest. Some institutions looked at exiting relationships that posed significant risk, rather than just closing the particular accounts reported on the SAR.

While acts of money laundering and fraud are often interconnected, FinCEN found that monitoring, investigation, and reporting for these suspicious activities was generally conducted by different groups within financial institutions, sometimes with limited interaction. The money laundering-related SAR process is managed within a bank's anti-money laundering (AML) or BSA compliance group, while the fraud-related SAR process is typically handled by other business lines within the bank, including corporate security, fraud prevention, loan risk and recovery, consumer lending operations, and credit card operations.

In addition, while banks indicated that automated transaction monitoring systems to generate "alerts" for further investigation provided added value to their efforts to identify suspicious activity, in the retail banking context, the banks unanimously indicated that they believe their best source of information on possible suspicious activity comes from referrals by front-line branch personnel and relationship managers.

The banks also provided feedback on where additional guidance would be helpful in fulfilling their AML program requirements. As a direct result of this feedback, FinCEN has already worked to respond in many areas, including providing guidance on the 30-day SAR filing clock and domestic SAR sharing with affiliates, as well as announcing the implementation of a system that will provide an acknowledgement to the bank after it files a SAR electronically through the BSA E-filing system. FinCEN will continue to work to address remaining areas of concern brought to our attention by the banks during the outreach meetings as appropriate.

During 2009, FinCEN has been conducting similar outreach to some of the largest money services businesses and will explore additional outreach opportunities with other industry groups and smaller institutions going forward.

Introduction

In 2008, FinCEN launched an initiative to visit some of the largest depository institutions in the United States in order to learn more about banking practices and how their AML programs operate, as well as the challenges of implementing these programs, to enhance our ability to ensure the consistent application of, examination for, and enforcement of the BSA.

In pursuing this initiative, FinCEN hoped that information obtained and discussed through the outreach would contribute to our broader understanding of financial industry practices, and of what information institutions need in order to effectively implement their AML programs. Specifically, FinCEN representatives were hoping to understand more about how the banks' AML programs operated, both technically and analytically, as well as how AML compliance was integrated with the banks' business plan.

Further, FinCEN was interested in exploring the opinions of large depository institutions regarding in-house financial intelligence or analytical units and their relation to BSA compliance programs, in order to help inform our efforts to develop additional guidance for the financial industry.

FinCEN used the Federal Deposit Insurance Corporation (FDIC) Institution List of Top 100 Banks and Thrifts Nationally by Asset Size (as of September 30, 2007) to identify the top 15 depository institutions. Once the institutions were identified, a letter was sent to the appropriate senior official within each institution to outline the goals of the FinCEN outreach initiative and invite the institution's participation.

Between April 16, 2008 and January 28, 2009, interdisciplinary teams from FinCEN visited eight depository institutions in conjunction with this outreach effort. The remaining institutions were not visited, either because of scheduling difficulties or extenuating circumstances, including mergers with other financial institutions during the time period of the outreach effort.

Although FinCEN reached out generally to these institutions to participate in the outreach initiative, each institution was asked to develop its own agenda for the meeting. Accordingly, the topics covered and issues discussed with each institution varied.

While visiting with the depository institutions, FinCEN received several demonstrations that provided additional insight into how the banks' AML programs operate. Demonstrations were provided in the following areas:

- Account opening
- Wire transfer monitoring
- 314(a) process
- Transaction monitoring
- Alert processing
- Case management
- SAR filing

This report summarizes the information gathered by FinCEN during the course of the outreach to the largest depository institutions. In order to safeguard the proprietary business information provided by the banks, no bank names are used within this report.

FinCEN would like to express its appreciation to all the banks and their staff that devoted their time and effort to participate in this outreach initiative. FinCEN team members found all of the meetings to be very informative and valuable toward furthering FinCEN's broader mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems from abuse by promoting transparency in the U.S. and international financial systems.

Bank Secrecy Act/Anti-Money Laundering Programs

The Bank Secrecy Act (BSA) was enacted by the U.S. Congress in 1970 in response to concern over the use of financial institutions by criminals to launder the proceeds of their illicit activity.[1] The BSA has been amended on several occasions, most significantly by the Money Laundering Control Act (MLCA) of 1986[2] and Title III of the USA PATRIOT Act of 2001.[3]

1. See http://www.fincen.gov/statutes_regs/bsa/ and Titles I and II of Public Law 91-508, as amended, codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5314, 5316-5332.
2. See Public Law 99-57 and 18 U.S.C §§ 1956 and 1957.
3. See Title III of Public Law 107-56, available at http://www.fincen.gov/statutes_regs/patriot/

The BSA authorizes the Secretary of the Treasury, inter alia, to issue regulations requiring financial institutions to keep certain records and file certain reports[4], and to implement anti-money laundering programs and compliance procedures to guard against money laundering.[5] The authority of the Secretary to administer the BSA has been delegated to the Director of FinCEN.[6] The BSA's overarching goal is to "require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."[7]

While some requirements in the BSA and its implementing regulations apply to individual persons, most of the BSA's statutory and regulatory requirements apply to financial institutions.[8] The statute defines the term "financial institution" broadly. It includes traditional financial institutions such as banks, securities broker-dealers, and insurance companies. It also includes cash-intensive entities that handle significant amounts of currency such as casinos and money transmitters, as well as entities not traditionally considered financial institutions but which engage in transactions that can also be vulnerable to money laundering, such as dealers in precious metals, stones, or jewels, and vehicle sellers.

One of the key provisions of the BSA is the requirement for financial institutions to establish anti-money laundering programs, which at a minimum must include: the development of internal policies, procedures, and controls; designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs.[9]

All of the banks FinCEN visited with during its outreach program have highly developed corporate-wide, risk-based AML procedures tailored to their various lines of business (LOBs). In some banks, the LOBs have dedicated AML officers running the day-to-day operations within each business line. These officers oversee training and self-testing and escalate matters as appropriate. In one bank, for example, there are over 80 LOBs. Each has its own BSA coordinator, tailored procedures, and self-testing.

---

4. See 31 U.S.C. §§ 5313 and 5318(g).
5. See 31 U.S.C. § 5318(h).
6. See Treasury Order 180-01 (Sept. 26, 2002).
7. See 31 U.S.C. § 5311.
8. See 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 103.11(n).
9. See 31 U.S.C. § 5318(h).

Technology was cited as the primary cost driver of the banks' AML programs. One bank noted that half of its annual AML budget was devoted to technology. Technology challenges were discussed at each bank, specifically related to vendor issues, fine-tuning of peer groups used in the transaction monitoring process, development of case management systems, integrating AML systems with fraud and other risk management systems, and integrating AML systems during and after mergers and acquisitions.

Most banks visited have established the equivalent of an AML oversight committee, which meets on a regular basis, usually monthly or quarterly. These committees are typically chaired by the global head or director of AML or BSA officer and are convened as a mechanism to discuss and share best practices, oversight, and provide guidance to the AML group. These committees also oversee a bank's AML risk assessment program.

Risk Assessment and Due Diligence

A bank's risk assessment program enables leadership within the bank to better identify and mitigate potential vulnerabilities within the bank's BSA/AML controls.

Banks provided information on risk management practices involving AML program review, product risk assessment, client risk assessment, geographic risk assessment, and enhanced due diligence. Governance of the program is typically conducted by key committees established to ensure the timely escalation and consideration of issues by senior management, as well as structured communications and surveillance established to identify, track, and escalate AML issues across the firm.

The risk assessment process requires each LOB to review the entirety of its business, evaluating risks and controls pursuant to consistent standards. This includes defining the inherent risk factors, describing the customer base (segment, size, geography, entity ownership) and the products offered in each major business area, identifying the degree of AML risk throughout, and describing the associated risk mitigation/control program.

Risk assessments are generally completed and housed in Web-based applications, which permits the LOBs to update AML risk and control data in a more efficient manner and enhances the accessibility of the assessments.

Using detailed manuals developed within the bank, risk assessments are conducted on business units, most using a three-tiered rating system. AML controls in place are also assessed. The manuals help promote cross-business consistency while providing flexibility.

Customers are also risk-ranked based on products and services offered, geography, customer type, and account activity.

Geographic risk assessment was highlighted as particularly time-consuming. One bank noted that it currently evaluates and risk-ranks over 200 countries. The assessment includes a review of daily news clips, so time is spent on country assessment each day. The bank is exploring possible vendor options to facilitate this research in hopes of transitioning to an annual country review.

Many banks also risk-rate their employees, based on their position. One bank noted that high risk employees are the gatekeepers (front-line relationship managers), transaction handlers (operations personnel, back room cash managers), and risk managers (senior managers, legal and compliance positions). Another bank also noted their high risk employees also include employees with independent testing and oversight responsibilities.

One bank utilizes the Quantity of Risk Matrix provided in the FFIEC BSA/AML Examination Manual and tailored it to fit their operational needs. The 2007 AML Risk Assessment was enhanced to include the *quantity* of risk, in addition to the quality of risk, which was the focus of the assessment in 2006. The AML Risk Assessment is a subset of the bank's compliance risk assessment.[10]

SAR Filings and Account Closure Procedures

The BSA authorizes the Secretary of the Treasury to require a financial institution to file a suspicious activity report (SAR) on any suspicious transaction relevant to a possible violation of law or regulation.[11] Suspicious activity reporting rules apply to banks, casinos, broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities, most money services businesses, and certain insurance companies.[12]

10. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf (p. 18).
11. See 31 U.S.C. § 5318(g).
12. See 31 CFR §§ 103.15-103.21.

The bank SAR rule requires a bank to report a transaction exceeding $5,000 where the bank knows or has reason to suspect that: (i) the transaction involves funds derived from illegal activities or is intended to conceal such funds to avoid a transaction reporting requirement; (ii) the transaction is designed to evade any requirement of the BSA; or (iii) the transaction has no apparent business purpose or is not the "normal" variety of transactions engaged in by a particular customer.[13]

To protect the confidentiality of these reports, the statute forbids any filing institution or its personnel from notifying anyone involved in the transaction that the transaction has been reported, a prohibition that extends to any government employee or officer, unless the notification is necessary to fulfill the official duties of the employee or officer.[14]

In addition, the statute contains a "safe harbor," which protects any financial institution and its personnel filing a SAR, whether the filing is mandatory or voluntary, from liability on account of the report or for failing to give notice of the report to any person who is identified in the report.[15]

During meetings with the banks, SAR filing procedures were described as a staged process starting with an alert or referral. Some banks noted that the $5,000 *de minimus* threshold is not a significant consideration when filing a SAR; if the activity is considered suspicious they will file regardless of the dollar amount involved. One bank noted that electronic surveillance used to detect suspicious activity is supplemented by LOB specific training that provides examples of potential suspicious activity that may arise outside activity covered by electronic surveillance.

Banks had differing policies relating to SAR filings and account closures. For some banks, one egregious SAR filing could lead to an account closure; however, many banks stated they initiate the account closure process following two SAR filings.

One bank noted that it does not close accounts; rather, it decides to "exit a relationship" with a customer based on a set of circumstances. It notes, however, that exiting a relationship is considerably harder than simply closing an account, since identifying the complete relationship can be a complicated and lengthy process (some customers hold hundreds of accounts and utilize many bank products and services, including credit products).

13. See 31 CFR § 103.18.
14. See 31 U.S.C. § 5318(g)(2).
15. See 31 U.S.C. § 5318(g)(3).

All banks stated that they will keep an account open for investigative purposes if they receive a request from law enforcement; however, several banks noted that they ask either that law enforcement keep them informed of the status every 6 months or that the request from law enforcement be provided in writing.[16]

Several banks indicated that if they detect that a customer is structuring transactions, they will typically send a brochure, letter, or other educational materials to the customer that explains BSA reporting requirements. If activity continues after this outreach, the bank will close the account. Since the conclusion of our outreach, we have since heard that banks are also providing FinCEN's educational pamphlet released in February of this year entitled, "Notice to Customers: A CTR Reference Guide," which is another resource available to address customers' questions about BSA reporting requirements.[17]

In addition, the banks indicated that they are very careful and serious in their SAR filing decisions. The banks were emphatic that after careful review they were filing SARs that were required and may merit law enforcement investigation.

Further, during one of the visits, a bank representative indicated that occasionally, they re-acquire customers during mergers and acquisitions that they have previously exited due to suspicious activity. This led FinCEN to wonder what customers that have been exited from a large bank generally do with their banking relationships post-exiting and what policy implications this may have for the financial system and FinCEN's work. FinCEN is currently conducting research in this area.

Fraud-Related SARs

In many banks, the filing of fraud-related SARs is handled by various business lines within each bank, including corporate security, fraud prevention, loan risk and recovery, consumer lending operations, and credit card operations. However, one bank noted that while various business lines may make referrals of potentially suspicious activity, all of its SARs are filed by their BSA office.

Several banks noted they are witnessing an increase in fraud-related SARs, specifically in the areas of mortgage loan fraud, home equity loan fraud, credit card fraud, and general account misrepresentations and false statements. Several banks commented that FinCEN's *SAR Activity Reviews* and mortgage loan fraud studies are helpful tools to assist in identifying this type of activity.

16. See http://www.fincen.gov/statutes_regs/guidance/pdf/Maintaining_Accounts_Guidance.pdf
17. See http://www.fincen.gov/whatsnew/html/20090224.html

Fraud vs. Money Laundering

In contrast, FinCEN's work in the fraud area illustrates that while fraud and money laundering are often viewed as separate criminal enterprises, acts of fraud and acts of money laundering are often quite interconnected. The financial gain of the fraudulent activity ultimately needs to be integrated into the financial system, so money laundering is often a product of fraud.

Therefore, it was of interest to FinCEN that many banks' AML programs are run entirely separately from their fraud detection programs. Several banks noted the challenge that a successful AML program does not recoup losses like anti-fraud programs – with pure money laundering, there typically is not a loss for the bank, meaning there are no funds to recoup.

However, from a due diligence perspective, information financial institutions have available and collect to comply with their anti-money laundering program requirements in many ways mirrors the information they would already be gathering for anti-fraud purposes; customer and transactional information used for AML purposes is often the same customer and transactional information needed for fraud investigations. As a result, the resources being spent on fraud detection and prevention within financial institutions may well support the AML program, and vice versa.

In fact, one bank also observed that, historically, as AML programs and fraudulent activity became more sophisticated over time, efforts by banks to combat fraud and money laundering diverged. This bank noted that they are now starting to see fraud and AML programs at their institution, as well as others, merge back together because there is an increasing recognition of the similarity of the data being collected to investigate fraud and money laundering. The bank also noted that with the increasing convergence of fraud and AML investigations taking place within the bank, there is yet another benefit to merging anti-fraud and anti-money laundering resources and tools.

Another bank noted, however, that notwithstanding the linkages, fraud investigations and controls are distinct from AML in key respects, and no one organizational model will be appropriate for all financial institutions.

FinCEN understands that selling the business case for fighting fraud is easier because it impacts the bank's bottom line (for frauds committed against the bank) and the bank's customers (for frauds committed against customers). Many banks noted that while there is a genuine interest within all levels of the bank to fight money laundering, it remains an ongoing challenge for AML officers within the bank to make as strong a business case as their fraud-prevention counterparts. For the financial institution, the business case for fighting fraud is a much easier argument to make when every investigation not only works to recover the proceeds of fraud, but also aims to detect and prevent fraud from taking place so that there is no loss to begin with.

These observations became the genesis of a speech Director Freis delivered at the Florida Bankers Association in September 2008 and again in a speech before the Association of Certified Fraud Examiners in July 2009. In his remarks, Director Freis discussed how acts of fraud and acts of money laundering can be ***interconnected***, and he encouraged banks to leverage their fraud resources with their AML efforts to start taking advantage of significant efficiencies that are available through such leverage.[18]

The interconnectedness of criminal activity was also discussed in an analytical study that FinCEN released in March 2009, which looks at the relationship between mortgage fraud and other financial crime, and identifies how financial crime runs through the different financial sectors. [19]

The banks expressed their appreciation of FinCEN's analytical products in the mortgage fraud area, which in some cases resulted in institutions changing some of their processes related to risks of fraud in mortgages. It was also noted by several banks that feedback provided by FinCEN on the value of the BSA data has resulted in a much better understanding within the banks of its importance and usefulness. Several banks noted that the value could be improved by providing analysis of more current trends.

18. See http://www.fincen.gov/news_room/speech/pdf/20080923.pdf and http://www.fincen.gov/news_room/speech/pdf/20090713.pdf

19. See http://www.fincen.gov/news_room/rp/files/mortgage_fraud.pdf

Currency Transaction Reports and the Exemption Process

Pursuant to Bank Secrecy Act regulations, a bank is required to file a Currency Transaction Report (CTR) for each transaction in currency of more than $10,000 by, through, or to that bank. Additionally, multiple currency transactions totaling more than $10,000 during any one business day must be treated as a single transaction if the bank has knowledge that they are by or on behalf of the same person.[20]

The Money Laundering Suppression Act of 1994 (MLSA) amended the BSA by authorizing regulations exempting transactions by certain customers of depository institutions from currency transaction reporting.[21] FinCEN issued exemption regulations in two phases, specifying the criteria under which a bank may take advantage of the exemption authority.[22] Under Phase I exemptions, transactions in currency by banks, governmental departments or agencies, and public or listed companies and their subsidiaries are exempt from reporting.[23] Phase II allows depository institutions to exempt from reporting transactions in currency between it and "non-listed businesses" or "payroll customers."[24]

The banks participating in the outreach program indicated that candidates for exemptions are identified by relationship managers, branch, and back office personnel, as well as by transaction monitoring. Banks use an online application form to submit new exemptions for review. The exemption approval process typically involves the review and decision of the bank's AML oversight committee and/or the bank's retail AML compliance official.

In addition to Phase I, some banks indicated that they do utilize Phase II exemptions. These banks noted that they actively work to identify new customers to exempt and set goals for how many exemptions they aim to add. One bank commented that they view exemptions as a customer service tool because customers would not need to spend time providing the bank with the requisite CTR information (including conductor information for cash deposits made at branches). This bank's largest customer exemption categories are government entities, publicly traded companies and their subsidiaries, and restaurants. All exemptions are vetted by the bank's BSA team and are reviewed on an annual basis.

---

20. See 31 C.F.R. § 103.22(b).
21. See section 402 of the Money Laundering Suppression Act of 1994, Title IV of the Riegle Community Development and Regulatory Improvement Act of 1994, Public Law 103-325 (Sept. 23, 1994).
22. See 31 CFR § 103.22(c).
23. See 31 U.S.C. § 5313(d).
24. See 31 U.S.C. § 5313(e).

Another bank also noted that exemptions are a "business positive." Management was complimentary of the new CTR exemption regulation, stating that it will free up resources previously spent on the biennial review process, enabling the bank to increase their number of exemptions.

One bank commented that most of its time in the exemption process is spent on the annual review of non-listed businesses, which requires the bank to review, verify, and document once per year the information supporting each designation. In addition, the bank must review and verify at least once per year that management monitors these accounts for suspicious activity.

Some banks, however, note they utilize Phase I exemptions almost exclusively, with very minimal use of Phase II exemptions. Two of the banks noted that while there is a recognized business need for some exemptions, so as not to inconvenience certain customers, from a regulatory risk perspective there is little reward for granting Phase II exemptions: they felt that they were exposed to regulatory scrutiny for failing to properly exempt, but not for failing to exempt.

Two banks commented on the difficulty of identifying cash transactions, because systems are designed to capture the *amount* of the transaction, not whether it took place in cash or check, for instance. This results in a significant amount of back-end work to ensure that all cash transactions conducted by or on behalf of a single person where the total of those transactions exceeds $10,000 are identified, aggregated (where required) and reported.

Near the conclusion of the outreach program, in December 2008, FinCEN issued a final rule simplifying the requirements for depository institutions to exempt their eligible customers from CTR reporting.[25] The final rule makes the following changes to the current CTR exemption system:

- Depository institutions will no longer be required to review annually or make a designation of exempt person (DOEP) filing for customers who are other depository institutions, U.S. or State governments, or entities acting with governmental authority.
- Depository institutions will be able to designate an otherwise eligible non-listed company or a payroll customer either after 2 months time (previously 12 months) or after conducting a risk-based analysis of the legitimacy of the customer's transactions.

25. See http://www.fincen.gov/statutes_regs/frn/pdf/frnCTRExemptions.pdf

- FinCEN's guidance on the definition of "frequent" transactions will be changed to five transactions per year instead of the current eight transactions per year.
- Depository institutions will no longer be required to biennially renew a designation of exempt person filing for otherwise eligible Phase II customers, but an annual review of these customers must still be conducted.
- Depository institutions will no longer be required to record and report a change of control in a designated non-listed or payroll customer.

Transactional Monitoring and Alert Review

One bank noted the importance of taking a "layered" strategy toward AML compliance as it relates to transaction monitoring. The selection of tools, data and intelligence sources, and the extent to which AML operations relies on them for monitoring, is driven by the risks posed by the customers, products of a LOB or sub-LOB, and the capabilities of the tools. Several banks noted that no one tool can catch everything.

Peer Groups

Several banks utilize various software applications to conduct transaction monitoring. Transaction monitoring systems compare account activity value and volume levels to other accounts in a "peer group," accounts expected to transact in similar ways over time. Peer groups may be segmented by LOBs, product types, geography and/or account types. Comparisons are also made between account activity value and volume levels and the historical transaction activity within the same account. Account activity is compared to a set of pre-defined rules. Variance from normal activity levels causes "alerts" or "events" which are scored and totaled at the account or customer levels. When a score crosses a defined threshold, an alert is generated for investigator review.

One bank noted that it has dedicated staff resources to focus solely on studying and understanding its data in order to effectively shape these peer groups.

Alerts

The number of alerts generated within each bank varies based on a number of factors, including the number of transactions running though the monitoring system, as well as the rules and thresholds the bank employs within the system to generate the alerts.

Banks typically score alerts based on elements contained in the alert, which in turn determines the alert's priority. Banks will typically review and re-optimize their alert programs every 12-18 months.

Banks noted that a significant number of alerts are ultimately determined to be "noise" generated by the software. One bank noted that it is working continuously to reduce the "noise" generated by the software and to develop typologies to enrich the data and reveal the most critical information.

Typologies and Manual Monitoring

Banks build typologies gleaned from previous investigations into their investigative strategy, creating risk models that assist the monitoring tools to identify suspicious activity.

For instance, one bank developed a typology based on referrals from branch locations involving cash flows between a border state and the mid-west. The accounts were being opened on the border; however, all of the activity within the accounts was occurring in the mid-western United States. The bank continues to work with Immigration and Customs Enforcement on an ongoing basis to assist in uncovering activity tied to human and drug smuggling rings.

In addition to relying upon transaction monitoring systems, banks also conduct manual monitoring within the LOBs and/or their "financial intelligence unit" (FIU).[26] For example, one FIU currently monitors wires involving Lebanon, Brazil, Pakistan, the Tri-Border Region and the Channel Islands. The FIU also monitors foreign currency transactions and attempts to use domestic stored value cards overseas.

Evaluation of Transaction Monitoring Tools

The level of satisfaction with transaction monitoring tools varied by bank. One bank indicated that it is very happy with the system it employs, noting that the tuning of the peer groups is done annually, which it hopes will help keep the false-positive rate down. The bank found the most benefit comes from the vendor user-groups where the bank is able to interact with its peers and discuss best practices.

26. A more detailed discussion of financial intelligence units follows on pg. 18.

Another bank noted that it is continuing to work with its vendor to improve the quality of alerts generated. In some cases this requires reconstruction of existing peer groups and adjustments to alerting thresholds to reduce noise while increasing alert to case yield. The bank is also working to enrich alerts with additional data to target specific suspicious behaviors.

This bank also has developed an in-house monitoring tool used for certain transaction types. It provides filter algorithms consisting of LOB-specific parameters and established rules looking for specific behavior. Alerts are generated when activity exceeds the parameters defined within the filters. Unlike some commercially available software, alert settings can be changed and the results observed immediately. This system uses input based on hypotheses about the activity the bank is trying to stop, rather than just looking for outliers.

Bank Referrals

Despite the level of resources invested in automated monitoring tools, the banks were unanimous in their belief that referrals from their officers and employees within their branches and operations remain the most productive source of information. Because bankers have direct access to the customer and the ability to detect intangible warning signs, such as demeanor, these front-line referrals most often do result in an investigation.

One bank estimated that over 80 percent of its suspicious activity referrals are generated from bank personnel, while the rest are the result of alerts generated by the transaction monitoring systems and reports. Another bank noted that 25 percent of its investigations originate from staff referrals and 45 percent of its AML SARs that are ultimately filed originated from these referrals.

The method for reporting branch referrals of suspicious activity varies by bank, but it is typically done on an internal report similar to the SAR form or through a toll-free hotline available to branch employees.

Investigations

Several banks noted that they focus extensively on the narrative portion of the SAR and that this section is written with law enforcement in mind. In some cases, the managers and investigators within the bank's investigations unit are former law enforcement officers who have experience with financial investigations and are knowledgeable about the information that law enforcement needs. Other banks stressed that they try and tell a clear story of the suspected activity and construct their narratives to keep other end-users of the BSA data in mind, such as regulators, FinCEN analysts, and SAR Review Teams.

Case Management

Each bank employs a different case management tool to track the investigation's progress through to a SAR filing determination and if warranted, through to the SAR filing process.

One bank's case management system compiles transaction data, customer profile data and related account information (debits and credits). The system allows the analyst to check other databases while working in the application and pull all source information together into a concise package for analysis and management review and approval.

Investigators focus on trying to determine where the money came from, what happened to it while at the bank and where it went when it left. If a SAR is filed, this bank conducts a post-investigation to determine if suspicious activity continues and if a supplemental SAR is required. If a second SAR is necessary, the account closure process is generally initiated.

This bank indicates that 65 percent of investigative cases result in SAR filings, up from 50 percent not long ago. SAR clocks are built in to meet time requirements and the management system alerts the user when deadlines are approaching. The bank also noted that it has had good experiences with examiners not questioning the bank's decisions to file – or not to file – a SAR.

The bank provided a demonstration of its SAR filing tool, which populates the SAR form from investigative details in the case management tool. The system will alert to blank fields and some fields must be filled in before proceeding and/or submitting the SAR form.

Another bank noted that its case management system maintains timelines and due dates for action by analysts and investigators to ensure deadlines for filing are met. The case management system provides an area where the analyst or investigator can journal and include investigative notes. These entries, in addition to manager review, are all time and date stamped within the system. Any due diligence that has been discovered or supporting documentation can be included as PDF files within this environment. If, after the investigative process, a decision is made not to file a SAR, this will be noted within the case management system.

In various banks, investigators participate in monthly group meetings that provide the ability to discuss issues across the various LOBs. A business group will discuss its cases or any new trends or anomalies discovered. This interaction allows for cross training to understand the nuances that exist within the different business lines.

One bank explained that once an alert is generated by their monitoring system, 6 months of account activity is reviewed. Investigators have 2 weeks to complete their research and analysis on an alert before making a determination as to whether an investigation needs to be opened. Once a decision is made to initiate an investigation, the alert is entered into the bank's case management system. At this point, the timeline for filing a SAR starts.

Investigators make every effort to make SAR filing determinations within 30 days, although research will sometimes require 45 days.

If a determination is made not to file a SAR, the investigator reflects this as an "unfiled case." Supporting documentation as to why the determination not to file was made will be included, as well as an indication as to whether or not the account will continue to be monitored.

Money Services Businesses

For several years, FinCEN has emphasized the importance of ensuring that money services businesses (MSBs) that comply with their responsibilities have reasonable access to banking services.[27] The issue of providing banking services to money services businesses was discussed during the outreach meetings and FinCEN received information during the meetings indicating a wide variety of bank approaches to this issue.

Since these meetings, FinCEN has heard early indications, particularly through our outreach meetings with the MSB community, that generalized concern about the availability of banking services seems to be easing somewhat, though there are still difficulties confined to specific geographical regions, to certain categories of MSBs, as well as potential difficulties based on the size of the business activity. Also, in May 2009, FinCEN issued a Notice of Proposed Rulemaking (NPRM) designed to make the determination of which businesses qualify as an MSB more straightforward and predictable.[28] FinCEN is currently in the process of reviewing the comments received on the NPRM following the close of the comment period on September 9, 2009.

One bank indicated that it will not maintain accounts for certain categories of businesses that it considers a higher risk for money laundering, including those where more than 50 percent of an account's activity involves MSB activity (check cashing, money transmitting, etc.). This bank indicates that the amount of due diligence required to bank a customer with more than 50 percent of MSB-related activity is cost-prohibitive. This bank will also not service payday lenders, title lenders, embassies/ foreign consulates or shell banks.

Another bank noted that it continues to bank MSBs as a matter of good and fair business practice, but its front-line retail staff is prohibited from opening the accounts. The business banking staff responsible for originating MSB accounts have a 5-question test that they present at all account openings. The questions relate to the way the MSB operates (i.e. clientele, countries of permissible remittance, etc.). If one or more of the questions is answered in an unsatisfactory manner, the prospective account is referred on for additional enhanced due diligence before any decision is made. As a general matter, site visits are conducted prior to any MSB account opening, and all MSB accounts are placed in the "high risk" category throughout the life of the business relationship.

---

27. See http://www.fincen.gov/statutes_regs/guidance/pdf/fincenadv04262005.pdf

28. See http://www.fincen.gov/news_room/nr/pdf/20090512.pdf

Training

The BSA requires financial institutions to establish an ongoing employee training program as a part of fulfilling their anti-money laundering program requirements.[29] As noted in the 2007 FFIEC Examination Manual:

> "Banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA."[30]

During the outreach meetings, each bank provided an overview of its employee training program, policies, and procedures, which varied between banks. Some banks indicated that all of their associates are trained annually, including Board members, with very minimal exceptions being made (such as aviation, corporate dining staff). Other banks noted that annual AML training is required only for their high-risk employees, although low-risk employees are offered the training on an optional basis. One bank indicated that its AML compliance officers are required to complete an internal certification program.

Some banks use "knowledge checks" in lieu of quizzes to ensure an understanding of the material, while some banks do include testing with a certain pass-rate before credit is given. Several banks noted that they train their employees through additional multiple channels including: Web-based training, workshops, quarterly town halls, and additional courses as needed by various compliance teams.

The completion of AML training is tracked internally. One bank noted that failure to complete the required training is taken very seriously and may lead to discipline up to and including monetary penalties and/or termination. Several employees have been terminated since implementation of the policy. Another bank noted that the successful completion of AML training is a part of the bank's code of conduct statement. Violations for failure to complete training are potential grounds for termination. Bank employees who attend conferences or other training events are required to report back and share what they've learned with their colleagues.

29. See 31 U.S.C. § 5318(h)(1)(C).

30. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf (p. 33)

314(a)

FinCEN's regulations under Section 314(a) enable Federal law enforcement agencies, through FinCEN, to reach out to more than 45,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering.[31]

FinCEN receives requests from Federal law enforcement and upon review sends requests to designated contacts within financial institutions across the country once every 2 weeks via a secure Internet Web site. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial institutions in searching their records.

The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. Financial institutions have 2 weeks from the transmission date of the request to respond to 314(a) requests. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request.

Several banks noted that they recognized the value of the 314(a) process and believed that these resources were being well utilized in the investigation of significant money laundering and terrorist financing cases.

From a process standpoint, several banks noted that if they have a 314(a) match, these subjects are treated similarly to how alerts are handled. For example, one bank indicated that in addition to completing the required checks as part of the 314(a) process, when it has a positive match, it will investigate further and file a SAR if deemed necessary. Occasionally, this bank will see 314(a) subjects as customers already identified as suspicious.

Another bank estimated that for about 25 percent of the requests it will have 1-2 positive matches. If the bank has a positive match on a 314(a) request, law enforcement is contacted, if appropriate, and a subsequent SAR will be filed if needed. For this bank, if a match is found, a SAR investigation is started immediately. In some cases, the bank has found that an investigation is underway. This bank will consult with the law enforcement point of contact to resolve uncertain matches.

31. See 31 CFR § 103.100(b).

Similarly, another bank also noted that if they have a positive match, as a matter of course, a SAR investigation will be opened. While not required by regulation, the bank noted that they view this as a matter of safety and soundness. In addition, even if there is not an exact match, but the bank determines they have a customer with a very similar or apparently related name, an investigation will be opened. If subject of the 314(a) request is a corporation, and the bank has a customer that is the registered agent for that corporation, they will also open an investigation.

While the issue was not specifically addressed at all institutions, two banks indicated that they do not keep 314(a) subjects on a continuing watch list.

314(b)

Section 314(b) of the USA PATRIOT Act allows regulated financial institutions to share information with each other for the purpose of identifying and, where appropriate, reporting ***possible money laundering or terrorist activity***.[32]

Banks found the 314(b) process very useful from an investigative perspective. Several banks noted that they often use the 314(b) process throughout the course of a SAR investigation, before filing a SAR, or making a decision to close an account. One bank's investigative team characterized the 314(b) program as a very useful tool in obtaining additional information about a case, while another bank characterized its use of information sharing through 314(b) as "extensive." The bank noted that its experience with 314(b) has allowed it to see a "panoramic view of activity, not just a snapshot."

Another bank characterized the 314(b) process as a "very efficient" way to share with other banks. The bank noted that it had shared information through 314(b) with three other financial institutions, which resulted in a large post-Katrina fraud investigation.

One bank, however, noted that it has recently experienced an "explosion" of 314(b) requests. The bank estimates there has been a 150-200 percent increase in these types of requests in the past 6 months. The increase has had an effect on the 30-day clock monitoring for SAR filings, and the bank has found that it is sometimes filing SARs only to have to file an amended SAR.

FinCEN understands that some banks were hesitant to share information under the 314(b) program as it related to ***suspected fraud***. Following ongoing discussions regarding this issue during these outreach meetings and within the Bank Secrecy

32. See 31 U.S.C. 5311 note; implementing regulations are at 31 CFR § 103.110.

Act Advisory Group,[33] FinCEN issued guidance on June 16, 2009 to clarify the scope of permissible sharing covered by the section 314(b) safe harbor. The guidance clarifies that financial institutions, upon providing notice to FinCEN and using procedures designed to safeguard the information, are permitted to share information with one another.

Sharing of information is permitted to identify and report activities, such as suspected fraud — or other specified unlawful activities (SUAs) — if there is a nexus between the suspected fraud or other SUA and possible money laundering or terrorist financing activity.[34] We expect this guidance to result in further exchange of information among financial institutions for the purpose of fighting fraud.

Financial Intelligence Units

The vast majority of banks that were visited had established stand-alone "financial intelligence units" (FIUs) to support their efforts to comply with reporting requirements under the BSA. Although the name is the same, this should not be confused with FinCEN's role as the financial intelligence unit of the United States.[35] Naturally, the FIUs within the banks varied greatly in size and organizational structure depending upon the size of the bank and its risk profile.

In some cases, mostly with the larger regional banks, the FIU was housed within the same complex or city as the bank's headquarters; however, in a few cases, the FIU was housed in the same complex or city as the bank's compliance function rather than its headquarters. In these cases, these geographical differences were the result of mergers or acquisitions where an infrastructure and personnel were already in place at a separate location to house the bank's FIU.

The FIUs operate in many ways like FinCEN's analytical function. The investigations, analyses, information-sharing, and regional breakdowns are organized and performed in a similar manner. Significant transaction monitoring, alert processing, 314(a) and OFAC searches, SAR filing determinations, and relationship termination recommendations all originate within the FIU.

---

33. The Bank Secrecy Act Advisory Group consists of representatives from State and Federal regulatory and law enforcement agencies, financial institutions, and trade groups.

34. See http://www.fincen.gov/news_room/nr/pdf/20090616.pdf.

35. See Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit, available at http://www.egmontgroup.org/files/library_egmont_docs/egmont_final_interpretive.pdf.

Partnerships with Law Enforcement

All of the banks maintain active, engaged relationships with Federal, State, and local law enforcement officials. One bank noted that in the first months of 2008, they had received over 100 requests for supporting documentation from law enforcement as a result of SARs that they had filed. Despite this number of requests, the bank also noted that many in the local law enforcement community do not realize they can obtain documentation in support of a SAR from the filing bank.

Several banks noted their investigators are active with the SAR Review Team within their banks' regions. The banks characterize their interactions with these teams as very beneficial.

Some banks noted that they draw on the SAR Review Teams to assist in training bank employees within their FIU. One bank also noted that they engage closely with their law enforcement contacts to: gather feedback on the usefulness of the SARs that are filed; during the process of producing underlying SAR documentation in response to subpoenas received on SAR suspects; and in cases where the bank notified law enforcement prior to, or concurrent with, SAR filing.

Independent Testing (Audit)

The BSA requires financial institutions to independently audit their AML program to objectively evaluate and test the overall program.[36] The independent audit assists the bank's management in identifying possible areas of weakness where enhancement or stronger controls may be needed.

Several banks noted that they have an internal audit team designated as its independent tester and that the audit function is a separate division reporting to the Board of Directors.

One bank noted that a majority of audit time is spent in the know your customer/ customer identification program. Monthly regulatory audit council meetings are held to discuss issues, exams, regulatory changes, and hot topic updates. Additionally, monthly meetings are held with the in-house Federal regulatory agency team.

Another bank noted that its audit team is supplemented by auditors specializing in the particular area being audited. In the past, the bank had contracted out some of their audit work but no longer does so.

---

36. See 31 U.S.C. § 5318(h).

This bank's independent testing approach includes the performance of independent risk assessment to determine risk in LOB areas, as well as targeted audits as warranted by the risk assessment and other organizational changes. The audit team also performs an annual corporate-wide audit of the overall BSA/AML compliance program.

All of the bank's areas are covered in some manner over a 2-year cycle. The audit plan is set annually, and adjusted as necessary for changes in risk. Targeted audits include detailed transaction testing to validate enhanced due diligence. Findings are reported formally after each audit, along with management's action plan. The audit team follows up on each action plan to ensure the corrective action is implemented. BSA/AML results are reported regularly to the Board of Directors throughout the year, along with an annual summary.

Another bank noted that its internal audit function team has AML subject matter experts who keep updated on changes to the regulations and compliance practices. There are three areas in which this bank's AML program is audited:

1. Corporate Sector Review – this is a review of the AML and sanctions compliance function.
2. Sector Reviews – this includes product reviews. These reviews are conducted out in the field where the products are sold to the customers.
3. Regional Reviews.

Business entities are cycled through the audit process. The cycle may increase depending on the risk level of the business entity. Typically, an entity is cycled every 2 to 3 years for audit purposes; however, entities with an AML component are usually considered to be higher risk and are, therefore, audited more frequently, usually on an annual basis.

Another bank noted that they engage their auditors in many projects, particularly in process and technology changes so that the auditors are not only familiar with these processes and technologies once deployed, but they can make directional recommendations before the bank fully implements any changes.

Issues Raised by the Banks

SAR Sharing

One bank emphasized its strong feelings that geography should not be an inhibitor to SAR sharing with affiliates. This bank has staff located in different parts of the world, but noted that they are all employees of the bank. Even if these employees are overseas, the bank felt they should be able to view/share a SAR filed in the United States. The bank emphasized the ability to share the SAR should be dependent on the need to know the information, not one's geographical location.

Another bank brought up the difficulties in the current domestic SAR sharing process and its frustrations with having to utilize the 314(b) process to share with affiliates. At the time of the meeting, FinCEN stated that guidance was in development that would address the issue of SAR sharing with domestic affiliates. The bank was very receptive to FinCEN's effort to address this issue.

In March 2009, FinCEN proposed amendments to our SAR regulations to expand the confidentiality of SAR information, along with a parallel proposed guidance document on "SAR sharing" to ensure that the appropriate parties, but only those parties, have access to SARs.[37] Among other things, these proposals clarify the responsibilities of both government employees and financial institutions to protect this information. Law enforcement investigators should receive higher caliber information from SARs, and corporate affiliates are able to share information with each other about dangerous customers who can harm the institution's bottom line or reputation.

In June 2009, FinCEN Director James H. Freis, Jr., issued a statement following the annual plenary meeting of the Egmont Group, held in Doha, Qatar. The Egmont Group is an international network of financial intelligence units from more than 100 jurisdictions. The Director's statement noted the guidance that FinCEN has proposed to facilitate SAR sharing among domestic affiliates is a first step to raise awareness and remove some of the impediments that are preventing nations across the globe from fulfilling some of the Financial Action Task Force principles designed to protect corporations, institutions, and financial markets. The G-20 leaders have also noted the need to promote greater sharing of AML-CFT information across jurisdictions.[38]

---

37. See http://www.fincen.gov/news_room/nr/pdf/20090303.pdf.

38. See http://www.g20.org/Documents/g20_wg2_010409.pdf, Key Message #38

Regulatory Observations

The banks expressed consistent high praise for the Federal Financial Institutions Examination Council (FFIEC) Exam Manual and stated that it has become a very helpful resource and provided helpful insight into regulatory expectations as well as promoting consistency within the examination process.

Several banks commented generally on examination issues and noted that they have observed a phenomenon of expanding expectations and what they see as a constant "raising of the bar." While the legal standard is not being raised, banks feel that the more you do, the more is asked of you, and that whenever another large bank implements a new system or procedure, other large banks are expected to implement those same systems and procedures as well, even though those procedures may be above and beyond what the bank views as appropriate based on a risk assessment.

Information Technology

When discussing budgetary issues, many of the banks stated that their principal cost driver is the technology infrastructure that needs to be in place to run their AML program.

All of the banks discussed information technology (IT) challenges, particularly relating to transaction monitoring and integration of systems, most notably during mergers. One bank noted the expectation for continuous improvement and the need to upgrade software often in order to meet changing regulatory expectations. The bank noted that this is expensive in time, resources, and cost. It also diverts attention from system performance, analysis of false positives, and other configurations that may have an impact. The bank also has been impacted by the need to change system requirements mid-project due to evolving regulatory needs, resulting in additional expense and time and in direct conflict with project management framework.

Several banks also noted how difficult it is to implement a cohesive IT approach across their enterprises, as LOBs use different systems.

Civil Money Penalties

Several of the banks noted that following the announcement of a FinCEN civil money penalty, bank staff would closely analyze the case and felt that the public documents provided insight as to how the penalties were justified.

Banks also expressed concern that while a non-systemic event will be handled as such by regulators, it may result in a prosecution by the Department of Justice (DOJ). There is a desire for regulators and DOJ to develop consistency in how these events are handled across agencies. In these discussions, FinCEN reiterated that it continues to work closely with DOJ in coordinating enforcement actions.

In October 2008, FinCEN Director Freis focused his speech before the American Bar Association/American Bankers Association Money Laundering Enforcement Conference on this specific issue -- the objectives and conduct of BSA enforcement -- emphasizing the importance of collaboration with DOJ and the appropriate Federal banking agency when any potential concurrent civil or criminal action against a financial institution is contemplated.[39]

The 30-Day Clock

Two banks noted that a significant amount of time was dedicated to their views on the 30-day SAR filing period. The banks maintained that there is no definitive judicial or regulatory decision that provides clear guidance as to when the statutory 30-day SAR filing period begins to run, nor was it clarified in the most recent exam manual when a transaction should be determined to be suspicious.

For example, the banks felt that the regulations require a SAR to be filed "no later than 30 calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing the SAR" and view this as a completely subjective approach to risk assessment. Moreover, they maintain that most of the transactions, events, or referrals that are or can be investigated for purposes of possible suspicious activity prove to be unworthy of investigation or filing.

The banks suggested a more practical approach for regulating the SAR filing that recognizes the need to manage events and review cases in order to determine whether a SAR should be filed, and then a 30-day period to prepare and file the SAR. Another suggestion they offer is to implement a 60-day or even 90-day time frame from receipt of a referral or generation of an alert to the date the SAR should be filed.

FinCEN explained in the meetings that the 30-day period was meant to balance appropriate review within a bank with getting timely information to law enforcement to carry out fuller investigations where appropriate. Building upon the feedback from banks, FinCEN issued guidance on the 30-day filing requirement in its October 2008 issue of the *SAR Activity Review: Trends, Tips and Issues*.[40]

---

39. See http://www.fincen.gov/news_room/speech/pdf/20081020.pdf

40. See http://www.fincen.gov/news_room/rp/files/sar_tti_14.pdf

SAR Acknowledgements

One bank requested the addition of acknowledgements to its SAR BSA E-filings. The ability to receive an acknowledgement file will allow the bank to verify their submissions were loaded properly into the FinCEN internal database and would also provide their regulators with additional verification of their submissions. The bank indicated they would need approximately 6 months to update their systems to process a SAR acknowledgement.

On September 12, 2009, FinCEN implemented a system to provide an acknowledgement to financial institutions when they file a SAR electronically through the BSA E-filing system.[41] Specifically, the SAR acknowledgement will provide financial institutions with receipt of submission by providing acknowledgement files containing Document Control Numbers (DCNs) generated by the current system of record, WebCBRS.

To allow time to modify their own systems and processes to accept the DCNs, BSA E-filing users will be able to self-enroll to receive acknowledgements by form type when they are ready to receive and process the acknowledgement files. The acknowledgement files will also be available to filers in both the legacy flat file and as an XML file. When self-enrolling, the user can select to receive one or both types of acknowledgement files. In December 2009, FinCEN will implement SAR Validations, which will allow the BSA E-filing system to validate SAR documents and provide filers with feedback on the technical quality of their submissions.

Compliance Challenges

One bank commented on a new State privacy law which expands the scope of data covered. The law requires the bank to limit exposure to personal information. It limits the amount of personal information collected to only that information required for a business purpose, limits access to only those required to know such information, limits the use of the information to the purpose intended, and requires the secure disposal of the information when no longer needed. The bank is permitted to keep the information as long as it is legally required to do so (such as by the BSA).

41. See http://www.fincen.gov/whatsnew/html/20090826.html

Standardized Country Risk Ratings

One bank stated that it would like to see the government produce standardized country risk rankings that all banks can use for their AML monitoring. FinCEN noted that while there is no comprehensive U.S. Government country ranking, banks should consider a variety of factors in evaluating geographic risk and may utilize public documents such as the International Narcotics Control Strategy Report (INCSR), or information on deficiencies in the anti-money laundering and counter-terrorist financing (CFT) regimes globally highlighted by the Financial Action Task Force, to assist them in determining levels of risk.[42]

Requests for Guidance

During the meetings, FinCEN asked the banks for feedback on the value of FinCEN's products to help us determine what is useful to our financial industry partners or where additional guidance might be helpful. In these discussions, the banks expressed positive reactions to FinCEN's new Web site design, as well as FinCEN's Regulatory Helpline, which provides a forum for financial institutions to ask FinCEN questions relating to BSA requirements.

Banks raised a variety of issues where additional guidance was requested, specifically emerging trends and patterns, and transaction monitoring more focused on larger institutions and certain geographic areas.

One bank indicated they would like to see an update to the SAR narrative guidance that was published by FinCEN several years ago, such as what information banks should be including in their SAR filings. The bank would also like additional guidance on the ongoing activity date range issue. The bank stated that while there does appear to be clear guidance on the issue, it has been interpreted differently between the agencies. FinCEN is currently discussing related issues within the BSAAG Law Enforcement Subcommittee.

42. See http://www.state.gov/p/inl/rls/nrcrpt/2009/index.htm and http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-a004.pdf

Conclusion

Universally, the BSA/AML compliance teams within each of the banks participating in the outreach initiative expressed appreciation that FinCEN is committed to learning about their programs and challenges. In fact, one bank expressed their interest in having this type of outreach occur on an ongoing basis. There was an open and earnest exchange of information and ideas, and FinCEN will take into close consideration the feedback and ideas presented by the banks.

For 2009, FinCEN is conducting similar outreach to some of the largest money services businesses, and will explore additional outreach opportunities with other industry groups going forward.


FINANCIAL CRIMES
ENFORCEMENT NETWORK