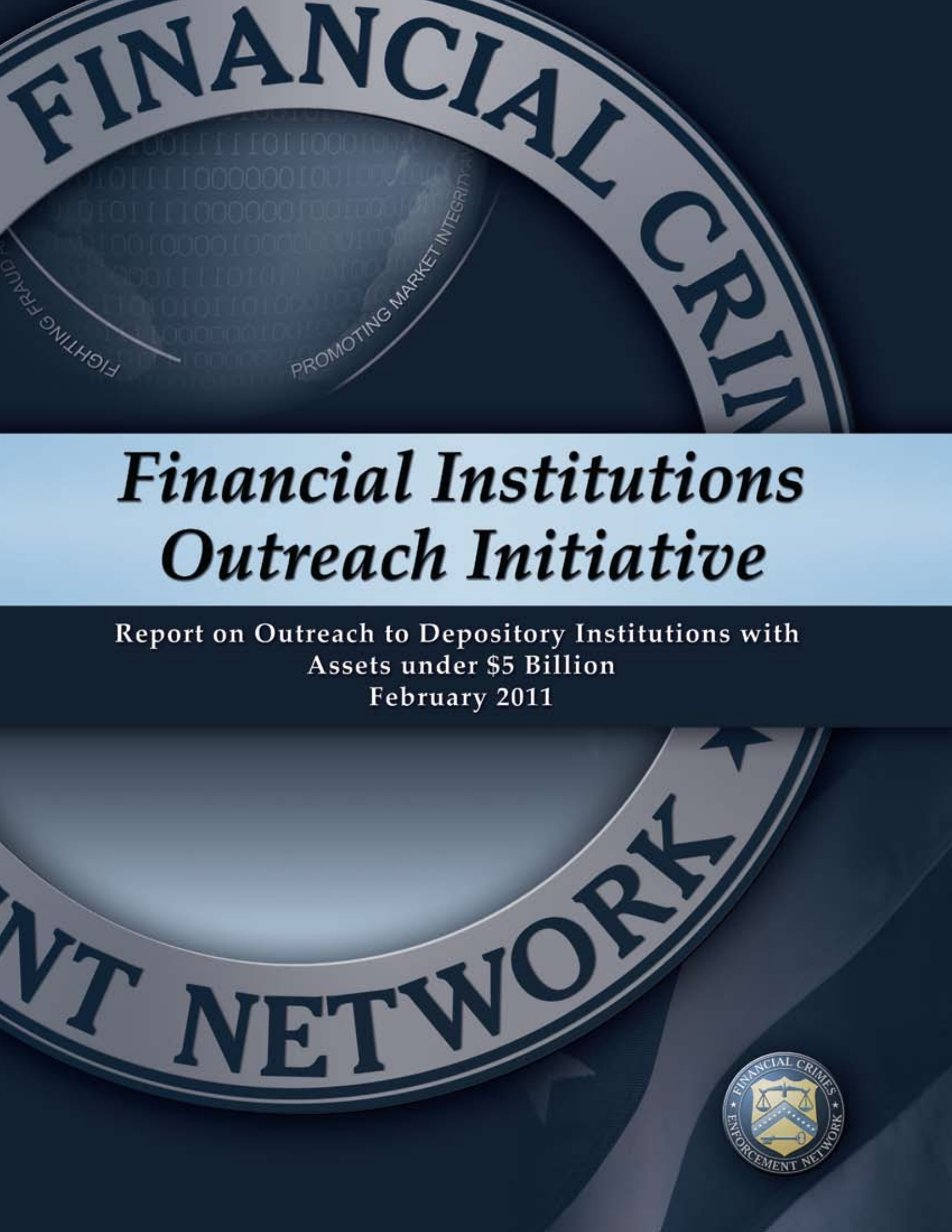

Financial Institutions Outreach Initiative

Report on Outreach to Depository Institutions with Assets under $5 Billion
February 2011

Financial Institutions Outreach Initiative

Report on Outreach to Depository Institutions with Assets under $5 Billion

February 2011

Table of Contents

Executive Summary

The Financial Crimes Enforcement Network (FinCEN) is engaged in a variety of initiatives to ensure that the regulatory component of our mission as administrator of the Bank Secrecy Act (BSA) is carried out in the most efficient and effective manner possible. FinCEN is unique among the Federal banking regulators, as we do not directly examine for compliance and, therefore, do not have the same kind of day-to-day interaction as do other regulators with the financial institutions that fall under our purview. This outreach thus provides additional insights to 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 aids in carrying out 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.[1] In 2009, FinCEN conducted outreach to some of the nation's largest money services businesses.[2] For 2010, FinCEN announced its interest in conducting outreach with representatives from the nation's depository institutions with assets under $5 billion.[3]

The purpose of this report is to share information FinCEN gathered in 2010 during this phase of outreach. 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.

Many depository institutions reported that, as compared to only a few years ago, they had a much better appreciation for regulatory requirements and were largely comfortable with the policies and procedures that they had developed and implemented to meet regulatory obligations such as reporting, and to manage the risks unique to their respective institutions. The institutions attributed this in part to more FinCEN publications and guidance, and, in particular, the availability since 2005 of the FFIEC BSA/AML Examination Manual, which helped make compliance expectations more transparent and consistent across regulators and examiners.

1. See http://www.fincen.gov/news_room/rp/reports/pdf/Bank_Report.pdf
2. See http://www.fincen.gov/pdf/Financial%20Inst%20Outreach%20Init%20MSB_final.pdf
3. See http://www.fincen.gov/news_room/nr/pdf/20091013a.pdf

While information technology posed challenges to a number of institutions, they similarly explained that better integration of older systems previously dedicated to separate lines of business, together with more systematically collecting and retaining information with respect to their customers, continued to facilitate better service to their customers, as well as meeting compliance requirements.

A few institutions affirmed that there was no additional information collected to comply with FinCEN's regulations that the institutions would not already collect to serve the needs of their business lines. Those institutions that described how they risk-rated their customers noted that only a very small portion (under one percent) of their customers were self-identified as in the institution's highest risk category, for which the institution's policy called for additional procedures or levels of scrutiny as risk mitigation measures. Every institution appeared to have an even smaller number of idiosyncratic customers or members that required a disproportionate amount of time and attention to meet both the customer's needs as well as the institution's compliance obligations.

In smaller institutions, BSA officers and compliance professionals often had multiple responsibilities. Regardless of the organizational structure, they stressed the importance of a close working relationship with management and lines of business, and a keen understanding of the products and services provided. Particularly important to them was the close involvement of compliance professionals in the development of new products and services, for example, offering remote deposit capture (RDC) services.

FinCEN learned that depository institutions are increasingly integrating their anti-fraud and anti-money laundering efforts. For instance, some institutions, in combining these functions organizationally, are even renaming this function as the "financial crime department" within their institution. And even in cases where the two functions may not be housed in the same department, there continues to be an increasing understanding of the importance of close collaboration on fraud and money laundering issues.

FinCEN also consistently heard of active interest in and support for BSA efforts at the institution's board of directors level. While board member awareness of, and appreciation for, BSA/AML regulations has grown in recent years, board members could benefit from more consistent awareness of the significant information made available by FinCEN and law enforcement on the use and usefulness of BSA filings from financial institutions. BSA officers and related professionals had familiarity with such information, but requested FinCEN assistance in helping them communicate this to board members and senior management.

Significant topics of discussion concerned the experience of the depository institutions in fulfilling the requirements to file Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs). FinCEN received positive feedback with respect to its BSA E-Filing System. As compared to traditional filing through paper forms, electronically filing BSA information increases the timeliness of data availability, reduces the cost of paper processing, streamlines BSA report submissions, improves both data quality and data security, and provides users with enhanced audit and recordkeeping capabilities.

With respect to SARs, institutions stressed that they filed reports only when warranted. Institutions emphasized that they took their obligations to file SARs seriously and sought guidance on how to make SARs more useful to law enforcement. In response, FinCEN emphasized the importance of the SAR narrative, where the banker should use his or her experience and good instincts to explain the basis for suspicion. While institutions differed as to whether SARs they filed were initially generated by automated transaction monitoring systems or from referrals from front-line personnel such as tellers, they consistently stressed the importance of, and positive results from, training and empowering their front-line personnel to identify and report suspicious activity. While IT systems were a critical tool to help meet their obligations, compliance officers underscored the importance of having sufficient, well-trained personnel to review and evaluate computer-generated reports, as well as act upon them.

Regarding CTRs, institutions again noted that they had largely developed procedures to facilitate compliance with this longstanding reporting requirement. FinCEN was encouraged to hear positive feedback regarding its rule changes effective in 2009 that broadened the ability of depository institutions to exempt categories of customers from the requirement to file CTRs, in particular by shortening the timeframe (from 12 months down to 2 months) before exempting new customers. A number of institutions were utilizing, and expressed appreciation for, a brochure provided by FinCEN designed to educate customers on the institution's obligation to file CTRs.

Institutions also consistently described situations of specific individual customers or members who preferred to deal in large amounts of cash, often observing that the customer purported not to want the government to know about his or her business. Many examples were provided with respect to customers who knowingly structured transactions in an attempt to avoid reporting requirements. With respect to longstanding customers where the institution did not believe the customer otherwise was involved in criminal activity, institutions expressed some reticence in filing SARs. (Note that the institutions participating in the outreach have filed a comparatively higher percentage of SARs that report structuring, when compared with depository

institutions overall). They also inquired about repeated filings on specific customers and review of ongoing activity. FinCEN explained how FinCEN and law enforcement use CTRs and SARs to seek out patterns of activity that may involve multiple financial institutions or significant amounts of money over time, and that these reports can help identify possible criminal activity, as well as tax evasion, that merit further investigation, and in some cases, prosecution.

More broadly, many BSA officers had contact or even good relations with some members of Federal, State, and/or local law enforcement. A number participated in regional roundtable meetings with law enforcement, while others had positive experience supporting law enforcement investigations, including when law enforcement sought more information underlying a reported SAR. The institutions would appreciate additional information and feedback from FinCEN and law enforcement as to the use and usefulness of reported information.

Institutions expressed comfort with their procedures and ability to promptly search and respond to FinCEN inquiries under the 314(a) system with respect to investigations of terrorist financing and significant money laundering. FinCEN notes that in the preceding 5- year period, approximately 64 percent of positive matches have come from institutions with assets under $5 billion. In addition, of the total number of institutions that have responded to 314(a) requests over this 5-year period, FinCEN estimates that 92 percent of these institutions have assets under $5 billion, reflecting the significant role smaller institutions play in the 314(a) process, and the high value of information these institutions are providing to law enforcement.

Institutions were comparatively less familiar with the 314(b) process under which, upon providing notice to FinCEN, financial institutions may avail themselves of a statutory safe harbor from civil liability for sharing information with one another to identify and report activities, including fraud, that they suspect may involve possible terrorist activity or money laundering. At the town hall meetings in particular, institutions participating in the 314(b) program strongly urged their counterparts to similarly engage in order to better protect their respective financial institutions.

More generally, institutions commented positively on FinCEN's Web site, guidance, and publications. Many institutions used this information to benchmark their institution's experience and to educate themselves and others throughout their institutions as to risks of criminal behavior they wish to avoid. A few institutions cautioned that sometimes they feel that there is too much information, and they rely on other sources, such as industry associations, to help keep them abreast of developments.

Multiple institutions spoke of seeing a troubling increase in elder financial exploitation, which is victimizing their customers. Those institutions take a proactive role in trying to assist their customers and work with appropriate State authorities to combat this problem.

Unique to credit unions, issues surrounding shared branching, particularly the risks and responsibilities from a compliance perspective, were discussed. In addition, concerns with difficulties in expelling credit union members were also raised. Participating credit unions consistently noted how their original membership base had grown and become more varied, including geographically, with a notable amount of international transactions among the credit unions.

FinCEN would like to thank all the institutions that volunteered to participate in the outreach program, including the institutions with which FinCEN was unable to meet.

Introduction and Nature of Meetings

In an October 2009 speech before the American Bankers Association/American Bar Association's Money Laundering Enforcement Conference, FinCEN Director James H. Freis, Jr. announced that FinCEN was interested in meeting with representatives from some of the nation's depository institutions with assets under $5 billion to hear about how these institutions implement their anti-money laundering programs, including unique challenges faced by institutions across this asset class and where additional guidance from FinCEN could be helpful.[4] This engagement would build upon FinCEN's previous outreach with representatives from a variety of industries that fall under BSA regulatory requirements, beginning in 2008 with large depository institutions,[5] followed in 2009 with some of the nation's largest money services businesses.[6]

Due to the large number of depository institutions with assets under $5 billion, FinCEN invited depository institutions to express their interest by applying to participate in this voluntary outreach. Interested depository institutions within this asset class were requested to contact FinCEN via e-mail by November 30, 2009. Based on the number of financial institutions responding, FinCEN would then select a cross-section of financial institutions to ensure our outreach would take place with a diverse representation of depository institutions with assets under $5 billion.

FinCEN received expressions of interest from 106 depository institutions in 34 states, with assets ranging from $14 million to $4.8 billion. Of the 106 depository institutions, 27 were credit unions from 17 states. Additional institutions and depository institution associations continued to express interest over the course of the year as awareness spread of FinCEN's outreach efforts.

While FinCEN asked volunteers whether they would like FinCEN to visit them or to come to FinCEN's offices, the primary focus was on opportunities to FinCEN representatives to learn about the depository institutions at their own place of business.

Based on a variety of factors, including asset size, charter type, and geographic location, between January and November 2010, FinCEN ultimately met with 18 institutions in 13 states. The asset size of the 18 institutions FinCEN met with during the course of the outreach ranged from $39 million to $4.8 billion. More than half of

4. See http://www.fincen.gov/news_room/speech/pdf/20091013.pdf
5. See http://www.fincen.gov/news_room/rp/reports/pdf/Bank_Report.pdf
6. See http://www.fincen.gov/pdf/Financial%20Inst%20Outreach%20Init%20MSB_final.pdf

the institutions (10 of the 18) had assets under $1 billion, with the majority of these (8 of the 10) having assets under $600 million. Of the remaining 8 institutions, 4 had assets between $1-2 billion, and 4 had assets ranging from $2 - $4.8 billion.

Geographically, these institutions ranged from inner city to suburban to rural agricultural areas (at least a 30-minute drive to the nearest competitor). Most were stand-alone institutions. A few had single bank, bank holding companies. A few of the depository institutions visited were part of bank holding company structures with more than one bank, thrift or trust company, as well as other affiliates, including investment advisors, insurance brokers, and real estate management companies. The charters of the participating financial institutions included State chartered banks (some of which were members of the Federal Reserve System), national banks, and Federal and State chartered credit unions.

The institutions were primarily funded through deposits from their customers or members. Many institutions described a large portion of their customer base as small businesses, providing those businesses with loans and other services, while also servicing the needs of the business owners or professionals. Many of the institutions were direct residential mortgage lenders; others had only secondary exposure such as through home equity lines of credit. Many of the institutions commented that they did not suffer great losses due to the recent downturn in the economy and housing market, because they employ conservative lending practices. Almost all participants commented on the direct and indirect impacts of the decline in home values on their business and the local economy and were very interested in discussing FinCEN's ongoing work to combat all kinds of mortgage fraud.[7]

Nearly all institutions - regardless of asset size or location across the country - had some international business, usually in the form of wire transfer activity related to imports or exports, customers or members who had established relationships locally and later moved overseas, or in processing remittances. Almost all institutions processed domestic and international wire transfers through a larger, domestic depository institution.

Wherever possible, FinCEN sought to organize such visits in combination with other business travel to the region, and usually, distinct from the individual depository institution visits, met with Federal, State, and local law enforcement and regulatory agencies in the area to discuss FinCEN's ongoing support for the work of those agencies. These visits also provided useful background information as to the regional business environment that added perspective to the visits to the individual depository institutions.

7. More information can be found at http://www.fincen.gov/mortgagefraud.html

The visits were hosted generally by the BSA officers, often in the institution's boardroom. In about half of the visits the depository institution's President/CEO/ Chairman of the Board met with the FinCEN representatives. Other participants varied from institution to institution, but most often involved others who worked closely with the BSA officer including others in compliance or fraud investigations functions, risk managers, auditors (including members of the audit committee of the board of directors), legal counsel, and business lines. Some of the institutions offered a tour of the facilities, such as the vault and teller areas, and introduced the FinCEN visitors to staff throughout the depository institution.

The meetings were informal and interactive, with the discussion driven by the preferences and suggestions of the host depository institution. Many of the institution staff members commented that they had never met or spoken with a FinCEN representative, and they appreciated the opportunity to learn more about FinCEN firsthand.

Throughout the discussions, the depository institutions illustrated their questions and explanations with actual examples of products or services; customer activities; issues that had arisen in the context of a specific transaction between a customer and a teller, upon review of transactions or generated reports, or raised by a board member, auditor, or examiner; often showing copies of documentation, reports, computer screenshots, or statistics to illustrate the point.

All of the BSA officers were prepared with specific questions they wished to ask of FinCEN. Most of these could be addressed by referral to publicly available reference material or a discussion of the purposes behind particular regulatory requirements. Every institution has a very small number of idiosyncratic customers or members that require a judgment call on the basis of the individual facts and circumstances as to how the institution serves that customer's needs as well as meets its compliance obligations (and, hence, these customers generally occupied a disproportionate amount of the institution's compliance efforts). It was not the purpose of the outreach visits to address — and, if requested, FinCEN declined to opine on — whether a specific approach was appropriate. (FinCEN did raise awareness, however, among the depository institutions of the availability of our Regulatory Helpline and steps as set forth in our regulations to obtain an administrative ruling should they wish to pursue a specific issue.)

FinCEN staff also held town hall style meetings in both Chicago, Illinois and Eden Prairie, Minnesota (kindly hosted by the Minnesota Bankers Association at their headquarters). Based on the number of institutions that expressed an interest in

meeting at FinCEN's offices, FinCEN invited a number of them to participate in two town hall meetings (one ultimately attended by five banks and the other by six credit unions) hosted at FinCEN's offices in suburban Washington, D.C. Of the 11 institutions that visited FinCEN's offices, five had assets under $1 billion. The remaining six institutions had assets ranging from $1.2 – $2.5 billion.

More than 50 institutions participated in these four town hall meetings. Similar to the outreach visits, these half-day town hall meetings did not have a set agenda, but rather involved active back-and-forth discussions touching upon a range of issues of interest to the participants. Most notably, the participants in the town halls openly shared experiences and views, and asked questions of one another.

While the number of depository institutions with which FinCEN met over the year represents a small sample of those with assets under $5 billion, even within this diverse sample of depository institutions there were more common themes than institution-specific issues, as relayed in this report.

Bank Secrecy Act/Anti-Money Laundering Program

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.[8] The BSA has been amended on several occasions, most significantly by the Money Laundering Control Act (MLCA) of 1986[9] and Title III of the USA PATRIOT Act of 2001.[10]

The BSA authorizes the Secretary of the Treasury, *inter alia*, to issue regulations requiring financial institutions to keep certain records and file certain reports,[11] and to implement anti-money laundering programs and compliance procedures to guard against money laundering.[12] The authority of the Secretary to administer the BSA has been delegated to the Director of FinCEN.[13] 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."[14]

While some requirements in the BSA and its implementing regulations apply to individuals, most of the BSA's statutory and regulatory requirements apply to financial institutions.[15] 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.

---

8. 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.
9. See Public Law 99-57 and 18 U.S.C §§ 1956 and 1957.
10. See Title III of Public Law 107-56, available at http://www.fincen.gov/statutes_regs/patriot/
11. See 31 U.S.C. §§ 5313 and 5318(g).
12. See 31 U.S.C. § 5318(h).
13. See Treasury Order 180-01 (Sept. 26, 2002).
14. See 31 U.S.C. § 5311.
15. See 31 U.S.C. § 5312(a)(2); 31 CFR § 103.11(n) (future 31 CFR § 1010.100(t)).

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.[16]

BSA/AML Policy Documents

Many of the institutions discussed their internal BSA/AML policy documents. A number of different sources had been employed in developing these documents: a few compliance officers emphasized that they personally had drafted the documents; others had relied heavily upon external consultants retained specifically to advise on BSA/AML policies; a number relied on industry associations or subscription sources for template documents; and many relied upon a combination of the foregoing. In essentially all institutions participating in the outreach program, the current policies have been in place for a number of years (often since shortly after the current BSA officer assumed that position and reviewed and revised as appropriate the institution's policies and procedures).

More recently, changes to the BSA/AML policy documents have been made primarily to address the development of new product lines or services (for example, related to offering customers remote deposit capture), in which case the compliance officer would seek out appropriate new information to update the institution's policies. In a few instances, changes had been made in recent years to implement suggestions from those conducting an independent audit of the AML program or in response to questions from examiners. Numerous compliance officers mentioned that the documents serve as a useful resource not only among those responsible for compliance, but also to others throughout the institution to whom they are made available.

For instance, one institution internally publishes an AML Risk Assessment, which is updated on an annual basis in response to changes in the institution's products and business units, or new regulatory requirements. The institution also internally publishes a document called the BSA/AML Overview, which summarizes the institution's AML framework. In addition, the institution internally publishes an AML Program Policy, which details how the institution's compliance program satisfies the necessary BSA regulatory requirements (i.e., the "four pillars"). The AML Program Policy document is annually reviewed and approved by the board of directors.

16. See 31 U.S.C. § 5318(h).

Key Employees

The BSA officer at many of the institutions visited had many years of experience at their institution, often having worked in other lines of business (a few having begun a career as a teller or customer service representative) or compliance areas before assuming responsibilities as BSA officer; a few had previously worked at other, generally larger banks. All BSA officers stressed the importance to their compliance responsibilities of close relationships, understanding, and communications with management, other parts of the institution, and those working in branch offices.

In many cases, particularly with the smallest institutions, the institution's BSA officer wore multiple hats within the institution. Most commonly, the BSA officer also handled security or fraud at the institution, either personally or by supervising the person(s) responsible for security and/or fraud. In one case, in addition to BSA responsibilities, the BSA officer at an institution was also the head of the institution's HR and Payroll departments.

One BSA officer at a $40 million asset institution indicated that the person serves as the compliance officer for two different institutions, working part-time for each. For institutions with over $1 billion in assets, most had a dedicated BSA officer.

At some institutions, the BSA function is handled by one individual, and this is the individual's exclusive responsibility. Several BSA officers in this situation noted that their management within the institution supported their efforts to obtain Information Technology (IT) systems to assist in monitoring transactions.

One institution noted that it has four employees within the Compliance Department and approximately half of their time is spent on AML/BSA issues. The institution also relies heavily on front-line staff and internal reports for suspicious activity monitoring. Compliance reports directly to the institution's Audit Committee. One of the board members in attendance noted that the goal of the Audit Committee is to provide support to Compliance and ensure this role is highlighted within the institution. The institution is also careful to involve the Risk Management Department in the development of new product lines from an early stage to avoid running afoul of regulatory requirements.

Another institution has eight members of its Compliance Department that handle BSA-related matters. Employee retention in the Compliance Department is higher than other departments within the institution.

Another institution noted that it has a risk committee composed of corporate counsel, key executives, two inside Directors, compliance, Human Resources, key operational personnel, the CFO, and the marketing department. The risk committee makes all decisions on business lines to work with.

Board of Directors

There was very consistent feedback regarding the involvement of the institutions' board of directors. Most of the institutions visited explained that they had long-term (a decade or more) continuity of many board members, in many cases including representatives of the controlling shareholders. They described an evolution of the board members' understanding of the purposes and requirements of AML/BSA regulations, accompanied by commitment to and support for compliance. The BSA officers provided an overview of practices for briefing board members (both regularly such as in the course of monthly board meetings and on an annual basis) as well as explaining the policies that were approved by the board.

Several institutions characterized their board of directors as "active" in oversight and audit activities and indicated that there is a strong commitment by the board to support a culture of compliance. One institution explained that the Director of Compliance provides a monthly memo to the full board to provide information on the SARs filed by the institution during that month. An annual presentation is also provided to the board on the institution's AML program, risk assessment, wire transfer activity, and any new products. A monthly "regulatory update" is also provided to the board, which is a synopsis of regulatory developments and their potential impact on the institution.

The BSA/AML Officer provides the institution's Executive Corporate Governance Committee with monthly and quarterly reports of all BSA-related matters. The reports include information on SARs and investigations into suspicious activity, though they omit the names of SAR subjects. The issue of how to inform the board members appropriately with respect to SARs while protecting confidentiality and avoiding tipping off the subject of the SAR was a common question or concern raised by compliance officers. In some cases, this was put in context of explaining the prominence of board members, including executive members, in the community served, meaning that a board member might know the subject of the SAR personally.

This led many institutions to conclude that it was a better practice not to include the names of the SAR subject or other identifiers in the information presented to the board, whether orally or in written briefing materials (especially read-ahead materials).

Alternative approaches involve limiting the sharing of detailed information to a subset of board members, such as the audit committee, or to executive members. A few institutions noted that executive board members also served in other capacities such as on an internal compliance oversight committee that oversaw the BSA officer's decisions on filing SARs or evaluating customers; hence, they believed that the same level of customer detail need not be shared with non-executive board members.

Additionally, several institutions understood that the meeting minutes of board meetings are sometimes subject to discovery in judicial and other proceedings, and therefore, any disclosure of the names of SAR subjects in board meetings could compromise SAR confidentiality.

Board members (some of which participated in the outreach meetings themselves) showed strong interest in trends with respect to the reasons for which SARs were filed, with a particular focus on cases of fraud or other activity for which the institution suffered a loss. It was reported in multiple situations that board members could be expected to ask more details about what has been done to prevent recurrences of activities of concern, in particular to prevent future losses to the institutions.

One institution's report to the board also includes information on: losses sustained by the institution as a result of fraud; wire activity; trends in fraud and suspicious activity; and controls implemented by the Risk Management Department to prevent further fraud and losses. Finally, the reports include a one-year look-back at BSA-related matters for trend analysis and comparison purposes. The BSA/AML Officer indicated that the board is highly supportive of the Risk Management Department's AML efforts. Other institutions had similar practices of reporting to the board of directors.

Many of the BSA officers personally conducted annual training for board members on BSA matters, while others supplemented such training through general management courses for board members, or specific input from BSA consultants. A number of the compliance officers mentioned that they included case examples or statistics from FinCEN publications such as the *SAR Activity Reviews* to put in context the risks or experiences at the particular depository institution.

During our outreach, FinCEN heard feedback from institutions that the board and senior management are generally supportive of BSA compliance efforts, and are more understanding now as compared to a number of years ago of the need for BSA

compliance. Board members and senior management asked many questions and were very interested in hearing from FinCEN representatives about how reports from the financial industry are used to combat financial crimes.

As discussed in greater detail later in this report, throughout these institutions, BSA officers were quite familiar with a range of FinCEN publications and information on the purposes behind the regulatory framework, in particular the uses and usefulness of BSA data, yet they struggled to effectively communicate this information within their institutions. Both compliance and line of business professionals noted that there is an ongoing need for compliance officers to educate management on the range of information available on the value of BSA data. As a result of this feedback, FinCEN published an article in the October 2010 *SAR Activity Review* to provide additional suggestions on how to discuss the value of BSA data with the board of directors.[17]

One institution noted that the FFIEC BSA/AML Examination Manual has succeeded in helping educate the board members as well − making issues less confusing and cumbersome to explain.

Another institution's BSA officer expressed frustration that whenever he approaches management to request additional resources, management asks if a computer system (as distinct from additional personnel) might be able to address the need. The BSA officer explains that while IT systems are helpful for monitoring transactions, you need people to be able to conduct further analysis and follow up on the alerts. In addition, the institution is growing at a fast rate, making it difficult to find an IT solution that works effectively.

The BSA officer followed up with FinCEN after our meeting to indicate that he used some of the information he gained from our discussions at a town hall meeting, particularly about how the BSA data is useful to law enforcement, when meeting with his management again to request additional resources for the institution's compliance efforts. This time, he was able to gain the support of his management for additional positions within his department.

17. See http://www.fincen.gov/news_room/rp/files/sar_tti_18.pdf, p.33

Integration of Anti-Fraud and Anti-Money Laundering Efforts

Many of the institutions indicated that their anti-fraud and AML programs are integrated, or work very closely together. In many instances, both anti-fraud and AML fall under the Compliance department within the institutions.

One institution expressed that it recognizes the benefits of integrating AML and fraud investigatory functions within the same department and that other institutions are increasingly integrating anti-fraud and AML functions together as well. As the institution theorized, small institutions with limited resources seem more willing to recognize that resources spent in one area can support the other. And from a due diligence perspective, the information necessary for the institution to comply with its AML program is often the same information necessary to investigate fraud cases.

Another institution also indicated that fraud investigations are mostly handled within its Compliance department. However, matters involving less than $5,000 are often handled within the Operations department, and credit-related fraud matters are often handled within the Lending department. For example, a customer allegedly used Remote Deposit Capture (RDC) in furtherance of a check-kiting scheme.[18] The Lending department took action by prohibiting the customer's use of RDC. Although some fraud matters are handled outside of the Risk Management Department, the institution's policy is that all institution-wide investigations into suspicious activity are escalated to the Compliance Department.

Also at another institution, Compliance, BSA, and Fraud are all in the same area. The institution's Security department reports through the BSA officer. Audit and Compliance report to the board Audit Committee. BSA used to be under Compliance until 3 years ago. Branch Managers have a dotted line to the Senior Branch Operations Officer so there is improved BSA compliance institution-wide.

18. RDC is discussed in greater detail beginning on p.61 of this report. RDC allows a financial institution to receive digital information from deposit documents captured at remote locations. RDC may allow a customer to scan checks and then transmit the image to the institution for posting and clearing.

Recognizing the importance of integrating anti-fraud and anti-money laundering, one institution noted that some institutions are beginning to rename this grouping the "financial crime department" within the institution. Under this organizational structure, all suspected fraud taking place within the institution is reported to this department. If a SAR is not ultimately filed, a case number is still created so the institution can document why a SAR was not deemed to be necessary. The institution indicated it has not received any push-back from its examiners, who have indicated they are pleased with the process the institution has established.

One institution noted that it formed a Fraud Committee within the past year which is comprised of representatives from Security, Compliance, Retail, Deposit Services, and Operations. The committee meets regularly to discuss new fraud trends and Regulation E claims, and the institution's AML officer noted that it was a good way for different parts of the institution to share information and be more proactive in dealing with customers. Some of the more recent trends the committee has discussed include Craig's List scams and lottery schemes.

One institution acknowledges that anti-fraud and anti-money laundering functions overlap, but they are still handled within separate departments.

Another institution has recognized for quite some time the overlap in functions necessary to investigate fraud and money laundering cases, and has integrated both within the same department for at least 20 years.

Elder Financial Exploitation

In general discussions of current trends that institutions are seeing in the fraud area, a recurring theme heard from the institutions regarded their efforts to combat elder financial exploitation. Multiple depository institutions explained that they view it as consistent with their institutional philosophy of serving their customers to try to help customers protect themselves, noting that these situations go beyond trying to protect the institution from losses or to meet regulatory requirements. A number of institutions provided specific examples where they had advised a customer not to make payment (or declined to process a payment instruction) for what might be a consumer or advance fee scam (such as a "fee" to receive lottery "winnings").[19] The more concerning situations involved those where third parties were seeking to appropriate the elderly person's savings or income streams.

19. See http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf

An institution in the Midwest discussed its ongoing efforts to educate its front-line staff on the warning signs that a customer may be a victim of elder financial exploitation. The institution's aggressive approach stems in part from a case in 2001 where an elderly customer fell victim to a fraudster claiming to be acting in his best interest as an investment advisor, who ultimately stole over $500,000 from the victim.

The institution has developed a Power Point presentation to train its staff on spotting possible elder exploitation. If they suspect a customer is being victimized, in addition to filing a SAR, the institution contacts officials in the local police department as well as state criminal investigators so a welfare check can be performed. The institution also makes a voluntary report to the state's Department of Human Services.

Another institution in the Washington, D.C. area also stated that cases of elderly exploitation were on the increase, but that it is difficult to engage law enforcement in these cases due to competing investigative priorities and limited resources. As a result, the institution spends a great deal of its own time trying to help customers that it suspects might be victims of abuse.

One Philadelphia-area institution stated that it has had good success working with the Philadelphia Corporation for the Aging, who has come in occasionally to speak to its front-line personnel about red flags for which they should be looking.

One California institution noted that California law requires institutions to report elder exploitation to the State of California Adult Protective Services if the victim is 62 years of age or older. When the institution becomes aware of suspected fraud, it reports such cases within 24 hours. The institution reports approximately one such case every 3-6 months.

As a result of the feedback FinCEN received from financial institutions during the outreach initiative on the prevalence of elderly financial exploitation, FinCEN is issuing an Advisory in conjunction with the release of this report that outlines red flags that may assist financial institutions in identifying if their customers are being victimized.[20]

20. See http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf

Check Fraud

FinCEN has been engaged for many years with combating a range of crimes related to fraudulent checks and continues to engage the financial industry in attempts to address these risks together.[21] Concerns over check fraud were also discussed at several institutions. One institution noted that it has seen an increase in the incidents of check fraud (in one month there were nine cases); however the institution feels that the monitoring systems it has in place are catching this activity at an early stage.

Another institution noted that it has seen more attorneys falling victim to check fraud, and the institution was preparing an advisory on the issue to send to its attorney customers. The institution noted that preparing and distributing advisories to customers to alert them to possible fraud is something that is done routinely.

21. See http://www.fincen.gov/news_room/speech/pdf/20101002.pdf

Information Technology Solutions

Similar to FinCEN's findings as part of our outreach to some of the largest banks, FinCEN found that institutions with assets under $5 billion also face technology challenges. With some of the smaller institutions where Compliance staffs can be as few as one person, IT solutions are relied upon quite heavily. However, like the largest banks, the selection of tools, data and intelligence sources, and the extent to which AML operations rely on them for monitoring, are driven by the risks posed by such factors as customers and products, and by the capabilities of the tools.

Whereas some IT investments were considered in part to meet regulatory expectations, more generally IT investments were viewed as part of the overall business strategy to better serve customers and manage risks across multiple business lines. Most of the institutions participating in this outreach had grown organically; a small minority mentioned the more complicated issues arising in integrating various computer systems or data sets in a merger or acquisition context. The discussions of IT issues generally related to two main areas: centralizing access to information about the customer; and the monitoring of customer transactions.

Customer Risk Rating

Several institutions discussed how customers are risk-ranked based on products and services offered, geography, customer type, and account activity. While many depository institutions implemented such risk-ranking methodology in conjunction with IT products offered by vendors (which have developed substantially in recent years), a common emphasis was on the need for each institution to tailor the systems to its own needs, preferences, and risk tolerances. By way of example, with several institutions, only a very small portion (under one percent) of their customers were identified as in the institution's highest risk category, for which the institution's policy called for additional procedures or levels of scrutiny as risk mitigation measures.

In a number of institutions, a distinction was made between collecting information with respect to new customers or relationships, and addressing situations involving longstanding relationships in which customer identification or other relevant information had not been complete. Even where this distinction was made, however, it was stressed that over time the institutions have gradually filled omissions where data had not been previously collected.

Compliance officers and lines of business representatives expressed the importance of collecting information about customers and their needs at the time of entering new business relationships. A number of compliance officers explained the process in which such procedures were developed in years past to meet regulatory needs. That notwithstanding, many characterized the questionnaires that have been developed for establishing new relationships as driven by serving business needs; there were no notable categories of information being collected solely for regulatory purposes. A few institutions nonetheless described examples where new customers questioned the amount of information collected at account opening.

One institution noted that the "new account" form that is used within the institution helps identify high-risk activity. In addition to asking what kind of business the prospective client is engaged in, the institution also asks to see the articles of incorporation and checks to see that the business is an active entity in the state in which it is registered. Some customers are placed on a watch list for 90 days if their business is deemed to be higher risk. Recently, the institution also decided to begin asking more questions about who owns or controls the business and is planning to add this information about beneficial ownership to the account opening form.

One institution risk-rates all of its customers into one of three categories: high, middle, and low risk. Factors in the risk-rating analysis include the customer's nature of business, location, duration of customer relationship, and other factors. High risk customer accounts are reviewed quarterly. Middle risk customer accounts are reviewed annually. Low risk customer accounts are reviewed as needed. Most of the institution's customers are low risk. Monthly reports are also generated and reviewed based in part on customer risk-ratings.

One institution's system automatically profiles customers into one of three risk classifications (high, moderate, or low). The system conducts due diligence based on 90 automated rules with respect to all customers, generating alerts based on account activity. However, the system also enables the institution to input its own rules and thresholds regarding specific customers designated by the institution as suitable for enhanced due diligence. The institution groups customers into the following categories:

- Low-Risk Customers
- Moderate-Risk Customers
- High-Risk Customers

- Credit Card Customers
- Private Banking Customers
- Non-Bank Financial Institutions
- Politically Exposed Persons ("PEPs")[22]
- Customers on Whom a SAR Has Been Filed

At the time of our visit, the institution had approximately 15,000 low-risk customers, close to 900 moderate-risk customers, and approximately 50 high-risk customers. The institution noted that it has one customer who is a member of parliament in another country, and therefore, a PEP. The system retains data for a period of 13 months.

Another institution noted that out of its approximately 16,000 customers, only about 25 were deemed high risk, while yet another estimated that out of approximately 50,000 accounts, an estimated 60-70 were high-risk.

Another institution uses an automated system that assigns a numerical structure to risk rate its customers. The higher the customer's risk rating and the more unusual its transactions, the more likely the customer is to be flagged for suspicious activity. The institution considers factors including the following when risk-rating customers:

- Business accounts are considered riskier than individual accounts.
- Checking accounts are considered riskier than savings accounts.
- Non-local individuals or businesses (especially those from outside the United States) are considered riskier than local entities.
- Accounts that deal with high volumes of cash, wires, or both are considered risky.
- Accounts with multiple SARs are considered high risk (but are not necessarily closed).

22. FinCEN's regulations require financial institutions to identify and apply enhanced due diligence to private banking accounts held by or for the benefit of senior foreign political officials, commonly referred to as Politically Exposed Persons (PEPs). However, the term PEP is not used in FinCEN's regulations and should not be confused with the definition of "senior foreign political figure," which is used in FinCEN's regulations. See 31 U.S.C. § 5318(i)(3); 31 CFR § 103.178(c) (future 31 CFR § 1010.620(c)); and 31 CFR § 103.175(r) (future 31 CFR § 1010.605(p)).

- Some entities, including PEPs, financially exposed persons, MSBs, lottery service providers, and ATM operators are automatically considered high risk.

The institution receives automatic alerts on any activity involving customers deemed high risk.

Another institution noted that it checks some customers against the states' online courts records database to ensure they are not involved in any past criminal activity, or to be aware of when a previous customer has been released from prison so it can ensure they do not attempt additional transactions at the institution.

Transaction Monitoring

Review of reports from transaction monitoring software is a key part of the responsibilities described by BSA officers and other compliance staff, whether on a daily, weekly, or monthly basis. Many described how they were increasingly using technology either to automate the production of certain reports or to better highlight information requiring review and/or further investigation.

One institution discussed its system which assists branch staff in identity verification at account opening. Another system is also used to assist staff in identifying suspicious activity, although the institution indicated it was looking for a new solution in this area. Reports are generated from the institution's core processing system to supplement the current transaction monitoring system and assist in identifying suspicious activity.

One institution with an MSB subsidiary expressed frustration that there is no AML solution for MSBs on the market, as compared to many products available for depository institutions. As a result, the institution needs to manually review reports for its MSB that were developed by its internal IT department. The institution also utilizes a system that helps with cash aggregation for CTR purposes and collects customer information for anyone who has ever used services at its MSB.

This same institution uses one system to monitor check transactions and a different system for all other forms of transaction monitoring. Transactions are processed nightly from tellers, item processing files, and a feed from the institution's wire processors. The system takes one day to return transaction data. The system then generates "alerts" and "cases" directly from the data. However, an alert is generated immediately if the system detects a match on any list provided by the Office of Foreign Assets Control (OFAC).

Another institution noted that it currently receives daily, weekly, and monthly alerts from its transaction monitoring system; the alerts appear in a queue within the system. Alerts that are cleared without a SAR filing are documented in the system. Some of the rules the institution is testing include looking for structuring over a 7-and 30-day period and wire transfer velocity. The institution has different procedures for wire velocity in the $25,000 and $75,000 ranges. The institution is looking purely at dollar volume and velocity and does not focus on geographic risk. The institution is also in the process of testing combined rules, such as wires in/cash out, cash in/cash out, and MSB ACH activity (i.e., cash in/ACH out). These rules can be turned on and off as needed.

One institution recently converted from a manual transaction monitoring system to an automated program. Considerations in choosing a software system included initial purchase price, as well as monthly operating expenses. The purchase price of the automated system was around $200,000, which was more expensive than some systems but it fit the institution's needs and had a lower monthly subscription price than other systems. The price of the automated system is based on the institution's asset size.

It appears that institutions are seeing the value of investing in software to replace or supplement manual reviews, particularly in cases where there are few staff to assist in conducting manual transaction reviews.

Suspicious Activity Reporting

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.[23] 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.[24]

The bank SAR rule requires a bank to report a transaction exceeding $5,000 where the bank knows, suspects, or has reason to suspect that: (i) the transaction involves funds derived from illegal activities or is intended or conducted in order to conceal such funds, as part of a plan to violate or evade any Federal law or regulation, or to avoid any transaction reporting requirement under Federal law or regulation; (ii) the transaction is designed to evade any requirement under the BSA; or (iii) the transaction 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 the available facts.[25]

To protect the confidentiality of these reports, the regulation forbids any filing institution or its personnel from disclosing the existence of a SAR except as defined in the rule. Furthermore, this prohibition extends to any government employee or officer, unless the notification is necessary to fulfill the official duties consistent with Title II of the Bank Secrecy Act.[26]

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.[27]

---

23. See 31 U.S.C. § 5318(g).
24. See 31 CFR §§ 103.15-103.21 (future 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, and 1026.320).
25. See 31 CFR § 103.18 (future 31 CFR § 1020.320).
26. See 31 CFR §§ 103.15-103.21 (future 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, and 1026.320).
27. See 31 U.S.C. § 5318(g)(3).

Procedures

Many of the depository institutions walked through examples of the lifecycle from when the institution becomes aware of unusual activity, through the stages of review or investigation, decisions to file a SAR and the persons involved, and the process of drafting, reviewing, and submitting the SAR to FinCEN. The BSA officer most often played a central role in the SAR filing process, from investigation of potentially suspicious activity, to review and decisions whether to file a SAR, to responsibility for the actual submission to FinCEN. Notably, the BSA officer generally had responsibility for SAR filings even if investigatory processes were undertaken in other areas, for example, in a separate security or fraud office with respect to computer intrusion or suspected identity theft under the responsibility of that other office.

Several institutions noted that SAR Committees are used to make SAR filing determinations. While the make-up of such a committee varies from institution to institution, participation can include representatives from Compliance, Commercial, Wire Transfer, as well as tellers. Another institution indicated that while there is no formal SAR Committee, the BSA Officer will sometimes seek the opinion of others within the institution to help inform the decision of whether or not to file.

According to one institution's Compliance Manual, before filing a SAR, the institution's BSA Officer may meet with the Account Officer to determine if there is a reasonable explanation for activity that may on the surface appear suspicious. If the BSA Officer at this point decides not to submit a SAR, a file will be created and the supporting documentation will be retained along with a memo detailing the decision not to file.

Another institution requires its employees to report any potentially suspicious activity to the Security Officer within one business day. The Security Officer investigates all such cases, and also reviews the institution's automated monitoring systems for potentially suspicious activity. Once an investigation is completed, the Security Officer determines whether the incident meets the SAR reporting requirements. If no SAR is filed, the decision is documented and kept on file for 5 years. If the reporting requirements are met, the Security Officer prepares a draft SAR to be presented to the institution's Executive Security Committee for approval and final action. The institution also has procedures in place to deal with voluntary SAR reporting, as well as filing continuing or amended SARs. Based on all relevant risk factors, the institution may close accounts that show potentially suspicious activity.

The institution mentioned that regulators are often intensely focused on the 30-day time period from detection of suspicious activity to SAR filing. In particular, the institution's investigation into whether certain account activity is consistent with the account-holder's normal behavior may require more than 30 days. The institution requested that FinCEN issue guidance providing institutions with more flexibility in that regard.[28]

Several institutions noted that they provide information on SARs that are filed, typically monthly, to their institution's board of directors and Risk Committee. This includes how many SARs were filed, the dollar amounts involved, and type of transaction activity. The reports provided to the institution's leadership are nondescript without identifying information.

Usefulness to Law Enforcement

A consistent theme of discussion during the outreach meetings was the efforts of depository institutions to understand better the needs of law enforcement and thus how they could make SARs more useful. FinCEN representatives explained the different ways that SARs are used, as tips, to provide identifier information, to determine trends, and as a deterrent to criminal activity.[29]

Some of the institution representatives, particularly outside of the compliance area, had misconceptions about how BSA reports were used. There was nonetheless widespread recognition of increased amounts of information, as compared to a few years ago, made available by FinCEN and law enforcement representatives speaking to the financial industry about SAR usage and usefulness.

Several institutions expressed concern that they never see how SARs and other BSA filings get used by FinCEN and law enforcement. Specifically, institutions asked how FinCEN could process 16 million reports (SARs and CTRs) annually. Institutions also asked whether the large number of filings warrants an increase of the reporting thresholds. FinCEN staff generally provided an overview of how law enforcement and Federal regulators use SARs and other BSA data, and explained that there isn't a one-to-one ratio of SARs filed to criminal convictions.

---

28. See *The SAR Activity Review – Trends, Tips & Issues*, October 2008 found at http://www.fincen.gov/news_room/rp/files/sar_tti_14.pdf. See also http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (page 77); "The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation."

29. See http://www.fincen.gov/news_room/speech/pdf/20070910.pdf and http://www.fincen.gov/news_room/speech/pdf/20080227.pdf

FinCEN staff also explained that the BSA database (particularly CTRs) is a repository of financial transactions information that can serve as a unique investigative resource with respect to cases already under investigation—processes that might be very different from an investigation initiated from a SAR. The BSA database can also be uniquely valuable in terms of helping law enforcement allocate resources where risks are great, and this is a particular area where FinCEN focuses its own analytical resources and expertise to understand the "big picture" of criminal trends and patterns.

One institution had the misperception that a SAR filing will automatically get a customer in trouble even if the underlying activity is probably not illegal. Another institution felt a disincentive to file SARs because the result may be a subpoena from law enforcement for information. FinCEN staff mentioned that an institution would be better off getting a law enforcement subpoena than a story on the front page of the newspaper for failing to report its customer's money laundering activity.

Another institution explained that since the position of "SAR Investigator" is a relatively new career-path in the banking industry, there are very few people with expertise in drafting SAR narratives. FinCEN explained that while it does not provide a SAR narrative template, the most important information to include in the SAR narrative is "who, what, where, when, why, and how" in connection with the suspicious activity. Tables of numbers currently cannot be accommodated by the computer systems and thus should not be included in the SAR narrative (but this functionality is being reviewed as part of FinCEN's ongoing IT modernization, and could be accommodated as early as 2012).

Although institution personnel have attended SAR-related workshops, one institution noted that the guidance in such forums is often too subjective to be useful. The institution indicated that more guidance from FinCEN in the form of case studies would help institutions determine when to file a SAR and what to include in the narrative. FinCEN noted it had published guidance called "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting" to assist financial institutions in providing complete and accurate information in their SARs, particularly the narrative.[30] The institution acknowledged that FinCEN's published guidance on SAR narratives was useful, but suggested that institutions were slow to implement such guidance.

30. See http://www.fincen.gov/statutes_regs/guidance/pdf/SAR_Common_Errors_Web_Posting.pdf

One institution indicated that SAR narratives pose unique challenges. In particular, it is often difficult to know how much information to include in SAR narratives. For example, the institution had a loan customer that began to deposit cash that had a strong odor of pepper. (Pepper is sometimes used by drug smugglers to throw off drug-sniffing dogs.) The Drug Enforcement Administration (DEA) followed up with the institution only after it had filed seven SARs on the customer. Prior to the DEA follow-up, the institution had spent nearly 160 hours on the case, yet was unsure as to whether the SARs it had been filing were beneficial to law enforcement.

Another institution also expressed frustration at not knowing what happens to SARs once they have been filed. Specifically, the institution discussed how it expends substantial resources on investigations of suspicious activity and SAR filing, yet in the absence of seeing the results of such efforts, some of its managers undervalue the BSA compliance function. The institution suggested that it would be helpful if FinCEN could provide a minimal notice to institutions acknowledging that a SAR has been received and forwarded to the appropriate law enforcement agencies.

FinCEN stressed the utility of SARs to law enforcement, even though institutions may not be aware of exactly how SARs fit into an investigation. (Some of the most useful SARs may provide either a single piece of a broader puzzle or sufficient information to an investigator that there is no need to follow up directly with the filing institution.) FinCEN also encouraged the institution to regularly review FinCEN's Web site[31] and publications, such as the *SAR Activity Review, Trends, Tips and Issues*,[32] which include BSA success stories of how SARs and CTRs played an important role in investigative efforts. Additionally, FinCEN is aware that publicizing too much information regarding the utility of SARs may actually provide criminals with tips on money laundering methodologies and law enforcement techniques. FinCEN seeks to balance this consideration with the desire of financial institutions to see actual results from SAR filings.

While it will be discussed later in this report, several institutions noted that they do in fact utilize the information on BSA success stories from FinCEN's Web site and publications to train both front-line employees as well as the board of directors.

A number of institutions raised the term "defensive filings" of SARs, but almost always in the context of assuring FinCEN representatives that their respective institutions did not file SARs other than as appropriate and required. One institution

31. See http://www.fincen.gov/law_enforcement/ss/

32. See http://www.fincen.gov/news_room/rp/sar_case_example.html

emphasized that it does not engage in defensive SAR filing, but sometimes feels pressure to do so from its regulators. For example, in a recent joint State/Federal examination, the two regulators had conflicting views on whether a SAR should have been filed in a particular scenario. Accordingly, the institution now feels compelled to file SARs in similar future scenarios based on the desire to avoid a regulatory citation, rather than on the institution's analysis that the circumstances warrant a SAR.

FinCEN communicated that although institutions often raise the issue of defensive filing, it is FinCEN's experience that while the quality of SARs continues to improve, a number of those reviewed inevitably fail to articulate one or more of the basic who, what, when, where, why, and how questions. That notwithstanding, the vast majority of SARs exhibit activity that appears on its face to be consistent with regulatory requirements and guidance as to what is "suspicious." From the outreach discussions, it appeared that some persons use the term "defensive" to refer to a more cautious approach to the subjective question of what is suspicious, while others incorrectly apply this term to SARs reporting customers who knowingly structure transactions,[33] but the institution has reason to believe that the customer is not engaged in other illegal activity.

Regarding thresholds, one institution noted that it is not concerned with threshold amounts for filing SARs and that some of its filings are for amounts less than $5,000 (e.g., use of another's SSN). To date, the institution has not had anything serious enough to contact law enforcement at the outset, but in the past few years it has noticed increased law enforcement interest in SARs filed. The Internal Revenue Service (IRS) has requested underlying documentation 4 – 5 times. FinCEN noted that this could be an indication that SAR Review Teams[34] in their area were more active.

A number of institutions volunteered that they knew their SARs were being read, because law enforcement had requested the underlying documentation.[35] In another case, the BSA officer explained that although the requesting law enforcement officer had never mentioned a SAR, she received a subpoena for account information with respect to a customer and account that were detailed in a recently filed SAR.

---

33. See 31 U.S.C. § 5324; 31 CFR § 103.18(a)(2)(ii) (future 31 CFR 1020.320(a)(2)(ii)) (requirement to file a SAR for transactions designed to evade reporting requirements under the BSA).

34. SAR Review Teams and related task forces operate in over 100 locations throughout the country, typically coordinated through the U.S. Attorney's Offices, in conjunction with Internal Revenue Service – Criminal Investigation. SAR Review Teams, usually comprised of State, Local, and Federal law enforcement and regulatory authorities in the area, meet on a regular basis to review the SARs filed within their jurisdiction, and coordinate law enforcement investigative follow-up as appropriate.

35. A financial institution must maintain supporting documentation for a SAR and make the documentation available upon request to FinCEN, law enforcement agencies, and certain regulatory authorities, as specified in the regulation See, for example, 31 CFR §§ 103.18(b) and (d) (future 31 CFR §§ 1020.320(b) and (d)).

FinCEN will continue its ongoing efforts to provide feedback on the value of BSA information to financial institutions, and is mindful of depository institutions' interest in receiving more guidance to assist in making SAR filing determinations.

Automated vs. Branch Referrals

While technology plays a key role in alerting institutions to possible suspicious activity, all depository institutions noted the very important role their front-line personnel play in spotting activity that may be suspicious.

According to one institution's records for 2009, it conducted a total of 439 investigations into suspicious activity, resulting in 39 SARs filed. Out of 439 total cases, 167 cases were generated by alerts from tellers; whereas 272 cases were generated by the institution's automated system.

However, the automated system generated more false-positives. Out of 39 total SARs filed, only 4 SARs were initially generated by the automated system. Thirty-five SARs (nearly 90 percent of total SARs filed) were initially generated by alerts from tellers.

Another institution echoed that in most instances transactions are initially flagged as potentially suspicious by front-line employees (e.g., tellers, customer service representatives). Examples including hearing a customer say he or she needs to take cash out of a safe deposit box, customers saying they do not want a CTR filed, and seeing structured cashier checks. The tellers and customer base are stable so they know what transactions should look like and what is out of place. Front-line personnel notify the BSA Officer of the situation by e-mail, who then makes a SAR determination. Employees are not told of decisions to file a SAR.

One institution noted that approximately 20 percent of the SARs it ultimately files come directly from branch referrals. Another institution indicated that approximately 50 percent of its SARs originate from branch referrals, with the other 50 percent coming from the review of reports and transaction monitoring.

In terms of monitoring, one institution noted that customer accounts are monitored according to their established activity pattern and business accounts are also monitored to make sure the activity is what would be expected for their line of business. For example, the institution indicated that ATM operators are scrutinized to determine whether they are withdrawing more or less cash than they usually do, and the institution also checks to make sure the activity taking place in the account makes sense for an ATM operator.

One smaller institution noted that it currently outsources its transaction monitoring, as it does not yet have the capacity in-house to perform the monitoring itself. Account information is provided on a daily basis to the company, which reviews approximately 300-350 alerts each month.

When asked about identifying suspicious wire transfers, one institution indicated that unusual wires are fairly easy to spot, even from a manual transaction review. This is because the institution processes a relatively small number of wires (an average of 80 per day) and also because most of the large wires sent from the institution are originated by local governments and title companies, which are considered by the institution to be very low risk customers. The institution indicated any unusual large wires from other customers are very obvious and that any wires over $25,000 in a month ($75,000 for a business) are considered suspicious and are closely monitored. The institution does not send or receive many international wire transfers and does not have any country triggers when identifying suspicious wires.

Another institution mentioned that analysts reviewing daily aggregate transaction lists often find it difficult to know when patterns have emerged that warrant a SAR filing. FinCEN staff explained that judgment is required when cases are not clear cut.

Some institutions utilize an internal suspicious activity reporting form to facilitate the reporting of suspicious activity from the branch level up through to the BSA officer, however, in some smaller institutions the tellers simply reach out directly to the BSA officer by phone to inform them of the activity.

One institution that does utilize an internal SAR form estimated that it receives approximately 20 such reports each month from its 10 branches. The internal SAR form — i.e. a standard form for personnel to record unusual activity and for referring the matter to the compliance officer for further consideration or investigation— is available to all employees via its intranet. Of the 20 reports each month, about 4 ultimately result in a SAR filing, the majority of which are for structuring. Additional SARs are filed as a result of alerts generated from transaction monitoring software and other reports.

Another institution that just began in January 2010 utilizing an internal SAR form noted that approximately 90 percent of these reports resulted in a SAR. The institution's monthly monitoring program drives its daily monitoring and validates that it is on track.

Another institution noted that while it does receive some referrals from front-line employees, it feels they should be getting more, which is an issue it plans to address with training.

One institution noted that because its tellers know their customers so well, sometimes the familiarity can become too comfortable, actually making it difficult for the teller to be objective and identify and report suspicious activity.

Another institution noted that it most often sees an increase in branch referrals of suspicious activity immediately after the institution's annual AML training when the employee's awareness of the SAR requirements is most heightened.

There was no consensus among the observations of the participating institutions as to whether more SARs were generated as a result of (i) alerts that began with automated monitoring systems (such as a flag for possible structuring by monitoring multiple accounts tied to the same customer; or a flag with respect to a wire transfer in an amount significantly higher than normal activity for the customer) or (ii) from a referral from a member of the institution's staff directly observing a transaction or customer behavior.

Some institutions provided concrete numbers, while from other institutions a compliance officer provided a rough estimate based upon experience. Observations ranged from 80 percent of investigations leading ultimately to a SAR filing having been initiated from automated systems (20 percent from branch referrals) to almost the reverse: 90 percent from branch referrals (with 10 percent from automated systems). Most institutions believed the sources were more closely balanced: e.g., 60/40, 50/50, or 40/60.[36]

There was consensus, however, that a given branch referral was more likely to lead to a SAR being filed than a given automated system alert (including because the latter has false positives). It was clear from our outreach discussions that smaller depository institutions place a great deal of emphasis on training and empowering their front-line personnel to report suspicious activity, especially since these personnel are very well positioned to know what makes sense for their customers and what looks suspicious.

36. Note that these observations are based on informal discussions with a small sample of institutions that have varying business lines and customer activity.

The SAR Form

A number of depository institutions provided useful input into the practical aspects of trying to convey suspicious information to FinCEN, in terms of constructive suggestions as to how to improve the SAR forms themselves. This is particularly welcome as FinCEN progresses through an IT modernization process that will make the information in the reporting fields more accessible to law enforcement investigators. FinCEN has published for public comment suggested changes to the reporting forms.[37] One institution noted that FinCEN's recent proposal to modernize the SAR form[38] would be "very beneficial" to it, particularly the proposal to report different kinds of suspected structuring.

One institution mentioned that the activity codes on the current SAR form[39] pose challenges due to overlapping definitions, such as "check fraud" and "counterfeit checks." The institution made the following additional observations regarding the activity codes: (1) it is unclear what constitutes "bribery"; (2) the form should clarify whether "mortgage loan fraud" refers to residential or commercial loans; and (3) ACH fraud is common enough to warrant its own activity code, as opposed to being included as part of "wire transfer" activity. The institution stated that it finds the activity codes useful only for the purpose of reporting trends to the board.

One institution mentioned that the "check-the-box" activity codes on the SAR form are sometimes ambiguous and confusing, but its regulator is rigid in terms of citing for failure to check what it considers to be the right box. FinCEN explained that the activity codes are more of an aide than a primary objective as the financial institution completes the SAR form. In many cases, a financial institution might not have a view as to which category applies, but this should not prevent the institution from providing a full narrative, including the reason(s) why the activity was deemed suspicious.[40]

FinCEN and law enforcement might use the activity codes when focusing investigations on specific types of activity or in analyzing trends, but the value of the SAR depends on the sum of the information provided as opposed to the distinct code. (FinCEN also mentioned that law enforcement spends a significant amount of time analyzing the large number of SARs filed with the "other" activity code checked.)

37. See http://www.fincen.gov/forms/bsa_forms/
38. See http://www.fincen.gov/statutes_regs/frn/pdf/BSA-SAR-PRA-60-DAY-2010-(MGR)-(v1).pdf
39. See http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf
40. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (page 75); "When evaluating suspicious activity and completing the SAR, banks should, *to the best of their ability*, identify the characteristics of the suspicious activity." (emphasis added)

Another institution asked why the SAR form doesn't enable the inclusion of attachments (e.g., pictures of checks). FinCEN staff explained that the volume of SARs in the database makes it impractical to include a broad range of attachments. Current efforts are underway to consider implementing a capacity to include spreadsheets with transaction data. Law enforcement can request additional underlying data as needed. The most important part of the SAR form is the narrative.

Another institution raised two issues relating to the current SAR-MSB form.[41] With the SAR-MSB form, it was noted that there is nowhere to indicate structuring on the form (other than the narrative). It was also noted that the SAR Narrative form isn't "user friendly" from an institution's perspective as it does not allow for the inclusion of data in a tabular format. FinCEN discussed generally some of the changes that may be coming related to the forms through IT modernization to modernize the SAR form and address some of these issues.

90-Day Review and Repeat Filings

In the October 2000 issue of FinCEN's *SAR Activity Review, Trends, Tips, and Issues*, FinCEN provided guidance regarding repeated SAR filings on the same activity. As the report states:

> "One of the purposes of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This is accomplished by the filing of a SAR that identifies the activity of concern. Should this activity continue over a period of time, it is useful for such information to be made known to law enforcement (and the bank supervisors).
>
> "As a general rule of thumb, organizations should report continuing suspicious activity with a report being filed ***at least 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 that it must continue to review the suspicious activity to determine if other actions may be appropriate, such as terminating its relationship with the customer or employee that is the subject of the filing."[42]

41. See http://www.fincen.gov/forms/files/fin109_sarmsb.pdf
42. See http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf, p. 27

The 2010 FFIEC BSA/AML Examination Manual re-iterates FinCEN's guidance which suggests that institutions should report continuing suspicious activity by filing a report at least every 90 days.[43] The Manual also notes that "banks should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts." The Manual states that policies should include:

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

During our outreach discussions, a few of the institutions expressed frustration with the 90-day review, characterizing it as very time consuming. One institution indicated that its workload made it "impossible" to keep up with the 90-day review for every SAR that was filed.

Some of the other institutions asked for guidance regarding the 90-day reviews. One institution asked how ongoing SARs assist law enforcement, as the institution felt that once the first SAR is in the database, law enforcement has all the information it needs. FinCEN explained that ongoing SARs are crucial in providing law enforcement a more accurate picture of the type and scope of the suspicious activity. For example, only after multiple SARs are filed might it be clear that the subject is engaged in a pattern of activity, and the higher value of aggregate transactions might merit the allocation of overstretched law enforcement resources to investigate.

Another institution asked the technical question of how to file an ongoing SAR when suspicious activity stops for several months, but later resumes. FinCEN's guidance was that it is generally useful to law enforcement for the institution to make reference to previously filed SARs when the suspicious activity resumes.

One institution was highly critical of the 90-day review process, claiming that it merely adds to compliance costs. The institution argued that law enforcement should have a similar time-frame within which to act on SAR filings. The institution generally urged more coordination between law enforcement and financial institutions. In particular, the institution suggested that FinCEN or law enforcement should notify institutions when filed SARs are relevant to ongoing investigations (or at least notify institutions

43. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf, p. 76

when filed SARs have been reviewed). This would enable institutions to better determine whether to exit customer relationships. It would also enable the institution to update law enforcement of important developments quicker than through filing a continuing SAR. Institutions could also be exempted from conducting 90-day reviews with respect to accounts that law enforcement has chosen not to investigate.

One institution indicated that its policy is to maintain account relationships, even with customers on whom the institution has filed one or more SARs, unless the institution is at risk for losses.

According to another institution's Compliance Manual, after filing a third SAR on the same business or individual, the BSA Officer will meet with the Audit Committee and the Account Officer to determine if, based on the activities involved, the account should be closed. This does not preclude the BSA Officer from recommending, to this same group, the closing of an account after one SAR is filed if the activity involved warrants such action. The institution noted it often does close the account. A monthly report is prepared for the board of directors informing them of the SARs filed in the previous month.

Another institution with an MSB subsidiary noted that generally speaking, if two SARs are filed regarding activity through the MSB, the MSB will immediately stop doing business with the customer. There was one instance where a customer was exited after a third SAR was filed on the customer. The institution indicated that once a teller at the MSB questions customers, they usually don't come back because they can just go to another agent location.

While many institutions have internal policies to exit customer relationships after a certain number of SAR filings, credit unions, in particular, expressed frustration with the 90-day review process, particularly because it is more difficult for these institutions to exit member relationships.

One credit union noted that it had filed over a dozen SARs on a member because of the 90-day review and because of the difficulty of expelling members from the credit union. These additional SAR filings take up a great deal of time in terms of analysis and preparation by credit union staff.

FinCEN recognizes the challenges the 90-day review presents. As part of our information technology modernization efforts, FinCEN issued a SAR modernization proposal on October 15, 2010. As part of this proposal, data field #1 of the SAR would allow institutions to differentiate between an "initial report" and a "continuing activity report."[44]

44. See http://www.fincen.gov/news_room/nr/pdf/20101013.pdf and http://www.fincen.gov/statutes_regs/frn/pdf/BSA-SAR-PRA-60-DAY-2010-(MGR)-(v1).pdf, p.11

SAR Filing Trends

Many of the institutions noted that a large number of their SARs are for structuring of cash. This is discussed in more detail in the following section related to currency transaction reports.

In addition to reporting structuring activity, another institution noted that some of its SARs have been filed on charitable organizations where it was suspected a signer on the account was abusing the charity.

Another institution noted that some of the more recent trends it has been seeing within its institution include scams common on Internet sites such as craigslist.com as well as fake lottery scams.

Another institution indicated filing SARs involving suspicious wire transfers, or one person sending money to multiple receivers. The institution has also had trouble in the past with 419 scams. This has slowed, but the institution found it difficult to convince the customers it was in fact a scam. In an effort to protect the customer, the institution would cut off the transactions, but was frustrated because the customer could just go to another institution and complete the transaction.

One institution filed a SAR on a customer that had committed suicide after defrauding the institution and wondered whether the SAR filing was useful. FinCEN staff said that, while any particular decision to file a SAR is a subjective judgment based on relevant facts, SAR filings may be useful in such cases to help track assets to seize on behalf of victims.

Multiple institutions noted that they had filed SARs when customers made a range of transactions through a combination of their own personal accounts and their business accounts, for activities purporting to be either of a business nature or of a personal nature.

Currency Transaction Reports (CTRs)

The reporting of large cash transactions is one of the original requirements under the BSA,[45] and depository institutions thus have decades of experience with these reporting requirements. Notwithstanding the evolution of payments instruments, including the increasing movement away from checks and other paper instruments, individual institutions consistently described circumstances involving certain business customers (such as a grocery store) that had needs for cash services. Institutions also consistently described situations of specific individual customers or members who preferred to deal in large amounts of cash. In the latter circumstance involving individuals and as related to the applicability of SAR and CTR reporting, a common observation was made that the customer purported not to want the government to know about his or her business.

Many examples were provided with respect to customers who knowingly structured transactions in an attempt to avoid reporting requirements (perhaps misunderstanding that a CTR could be filed on the basis of multiple, aggregated transactions, or that structuring might be reported on a SAR). In some of those examples the institution explained that it had reviewed the behavior and that aside from the structuring, the institution did not believe the idiosyncratic customer was involved in other criminal activity. Institutions recognized that cash transactions might also be preferred in conjunction with attempted tax evasion.

Pursuant to BSA regulations, a depository institution is required to file a Currency Transaction Report (CTR) for each deposit, withdrawal, exchange of currency or other payment or transfer by, through, or to the institution which involves a transaction in currency of more than $10,000.[46] Additionally, multiple currency transactions totaling more than $10,000 during any one business day must be treated as a single transaction if the depository institution has knowledge that they are conducted by or on behalf of the same person.[47] These requirements stem from the sense of Congress in passing the BSA in 1970 that criminals were exploiting the anonymity of cash transactions, particularly in cases involving the proceeds of narcotics trafficking and with respect to tax evasion.[48] The BSA prohibits and criminalizes the structuring of transactions to evade reporting requirements, including attempts to cause a financial institution to fail to file a CTR.[49]

45. See 31 U.S.C. § 5313.
46. See 31 CFR § 103.22 (future 31 C.F.R. § 1010.311).
47. See 31 CFR § 103.22(c)(2) (future 31 CFR § 1010.313).
48. See H.R. Rep. No. 975 91st Cong. 2d Sess. 12 (1970).
49. See 31 U.S.C. § 5324.

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.[50] FinCEN issued exemption regulations in two phases, specifying the criteria under which an institution may take advantage of the exemption authority.[51] 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.[52] Phase II allows depository institutions to exempt from reporting transactions in currency between them and "non-listed businesses" or "payroll customers."[53]

In December 2008, FinCEN published a rule, which subsequently became effective on January 5, 2009, intended to simplify and clarify the process by which financial institutions exempt the transactions of certain persons from the requirement to report transactions in currency in excess of $10,000.[54] The amendments aimed to reduce the cost of the exemption process to depository institutions by eliminating the need to file a Designation of Exempt Person (DOEP) form[55] for certain customers and to enhance the value and utility of the remaining CTR filings for law enforcement investigative purposes by removing filings that FinCEN determined to have little value to law enforcement.

In July 2010, FinCEN released an assessment to examine whether this rule had its intended effect.[56] The study found that fewer CTR filings were made on transactions of limited or no use to law enforcement, while higher value CTRs are becoming easier to identify. And overall, CTR filings fell nearly 12 percent from 15.5 million in 2008 to 13.7 million in 2009, while certain classes of filings most valuable to law enforcement increased. FinCEN also saw for the first time in 2009 a slight *decrease* in the number of depository institution SAR filings − the first decrease since reporting began in April 1996, while the quality of information reported in SARs continues to increase, reflecting FinCEN feedback and guidance as well as ongoing financial institution diligence. End of year figures for 2010 continue to reflect a 3 percent decrease in depository institution SAR-DI filings from 2009 to 2010, as well as a slight decrease of under 1 percent for CTRs filed during this same time period.

---

50. 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).
51. See 31 CFR § 103.22(d) (future 31 CFR §§ 1010.315 and1020.315).
52. See 31 U.S.C. § 5313(d).
53. See 31 U.S.C. § 5313(e).
54. See http://www.fincen.gov/statutes_regs/frn/pdf/frnCTRExemptions.pdf
55. See http://www.fincen.gov/forms/files/fin110_dep.pdf
56. See http://www.fincen.gov/news_room/rp/files/18thMonthLookbackReport.pdf

FinCEN noted overall that institutions did not report practical difficulties in the preparing, reviewing, or filing of CTRs. Some mentioned that historically, albeit significantly improved over time, institutions did not have sufficient customer information readily available to complete the form (such as "customer occupation, profession, or business," which tellers might be reticent to ask the customer). Similarly, systems had been implemented over time to aggregate transactions (although exceptions occasionally arose, such as across business and personal accounts). Few institutions mentioned the $10,000 CTR threshold other than in passing; usually in the context of acknowledging the increasingly less common large cash activity for individuals as compared to certain businesses for which exemptions were useful.

Impact of Changes to CTR Exemption Regulation

In outreach discussions with the institutions, FinCEN was particularly interested in receiving feedback regarding how the exemption rule modification had impacted an institution's approach to CTR exemptions. Amendments with regard to Phase II exemptions appeared to have the most significant impact on the institutions with which we spoke. The Phase II amendments to the exemption rule were as follows:

- The 12-month waiting period was changed to 2 months, or upon conducting a risk-based analysis.
- The definition of "frequently" engaging in transactions by Phase II customers was changed from eight or more transactions per year to five or more transactions per year (if the customer has maintained a transaction account for 2 months, or it conducts a risk-based analysis.)
- Biennial filings are no longer required.
- Change in control need no longer be reported.

The feedback from the depository institutions was consistently positive, with some noting very significant benefits, others more limited benefits, while none articulated any negative aspect of the changes.

One institution specifically noted that shortening the time required before exempting new customers and the changes in the biennial renewal requirements were beneficial. As a result of the rule change, the institution is filing more exemptions and no longer filing biennial renewals, which reduced the institution's extra workload. Despite not having to renew exemptions with FinCEN annually, the institution does still review exempted accounts annually to ensure eligibility. Overall, the institution felt it was benefiting from the rule change.

Another institution noted that in response to the rule amendments, it was anticipating exempting more customers. In that regard, the institution intends to implement the current rule's definition of transaction "frequency." However, despite the amendments, the institution is still not comfortable reducing the "time" requirement, and does not intend to exempt customers who have maintained their account(s) at the institution for less than 1 year. A few institutions stressed the importance they placed on getting to know a customer and related activities over a period of time (for example, 6 months to 1 year, some noting seasonal impacts on business), before the institution would wish to consider an exemption.

Another institution characterized the CTR exemption changes as "great," and found it particularly helpful that it no longer was required to wait 1 year to exempt. The institution found this especially helpful as it was able to more quickly exempt a large grocery store that had recently become a customer. The institution currently has between 50-60 exemptions and seeks to exempt customers whenever it can.

Another institution stated that the January 2009 guidance expanding the CTR exemption rules has saved the institution a great deal of time. (Most of the institution's exempted customers are fast food franchises and similar businesses.) However, the BSA Officer commented that if the rules were truly "risk-based," the exemptions would not be limited to certain types of businesses. Many customers fall into the non-exempt categories (e.g., car dealerships) that the institution would exempt if permitted.

Yet another institution echoed that it is helpful to be able to exempt customers sooner, although it has found it has not exempted very many additional customers in the past year and a half because it has noticed a decline in cash flow, particularly with restaurants in the area, which the institution suspects is due both to the economy, as well as to the increased use and acceptance of debit and credit cards.

An additional institution cited the economy as a possible explanation for its decrease in CTR filings. Last year the institution removed two customers from its exemption list because they were not meeting the five transaction requirement. The institution noted that it has about 20 exempt customers; however, no additional customers qualified under the new rules because they did not have enough transactions or were ineligible businesses.

One institution commented that it currently has approximately 17-18 customers that are designated as exempt for CTR filing purposes. The institution indicated that exemptions save it a substantial amount of work. Specifically, CTRs require teller interaction and under its internal policies, a further review period of 6 weeks; whereas once the customer is exempt, no further action is required.

Another institution suggested that the list of businesses ineligible for exemption should be more flexible. For example, the institution has a customer that runs an airport bus service and only deals in cash. Since the business is engaged in the "chartering of buses," it does not qualify for an exemption, and CTRs must be filed on the customer every day.

Another institution stated that at this time, it does not exempt any customers from the CTR filing requirement. The institution explained that it does not have any payroll customers or large, cash intensive businesses that would qualify for exemptions, however, it is planning to review some of its more recent new accounts to determine if any of them may qualify for exemptions.

Some smaller institutions, particularly those that do not file many CTRs, indicated that given their current processes, it still takes longer to exempt someone than to file a CTR. These institutions also expressed concerns over the high level of scrutiny that examiners and auditors still give to exemptions.

FinCEN was encouraged to hear positive feedback regarding the CTR exemption process, particularly the shortened timeframe before exempting new customers.

Structuring and Cash Related SARs

One institution noted that it files approximately 150 SARs each year, the majority of which (about 70 percent) report structuring. The institution monitors all transactions between $5,000 and $10,000 for potential structuring. On the other end of the spectrum, another institution had filed 11 SARs since 2005. The institution asked whether it should voluntarily file SARs in cases where the dollar threshold is relatively low. FinCEN staff advised that voluntary SARs can still be useful to law enforcement because such reports can provide a clearer picture of the type and scope of the suspicious activity.

One institution expressed that it is confident that some customers engage in structuring for no reason other than that they value their privacy and they fear an IRS audit will result from a CTR filing. The institution finds it hard to file SARs in such instances. Similar sentiments were expressed by other institutions. Many of the customers so described were older, including business owners who had developed strong relationships with the institution over a period of decades. In contrast, institutions expressed much greater caution in newer relationships with individuals dealing in large amounts of cash (particularly for personal as opposed to retail business accounts).

Several institutions noted that customers who are general contractors pose unique SAR-related challenges in two scenarios. As one institution explained, first, contractors often withdraw cash to pay day-laborers. Second, other institution customers often withdraw cash to pay for the services of contractors (with a further presumption that the contractor would use the cash in turn to pay subcontractors and suppliers). In both scenarios, the institution suspects that cash payments may facilitate tax evasion. The institution acknowledges, however, that there is nothing inherently illegal about paying for services in cash. Accordingly, the institution is unsure of whether these scenarios should trigger a SAR filing.

FinCEN indicated that, while any particular decision to file a SAR is a subjective judgment based on relevant facts, the IRS may find SAR filings useful where the institution suspects tax evasion. FinCEN also referred the institution to an April 2008 report published by FinCEN, "*Suspected Money Laundering in the Residential Real Estate Industry*,"[57] that addresses similar contractor-related issues.

FinCEN found this to be a recurring theme heard from smaller institutions that contractor transactions are routinely suspected to facilitate tax evasion, whether income taxes or required withholdings with respect to workers.

A few institutions that provided safe deposit boxes for their customers described situations where they observed the customer inserting or removing large amounts of cash from the safe deposit box, sometimes in order to deposit some of the cash in their account. The institutions questioned the rationale behind such a transaction. Some institutions observed that notwithstanding deposit insurance and the soundness of the individual institution, some customers appeared to prefer cash, specifically during the economic crisis.

CTR Brochure

FinCEN produces a series of brochures, "Notice to Customers: A CTR Reference Guide" as a resource for financial institutions to help address questions frequently asked by their customers regarding the BSA requirement to file CTRs. The brochures were created at the request of financial institutions, and use plain language to explain the reporting requirement to those who may not be familiar with a financial institution's obligations under the BSA. The brochure is available free of charge on FinCEN's Web site for institutions to download, print, and distribute as they wish.[58]

57. See http://www.fincen.gov/news_room/rp/files/MLR_Real_Estate_Industry_SAR_web.pdf

58. See http://www.fincen.gov/whatsnew/pdf/20090224.pdf

Some institutions participating in the outreach meetings previously had produced their own written explanation of the regulatory requirements, but many have now started using FinCEN's brochures. Several institutions noted that the CTR brochure was very helpful and was utilized extensively at their branch locations. Most institutions indicated that this publication is provided at the branch level so tellers can provide the brochure to customers to help explain the reporting requirements. (FinCEN representatives observed copies of brochures in a number of branches visited, displayed near teller windows or together with the institution's informational and promotional materials for various products and services.)

It was suggested that it would be additionally helpful if the brochure could be translated into different languages, particularly Polish, Vietnamese, Mandarin Chinese, and Arabic. One institution suggested translating the CTR brochure into the same languages as the materials provided to educate MSBs on their regulatory requirements.[59] Currently, FinCEN's CTR brochure is also available in Spanish.[60]

FinCEN's Observations Related to Cash Reporting

FinCEN appreciated the observations of the institutions participating in the outreach meetings with respect to reporting of cash transactions. Institutions did not report significant practical difficulties in the preparation of CTRs and cash-related SARs. A range of institutions described multiple cases where cash transactions had raised concerns with respect to possible criminal activity or tax evasion. For a subset of customers, however, a number of institutions questioned the usefulness of the reporting to law enforcement where the institution did not see indicia of other illegal activity.

FinCEN reminded institutions that structuring itself is a crime, while explaining that in some circumstances these filings can indeed provide useful information, particularly as a pattern is developed over time, with increasingly large aggregate sums. Institutions appreciated the caution that, especially for customers using large amounts of cash, the institution might have little insight into some of the customer's activity. One of the benefits that FinCEN has in reviewing trends and patterns in BSA reporting is to see where a particular subject is engaged in activity through multiple financial institutions.

SARs filed with respect to structuring and other cash-related transactions were cited by institutions in the context of concerns regarding law enforcement only following up on a small portion of SAR filings, and with respect to concerns over customers that have been the subject of multiple or repeated SAR filings.

59. See http://www.fincen.gov/financial_institutions/msb/materials.html. Currently, these MSB materials are available in English, Spanish, Arabic, Chinese, Farsi, Korean, Russian, Somali, and Vietnamese.

60. See http://www.fincen.gov/whatsnew/pdf/espanol_CTRPamphlet.pdf

To put this in context, consider that the current SAR form has 20 categories of activity for the bank to note as a "summary characterization" in addition to the thorough description of the basis for suspicion in the narrative section. The first category is labeled "Bank Secrecy Act/Structuring/Money Laundering." Since suspicious activity reporting by depository institutions began in 1996, this characterization has consistently been the most commonly noted by depository institutions, accounting for almost half of all SARs filed since 1996, and in the more recent 2005 to 2010 period, accounting for 54 percent of all filed SARs.[61] In comparison, for the individual depository institutions participating in the outreach visits, their aggregate filings during the 2005 to 2010 period indicating BSA/Structuring/Money Laundering accounted for almost 80 percent of the SARs they filed.[62]

FinCEN acknowledges that notwithstanding the criminal prohibition against structuring, and taking into account the need of law enforcement to prioritize limited resources, isolated reports of structuring, at least in modest amounts, cannot be expected automatically to trigger an investigation or criminal prosecution. The government nonetheless does investigate and prosecute structuring, in particular where the investigation may suggest other criminal activity (that might not be apparent to a financial institution).[63] Some SAR Review Teams across the country are particularly active in developing investigations and prosecutions in structuring cases.

FinCEN appreciates the efforts of depository institutions both with respect to educating their customers on the regulatory requirements, and in reporting information that may be useful in investigations of criminal activity.

---

61. Note that this categorization includes activity other than structuring of cash transactions, and that a depository institution may cite more than one characterization if applicable. The next most commonly reported characterizations of suspicious activity are check fraud, mortgage loan fraud, credit card fraud, and counterfeit check. FinCEN regularly pushes updated statistics on SAR filings, broken out by type of filing institution, characterization of activity, and geographically by State, in its publication, *SAR Activity Review – By the Numbers*, available at http://www.fincen.gov/news_room/rp/sar_by_number.html

62. Even within this sample of participating institutions, only two institutions filed less than the national average of 54 percent. These two institutions focused on higher net worth customers, including through private banking and wealth management services, and had comparatively fewer cash transactions (and less focus on cash transactions in discussions with FinCEN) than the other participating institutions.

63. FinCEN has published examples of structuring prosecutions that have been facilitated by BSA filings. For more information on these cases, please see http://www.fincen.gov/news_room/rp/files/reg_sar_index.html#Structuring

BSA E-Filing

FinCEN's BSA E-Filing System supports electronic filing of BSA forms (either individually or in batches) through a FinCEN secure network.[64] As compared to traditional filing through paper forms, electronically filing BSA information increases the timeliness of data availability, reduces the cost of paper processing, streamlines BSA report submissions, improves both data quality and data security, and provides users with enhanced audit and recordkeeping capabilities.

During our outreach, FinCEN was particularly interested in hearing about the experiences institutions are having with the E-filing process, and for those that might not currently E-file, FinCEN discussed the benefits of transitioning to this secure system.[65]

FinCEN received very strong endorsements of the E-filing system, in particular at the town hall meetings, where industry representatives that had not yet begun E-filing were eager to hear the experiences of those that had. Those that were not E-filing largely did not have any specific reason not to do so, but rather had not fully considered the option, or had postponed learning more in light of work priorities or focus on changes to other technology. Those who had begun E-filing were very complimentary as to the ease of the process, the helpfulness of FinCEN's Helpdesk to begin the process, and the benefits and speed of the confirmations of reports filed. A number of institutions described their only regret as not having moved to E-filing sooner.

One institution noted that it currently batch-files CTRs and discrete-files SARs. The institution has never experienced any problems with the E-filing system and has found FinCEN's E-filing helpline to be very helpful.

Several institutions also indicated that they use E-filing for CTRs and SARs. They have had a very positive experience with the process and particularly like receiving the acknowledgements, which help streamline the components of regulatory examinations where examiners seek to confirm that required reports have been filed.

One institution that does not currently E-file is anxious to do so once it has a new transaction monitoring system in place.

Another institution indicated that it is extremely happy with the E-filing process and is appreciative that its regulators encouraged use of the E-filing process. Regulators helped educate the institution on the process.

64. See http://bsaefiling.fincen.treas.gov/main.html

65. See http://www.fincen.gov/whatsnew/pdf/E-File_Brochure.pdf

One institution indicated that it filed SARs electronically but had not yet begun using E-filing to submit CTRs. After discussing the benefits during our outreach meeting, the institution seemed interested in looking into E-filing CTRs as well.

One institution noted that the discrete E-filing works very well; however for an institution of their size, batch filing would be more desirable. Unfortunately, the third party vendor it uses is not currently able to receive batch SAR validations, and will be unable to do so for another 2 years when system upgrades become available.

The suggestion was made on a few occasions that a possible explanation for slower industry adoption of E-filing is a lack of awareness among vendors that are marketing IT solutions for BSA obligations, including report generation.

One institution provided positive feedback regarding the E-filing system, and mentioned that the transition to E-filing was easy. Additionally, the institution appreciates the feature that provides a confirmation of filing. Confirmations are very useful for recordkeeping purposes. However, the institution noted that the system doesn't provide confirmations after more than 60 days have passed since filing. The institution requested that FinCEN enable the provision of confirmations after 60 days as well.

One institution likes the ability to access and populate the SAR form through E-filing, except for the fact that the form always updates to the current date even if the form is saved and re-opened. Thus, when completing a SAR over several days, the date on the SAR is always the latest date.

As part of FinCEN's ongoing efforts to educate financial institutions on the benefits of E-filing, FinCEN hosted an informational Webinar in November 2010 to instruct financial institutions on the simple process of signing up and using E-filing.[66]

66. See http://www.fincen.gov/whatsnew/pdf/FinCENBSAEFilingWebinarPresentation_11-04-2010.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.[67] As noted in the 2010 FFIEC BSA/AML 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."[68]

During the outreach meetings, institutions provided an overview of their respective employee training programs, policies, and procedures, which varied among institutions.

One institution noted that all personnel who have contact with customers, who monitor or process customer transaction activity, or who handle cash in any way, receive appropriate training to ensure compliance with BSA, AML, and USA PATRIOT Act law and regulations, and to provide employees with the information needed to detect and report suspicious activity. All new employees are required to complete and pass BSA/AML training within their first 30 days of hiring.

Another institution noted that in addition to annual training, it also uses periodicals, and OCC and other agency reports and newsletters pertaining to BSA/AML issues. These are routinely sent to pertinent employees, senior management within the institution, and the board of directors.

One institution indicated that all employees receive BSA/AML training, tailored to job function, on at least an annual basis. New employees receive BSA/AML training upon hiring. Additional BSA/AML training is provided depending on job function. The institution also utilizes webinars and other Internet resources for training purposes. The BSA/AML Officer conducts annual BSA training for the board, and board members regularly attend conferences that address BSA-related issues. The BSA/AML Officer addresses BSA-related issues in quarterly Compliance and Operational Risk meetings. The BSA/AML Officer also addresses BSA-related issues at senior management meetings on emerging issues as they arise.

---

67. See 31 U.S.C. § 5318(h)(1)(C).

68. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (p. 37)

Another institution notes that all new customer service representatives are trained during their initial orientation. The institution has an on-line training program which all employees are required to complete annually. Employees are required to score above 80 percent to pass and are given three chances to do so. The institution contracts with an outside party for the training program, but it provides the content itself. All training for new customer service representatives is conducted in-person, and after that initial, in-person training, employees do the online training annually.

One of the institutions noted that fraud detection has become a part of the AML training that is provided to front-line personnel. For this institution, the training has been particularly effective in helping spot fraudulent activity. It noted that in the past year it only took $1,800 in losses in counterfeit checks.

The Compliance Officer of one institution meets with staff on a monthly basis for training that can involve BSA training.

Independent Testing (Audit)

The BSA requires financial institutions to implement procedures for the independent testing of their AML programs.[69] An independent audit assists the bank's management in identifying possible areas of weakness where enhancement or stronger controls may be needed.

The institutions participating in the outreach meetings employ a range of different models to meet the independent audit requirement. Many relied upon the bank's internal audit function; where representatives of that audit function participated in the outreach meetings, the institution explained the distinct roles, reporting lines and other indicia of independence. With respect to external auditors, sometimes the audit of the BSA/AML program was conducted by specialists in this area, in other cases by the institution general external auditor − albeit usually by a person distinct from those responsible for financial statement audits. A few institutions noted − as with other aspects of their experience in meeting BSA obligations − that they had adapted over time, first relying upon external consultants, but then transferring responsibility to internal auditors once programs and procedures had become more established and understood within the institution.

One institution noted that it uses an external auditing firm and the Audit Committee also goes through all reports to ensure sufficiency. The representative of the auditing firm indicated that their regulator has been satisfied with the audits performed by the company, and the institution has received consistently high marks from exams.

Another institution indicated that it undergoes an independent BSA/AML audit, conducted annually by an outside party. The institution also maintains one full-time internal auditor.

One institution's BSA/AML policy document commits the institution to "adequate and effective" testing of its BSA/AML program either by internal audit staff or a third party auditor. The annual independent review used to be conducted by an outside party. It has now been brought in-house and the institution hired a BSA auditor.

One institution has both an external and an internal auditor. The institution noted that auditor reports often result in changes to the institution's policies (e.g., RDC check review; requiring non-customers to provide a Social Security number when purchasing a cashier's check).

69. See 31 U.S.C. § 5318(h).

Money Services Businesses

Money services businesses (MSBs) are a category of financial institution subject to FinCEN's regulations. From time to time, questions arise as to how a depository institution meets its compliance obligations with respect to services provided to another institution that itself is subject to compliance obligations. 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.[70]

The issue of providing banking services to money services businesses was discussed during the outreach meetings, and FinCEN received positive indications at several meetings that previous concerns over the provision of banking services to MSBs are continuing to subside. Individual institutions had different approaches to how they view MSB customers; a small minority had adopted policies not to service MSBs as outside of their core customer focus; some were comfortable with their existing MSB customers; others were specifically looking to take on more MSBs as customers.

Regardless of the business posture regarding these potential customers, all of the participating depository institutions had developed specific procedures for MSBs, often beginning with attempting to properly identify MSBs at the time of account opening or providing new services, including requiring that decisions about new relationships be made in a centralized fashion as distinct from within a line of business or individual branch; the institutions also developed specific processes for overseeing MSB customer activity either on an ongoing basis or at regular intervals. Notwithstanding the varying approaches, institutions consistently explained that they were comfortable with their current posture with respect to MSB customers and their ability to provide services and meet compliance obligations.

One institution notes that it currently has a few customers that are MSBs engaging in check cashing, money transmission, sales of money orders, and sales of prepaid cards. These MSBs are typically agents of larger MSBs.

One rural institution explained that the MSB accounts it maintains are for businesses that provided services to seasonal farm workers, including check cashing and processing remittances to a number of other countries.

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

Another institution noted that it has many customers that are MSBs. They explained that MSBs are a good source of revenue, which in turn enables the institution to provide a wide range of services to its customers.

The BSA/AML Officer at another institution mentioned that the biggest challenge with respect to MSB customers is making sure these customers comply with the institution's own AML requirements. Nonetheless, the institution does not turn away MSB customers unless the MSB: (1) has an overly risky business model; (2) fails to obtain a license; or (3) does not answer the institution's customer due diligence questions to the satisfaction of the Risk Management Department. The institution did exit 4-5 MSB customers in 2009 because they were not comfortable with the customers' source of income, risky business model, or financial activity.

In another institution's experience, regulators are primarily concerned that the institution is adequately monitoring the accounts of its MSB customers for unexplained profitability and other suspicious activity. The institution is comfortable with its due diligence and account monitoring procedures with respect to its MSB customers.

One institution indicated that it is aware that some MSBs are having difficulty finding institutions that will hold accounts for them, and it does not want to summarily turn MSBs away. However, the institution also does not actively solicit MSB accounts. The institution currently has several MSB customers, mostly local-area convenience stores that also provide MSB services and some low-level check cashing businesses. The institution is not currently charging extra fees for its MSB accounts but is considering a $50 per month monitoring fee and the introduction of other fees to help justify taking on the additional risk an MSB customer may present.

Another institution uses a monitoring system to try to identify customer accounts that appear to be operating as MSBs, but have not identified themselves as such. When the software identifies such accounts, the institution requests documentation from the companies indicating the type of activity they were carrying out and proving that they had registered with FinCEN as an MSB.

One institution indicated that it used to have a large MSB customer, however, it frequently requested large amounts of cash, which caused vault and cash management issues; had security implications; and required extra tellers, extra work, and increased BSA monitoring. The account was subsequently closed from a profitability standpoint.

The institution also has several smaller MSBs as customers. The institution checks on an annual basis to ensure the MSBs are registered with FinCEN. The institution also visits the MSB locations, gets copies of their AML programs, and reviews training and financial statements. The smaller MSBs are agents of larger MSBs so they use an AML template, perhaps adding a paragraph on check cashing. The institution characterizes these reviews as very straightforward.

Another institution indicated that it currently maintained relationships with a very small number of MSB customers (one for more than 25 years, another for about 3 years), after exiting other MSB relationships over concerns that there was too much risk.

Another institution provides banking services to MSBs, but believes the compliance costs are very high. Most of the institution's MSB customers are agents of other MSBs (money transmitters) and check cashers. The institution often finds itself in the position of educating its MSB customers with respect to its BSA requirements. Only one of the institution's MSB customers was able to produce an AML policy document upon first request. The institution suggested that much of the problems related to MSBs would be solved if more MSBs were examined for BSA compliance by the IRS as agents of FinCEN.

One bank which had a check cashing MSB as a subsidiary described how certain compliance responsibilities were coordinated centrally. The business representatives of the bank clarified that they did not view the check cashing services as a way to identify customers that might be interested in opening accounts at the bank. To the contrary, they emphasized that they viewed the bank's customers (mostly served with commercial loans) as a very distinct population from the customers of the check casher, and that it was a specific business decision of the holding company to provide these distinct services to distinct customer bases.

On an encouraging note, the institutions consistently indicated that regulators do not discourage MSB relationships as long as they are well monitored. The institutions that do maintain relationships with MSBs take their review of their relationships with these customers very seriously.

314(a)

FinCEN's regulations under Section 314(a) of the USA PATRIOT Act enable Federal, State, local, and foreign (European Union) 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 significant money laundering.[71] Several institutions found it useful for FinCEN to explain the rationale of 314(a) and its utility to law enforcement. Some appreciated, while others were not aware of, the statistics on FinCEN's Web site, which are regularly updated, with respect to 314(a) requests and the results of these requests.[72]

FinCEN receives requests from Federal, State, local, and foreign (European Union) law enforcement agencies 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.

Over the past 5 years, FinCEN has received over 17,000 positive responses from financial institutions in response to 314(a) requests. FinCEN's records estimate that approximately 64 percent of these positive matches have come from institutions with assets under $5 billion. In addition, of the total number of institutions that have responded to 314(a) requests over this 5-year period, FinCEN estimates that 92 percent of these institutions have assets under $5 billion, reflecting the significant role smaller institutions play in the 314(a) process, and the high value of information these institutions are providing to law enforcement.

One institution manually downloads the 314(a) list, but is able to conduct an automated search of its records for matches.

---

71. See 31 CFR § 103.100 (future 31 CFR § 1010.520(b)).

72. See http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf

One institution estimated it has had approximately six positive matches, all on customer activity through its MSB subsidiary, but none for the bank. The bank will note in the comments that the "hit" is for its MSB. To date, law enforcement has followed up on one report.

Another institution noted that its 314(a) searches require a manual query of the institution's central database. The institution has only found three matches since it started receiving 314(a) requests, resulting in only one request for documents. The BSA/AML Officer suggested that it would be more efficient if the institution's core processor could conduct 314(a) searches for all of its clients.

One institution explained that it has had only one true 314(a) match and did not receive any inquiries from law enforcement regarding that match. The institution's 314(a) checks are completely automated and are run every 2 weeks. The institution has found its automated system very easy to use, and a 314(a) check observed by the FinCEN team took less than 5 minutes. The institution currently uses an 80 percent match parameter for 314(a) searches and manually eliminates false positives. The institution has tried other levels of matching, but anything lower than 80 percent resulted in too many false positives and anything higher than 80 percent was too restrictive.

One institution that conducts automated 314(a) searches has had one legitimate match and many false positives. The institution feels the 314(a) search system is relatively easy. The institution asked how long it should maintain the 314(a) search list if it also self-verifies. FinCEN advised that it is not necessary to maintain the 314(a) search list if it self-verifies. The institution also asked whether it should close accounts if the owner is a 314(a) match. FinCEN clarified that a 314(a) search match does not trigger any requirement to close an account. Many institutions that do have a match will initiate an investigation that might lead to the filing of a SAR and/or trigger aspects of the institution's own policy, including consideration whether to exit a relationship. FinCEN advised that in some cases law enforcement prefers that such accounts stay open, and referred the institution to FinCEN's previous guidance about written instructions from law enforcement to maintain account relationships.[73] FinCEN further advised that the institution can call FinCEN's Helpline with such questions if they actually arise.

73. See http://www.fincen.gov/statutes_regs/guidance/pdf/Maintaining_Accounts_Guidance.pdf

Another smaller institution noted that its 314(a) process is still done manually, but felt its process was efficient. Searches are done by the institution's BSA Officer, the support specialist, and the wire department. The institution does not use FinCEN's self-verification document, rather it keeps a spreadsheet to document compliance.

There were generally no concerns with the 314(a) process, and several institutions had positive comments regarding the new verification process. Many of the institutions have an automated process by which the 314(a) searches are conducted, but many institutions still rely on at least a partial manual review.

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***.[74]

In speaking with many of the largest banks in 2008, FinCEN found use of the 314(b) process to be quite extensive, with several banks noting 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. In our discussions with institutions with assets under $5 billion, however, FinCEN found there was rather limited use of the 314(b) program.

Several institutions noted that while they are a 314(b) participant, when they reach out to share with another institution they are frustrated to learn that the other institution is not certified to share. The institution that participates in 314(b) will try to encourage the other institution to sign-up, but there is reluctance to do so.

In multiple town hall meetings, the participants shared their experiences with 314(b) including how simple the procedure is to register with FinCEN and thereby provide a contact name for other institutions. One town hall subset concluded that if a compliance officer reached an institution that was not registered under 314(b), then the best option was to ask the counterpart to go to FinCEN's Web site to register, and 5 minutes later they could be sharing relevant information. One institution discussed experience in discussing a case with a counterpart (for example, seeking more information about a potentially suspicious wire transfer from the institution originating the transfer) in the absence of the institutions being registered under 314(b). Multiple other participants concluded that this was exactly the situation where the institutions should be relying on the safe harbor available under 314(b), and, absent such harbor, an institution could find itself in violation of laws and customer confidentiality obligations.

One institution stated that while it was an active 314(b) participant, it acknowledged that there are probably even more opportunities to share that it should take advantage of. The institution indicated it had a large and complex case in which 314(b) played a significant role, allowing it to receive information from another institution that it would not have ever learned of otherwise. The institution estimates it has been contacted about seven or eight times by other institutions wishing to share, but noted that each time the institutions were significantly larger than their own institution.

74. Implementing regulations are codified at 31 CFR § 103.110 (future 31 CFR § 1010.540).

One institution that is a 314(b) participant noted that it has not received any requests to share information from other institutions. The institution has made two inquiries with other institutions to share information, one which it characterized as "helpful," and the other as not.

One participating institution indicated that it has made many calls to other institutions, yet has not received any. While the institution thinks it is a great program, there may be some hesitation by other institutions to share proprietary information.

Pre-314(b), one institution noted that it could not even figure out who to speak with at larger institutions. While the institution has never initiated sharing through 314(b), it has received five 314(b) inquiries. It only provided information one time because the other requests appeared to be "fishing for information" and not related to money laundering or terrorist financing. The institution noted that perhaps there needs to be more training, clarification, and guidance/examples of what is acceptable to share via 314(b).

One institution noted that while it is registered to share, it has never made a request of another financial institution and has never received one either. The institution suspected that some of the hesitation to share may be tied to the reluctance of institutions to discuss check kiting cases with their competitors.

Another institution indicated that it signed up to participate in the 314(b) program for one year; however, it could never find enough other participating institutions. Therefore, it no longer participates itself.

One institution noted its very beneficial experiences with sharing through the 314(b) process, and was particularly comfortable with sharing given the protections that 314(b) certification provides. Its one concern was that some institutions with which it shares would like an e-mail detailing the request, and the institution is not comfortable doing so without confirmation that the companion institution has the appropriate encryption tools. Ideally, the institution indicated that it would be very interested to have a place to share information with other institutions via a secure network, and queried whether FinCEN would be willing to provide depository institutions with such a facility.

One institution that participates in 314(b) feels the program is not successful yet because institutions are generally not educated enough about what information they can and cannot release. The institution has found that other 314(b) participants are often not comfortable sharing information.

A few institutions questioned why institutions must annually re-apply to participate in 314(b). It is easy to forget to re-apply, and it often just gives examiners another reason to assess a technical citation. The institution also suggested that FinCEN create a login database that users can use to see a full list of participants with contact information. FinCEN clarified that a key reason for the annual notification to FinCEN was to ensure that contact information was reasonably current, which would be critical in making the contact information useful.

One institution that was not a 314(b) participant was under the impression that participation in 314(b) required a lot of work. The institution was also under the impression that not many other institutions participate in 314(b). The institution also had misconceptions as to the type of information that could be shared under 314(b). The institution relayed a story in which a customer had been wiring money back and forth to another institution in Texas at the end of each month. The institution suspected that the customer was doing so in order to give the appearance of an inflated monthly balance sheet on one of the accounts. The institution also relayed a story of an investigation involving $50 million and a customer that the institution suspected of being a "mule." The case involved transactions with an institution in Chicago. FinCEN staff explained the ease and advantages of participating in 314(b), and that 314(b) information sharing with the institutions in Texas and Chicago could have been useful in investigating those cases.

FinCEN understands that some institutions 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 Act Advisory Group,[75] FinCEN issued guidance on June 16, 2009, to clarify the scope of permissible sharing covered by the 314(b) safe harbor. A few institutions participating in the outreach meetings expressed great appreciation for this guidance, which they found very useful. At town hall meetings, participants urged their counterparts to review this guidance, which they expected to further bolster appreciation for the utility of using 314(b).[76]

FinCEN recognizes that more outreach is needed to encourage participation in the 314(b) program and addresses the issue of 314(b) participation in the October 2010 *SAR Activity Review*.[77] While participation in 314(b) is ultimately voluntary, FinCEN will continue to pursue avenues in which the importance of information sharing in order to protect the financial system can be conveyed.

---

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

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

77. See http://www.fincen.gov/news_room/rp/files/sar_tti_18.pdf (page 39)

Remote Deposit Capture

Remote Deposit Capture (RDC) allows customers to scan checks and then transmit the image to the institution for posting and clearing. This service, as well as the possible risks, was discussed with several of the institutions during FinCEN's outreach meetings.

At one institution, RDC technology permits checks and monetary instruments to be processed more efficiently. Generally speaking, RDC provides a method of depositing checks into an account by scanning the checks and then transmitting the scanned/digitized image to a financial institution. RDC reduces the cost and volume of paper associated with face-to-face transactions and the physical mailing or depositing of checks or monetary instruments.

The institution notes, however, that RDC may expose institutions to money laundering and fraud. As a result, the institution has developed policies, procedures, and processes to mitigate the risks associated with RDC and the Compliance Department monitors accounts for unusual or suspicious activity. The institution only permits existing account holders to utilize RDC. These customers must go through a credit check and are primarily borrowers or corporate customers of the institution (although if these customers also have personal accounts they may use RDC as well). For the first month after RDC is approved, each transaction is reviewed. After this time period, a sampling of transactions is reviewed each quarter.

For another institution, prior to allowing RDC, the institution obtains information on anticipated activity and then compares that to the customer's actual activity. The institution is implementing a new system it is hoping will help manage the review process. Currently it is manual. To date, the institution has not noted any problems with fraud associated with RDC. Site visits are made to customers to ensure deposited checks are secure and properly destroyed.

One institution noted that the RDC guidance provided in the recent release of the FFIEC BSA/AML Examination Manual was helpful, and it has instituted many of the controls to mitigate risk.[78] The institution indicated that its regulator did not extensively examine its RDC accounts during the last exam.

78. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (pages 204, 208, 209, 212)

Another institution has approximately 80 customers with RDC devices. One of the institution's challenges with respect to these customers is on-site inspections, since some of these customers are out-of-state. The institution is considering whether to purchase software that would enhance security by limiting the use of IP addresses from certain countries. When asked whether the institution's RDC imaging system is used for only recordkeeping purposes or for actually gathering data from the images, the BSA/AML Officer said that the institution's imaging system is "improving."

Another institution echoed the concerns about fraud associated with RDC, but feels it has the appropriate controls in place and keeps abreast of best practices in this area. The institution has an application process in place and only existing business customers are eligible for RDC. Transactions are reviewed quarterly, as they are for Automated Clearing House (ACH) customers, and transactions are monitored through the institution's AML software. RDC customers are also unofficially designated as "high risk" by the institution.

The recurring theme heard from institutions within this asset class is that RDC does present greater compliance challenges. Universally, compliance officers stressed the importance of the institution's business lines working with compliance officers when rolling out new products or services. Many cited the specific example of RDC.

Engagement with Regulators

There was a general consensus that the FFIEC BSA/AML Examination Manual, updated in 2010, has gone a long way toward improving industry understanding of compliance expectations and standardizing the examination process.[79] Of course, some institutions indicated that some uncertainty still exists, and that interpretation of the manual can vary between examiners. While one institution mentioned that it doesn't use the FFIEC BSA/AML Examination Manual because it is "overwhelming," the vast majority of compliance officers characterized the Manual as a critical reference to them. FinCEN suggested that that one participant may find it useful to focus on specific portions of the Manual most relevant to its institution's lines of business.

One institution noted that while the Manual has been very helpful, bank regulators still approach all the institutions the same way and have the same expectations for the smallest institutions as they do for the largest.

Another institution also shared positive feedback regarding updates to the Manual and changed some procedures as a result. The institution found the summary of changes, newly highlighted in the 2010 edition of the Manual, to be particularly helpful. The institution expressed that it is very useful to know upfront what examiners might be expected to be looking at in the next examination cycle.

Another institution expressed concerns that in its State, the Federal regulator is so busy dealing with failing banks it is sending examiners in from other States that are less experienced, and less familiar with the area and its issues.

One institution indicated that exams at the State level tend to focus more on State regulations, not as much on BSA/AML issues. Another institution stated that its last State banking exam was conducted in 2007, although they are supposed to be every 18-24 months.

One institution indicated that its State and Federal examiners communicate very effectively with each other. Regulators usually alternate exams, but sometimes they will conduct a combined exam. The BSA portion of the exams typically has been minimal. The regulators tend to rely on external auditor reports and board reports. The institution noted that while the regulators may differ on a few specific issues, there is no significant difference between them in their approach to BSA compliance.

79. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf

Another institution indicated that it also is examined annually on a State and Federal alternating schedule. Both State and Federal examiners use the BSA/AML Examination Manual and have standardized processes. Examiner manpower has remained fairly consistent throughout the financial crisis although the last BSA examiner seemed to push to finish up more quickly in order to help with lending. The regulators always have at least one person on the BSA area, on which they spend 1 – 2 weeks.

It was encouraging to hear feedback that the FFIEC BSA/AML Examination Manual continues to help improve the consistency of the examination process, and it was also of interest to note from several institutions that examiners are increasingly relying on the independent audit as part of the examination process.

One institution's examinations alternate between the Federal and the State regulator. The institution noted that there is some (but not a great deal of) inconsistency between the FDIC and State regulatory approaches to the BSA. The institution noted that the last State exam was very light with respect to BSA compliance.

On one visit, the institution's Chairman, President and CEO expressed general frustration with respect to current regulatory requirements, stating that for the past 5 years, regulations have become too burdensome and create a very difficult business environment for community banks. Prior to that time, the institution had seen a 10 percent annual increase in its customer-base, representing people who preferred community banks to large banks. He mentioned the negative effects that regulations have on customer service. He emphasized that community banks are more likely to know their customers than large banks.

In response to increasing regulatory burdens, the institution has had to hire more employees for its compliance, audit, and risk management departments. He stated that the institution will always comply with regulatory requirements, but that large banks have a huge advantage in that regard. For example, large banks can afford to have attorneys decide whether to file a SAR. Smaller banks can either file SARs defensively or run the risk of regulatory enforcement actions over cases that fall in the "grey area" of whether to file. Either way, the compliance burden is increased. He further argued that community banks are being forced to bear extra compliance burdens (e.g., increased capital requirements) due to the financial downturn, though it was not the community banks that caused it. He indicated that three small banks have recently tried to get his institution to buy them out. He generally feels that over-regulation could destroy community banking.

One institution mentioned that it has always fared well in its regulatory examinations. The BSA Officer commented that although the regulations claim to be "risk-based," regulators often have a more rigid "rules-based" approach. There are cases in which the institution is confident that no criminal activity is afoot, though the regulators would require a SAR to be filed.

One institution with multiple smaller affiliates under different charters, but for which many compliance policies or activities were coordinated centrally, noted that there is a big difference in approach between examiners from different Federal regulatory agencies. Inconsistency among examiners can be frustrating.

Across the board, depository institutions expressed support for the purposes behind the BSA and for a risk-based regulatory framework. Concern was often expressed that in the regulatory examination process, however, a review of individual transactions or other testing of the application of policies and procedures could lead to scrutiny of individual subjective decisions at a level of detail that appeared inconsistent with the broader purposes and risk-based approach. These concerns notwithstanding, overall institutions expressed views that the situation more recently had improved over the past, due to a better understanding of compliance expectations, in part due to publicly available information such as the Examination Manual.[80]

80. See, for example: http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (page 75); "SAR Decision Making" section.

Engagement with Other Institutions

A significant number of the institutions participate in regular, regional meetings with their peers from other institutions to discuss trends and best practices. In fact, the Chicago town hall meeting FinCEN attended was a bi-monthly meeting of approximately two dozen institutions in the Chicago metro area.

Another institution also noted that Compliance staff attends outside training programs throughout the year, including outreach programs sponsored by the Federal banking agencies, and seminars and conferences offered by various trade organizations. The institution is a member of a regional compliance group, which consists of about 60 institutions (core group of about 25). This group meets periodically to discuss compliance issues and share best practices.

Engagement with Law Enforcement

It was very encouraging to learn that so many of the smaller banks are actively engaged with the law enforcement in their areas. For instance, one institution explained it belongs to a peer group made up of institution representatives, as well as State, local, and Federal law enforcement officials and the State banking department, who meet each month at the local police department. A smaller law enforcement group meets weekly. The meetings are a good resource to engage and discuss issues of concern.

Another institution indicated that its primary interaction with law enforcement involved responding to subpoenas. The institution's security office has developed relationships with the local police department. The institution noted that it generally doesn't directly call law enforcement on issues, but would if there were any type of terrorist activity suspected.

Another institution indicated that it has good relationships with law enforcement and will occasionally contact the Federal Bureau of Investigation if circumstances warrant. It is common for law enforcement to contact the institution and request information or documents underlying a SAR (e.g., customer identification program (CIP) documents, signature cards, copies of checks, and other documents). Some calls from law enforcement have triggered investigations and SAR filings. For example, the institution has three customers whose accounts were hacked, and funds were fraudulently transferred via ACH. These customers first went to law enforcement before notifying the institution. Accordingly, the call from law enforcement triggered the investigation and SAR filing.

Another institution noted that images captured by its surveillance cameras are sometimes useful to law enforcement investigations.

One institution expressed concerns about law enforcement officers coming to branches unannounced and directly asking to speak with a specific employee. Although this does not happen often, it has happened in the past. The institution suggested that for this reason, they prefer to provide as little employee information as possible in SAR narratives.

Another institution mentioned that law enforcement would benefit from greater interaction. First, the institution could write more useful SAR narratives if law enforcement communicated specific needs. Second, the institution could explain banking terminology and concepts to law enforcement to enhance the utility of

the information contained in the SAR. In that particular case, FinCEN invited the institution's staff to participate in the local High Intensity Financial Crime Area (HIFCA) group's various bank outreach efforts, including quarterly banking roundtable meetings.[81] FinCEN further explained that part of the HIFCA group's outreach efforts include teaching SAR review teams how to read SARs.

One institution indicated that it has contacted the FBI and IRS to report suspicious information it felt those agencies would be interested in. In one particular case, the institution has had extensive contact with the FBI regarding an account that is of concern due to the business model and frequent international wire transactions. The institution indicated that it has contacted FBI as well as the FinCEN hotline regarding this customer and had been advised by both agencies to keep filing SARs.

Another institution noted its very active engagement with law enforcement, particularly the SAR Review Team in its area. That SAR Review Team meets monthly and looks at every SAR filed within its jurisdiction. The institution also noted that the local IRS office is very responsive in assisting with structuring cases.

One institution expressed frustration that law enforcement was unwilling to act on cases the institution was confident involved illegal activity. For example, the institution's BSA/AML Manager contacted four separate law enforcement agencies before one would investigate a case. Ultimately, the case involved substantial criminal activity reported in the news. In another incident, the institution filed a SAR and contacted law enforcement with respect to a structuring case involving $500,000. Law enforcement didn't follow up on the case until all of the money in the account had been depleted.

One institution was supportive of its local SAR Review Team, but expressed frustration at what the institution perceives as the SAR Review Team's lack of consistency and failure to follow up on SARs. The institution suggested that the local SAR Review Team focuses too much on cases that involve structuring. The institution was led to believe that the SAR Review Team won't refer cases for investigation unless they involve more than $100,000.

One institution noted that in its experience law enforcement was not well-versed on SAR confidentiality obligations. This is a concern to staff at the institution, who fear that law enforcement will disclose the existence of SARs. This sentiment was not

81. HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the Federal, State, and local levels in high intensity money laundering zones. For more information, see http://www.fincen.gov/law_enforcement/hifca/index.html

expressed by other institutions. FinCEN takes the confidentiality obligations with respect to SARs very seriously, and undertakes to educate law enforcement as to these obligations. FinCEN recently amended its regulations to clarify that confidentiality obligations with respect to SARs also apply to government officials accessing SARs in carrying out their public duties.[82]

One institution gets five or six requests for information from law enforcement annually. One law enforcement agency requested SAR information, but the institution is very cautious about SAR disclosure.

Overall, most participants described good relations and interactions with representatives from a range of Federal, State, and local law enforcement agencies. Institutions often cited increasing interaction in recent years as improving their appreciation for how SARs and other reports are used by law enforcement. Nonetheless, a consistent comment was a wish that FinCEN and law enforcement were able to follow up on more of the SARs filed.

82. See http://www.fincen.gov/news_room/nr/pdf/20101122.pdf

Response to FinCEN's Outreach and Published Materials

As part of the outreach discussions, FinCEN invited general comments and suggestions with respect to the publications and range of information that it makes available to financial institutions. FinCEN consistently received very positive feedback. A number of institutions cautioned that sometimes they feel that there is too much information, i.e. the compliance officer struggles to find the time to review and appropriately consider information that is believed to be relevant to the institution. Some institutions discussed other information sources, such as industry association bulletins, that they found useful to help keep them aware of relevant new information. FinCEN did not receive any specific comments with respect to a publication or information characterized as not useful to an institution (albeit some materials were not applicable to the products and services of a particular institution).

One institution indicated that it is useful to understand the reasoning behind regulatory requirements or changes. FinCEN explained that when we publish guidance, Notices of Proposed Rulemaking, or Final Rules, we strive to provide a detailed explanation of the reason why it is necessary.

FinCEN's Web site

Institutions provided universally positive feedback on FinCEN's Web site. A number particularly noted the Answers to Frequently Asked BSA Questions.[83] Another institution indicated that it often uses FinCEN's published MSB educational materials to train new tellers.[84] The institution noted it would welcome similar materials geared towards banks. Some institutions requested that FinCEN consider utilizing an improved search engine on its Web site, indicating that they found it more difficult to locate MSB information, due in part to less familiarity with MSBs. More generally, participants found the reorganization of the Web site in 2008, which made information accessible by regulated industry (i.e. banks, MSBs, casinos, securities and futures, etc.), to be quite helpful.

83. See http://www.fincen.gov/statutes_regs/bsa/bsa_faqs.html

84. See http://www.fincen.gov/financial_institutions/msb/materials.html

Regulatory Helpline – BSA Resource Center

FinCEN maintains a toll-free Regulatory Helpline for financial institutions with questions relating to BSA and USA PATRIOT Act requirements and forms.[85] Most institutions were aware of FinCEN's Regulatory Helpline, and the feedback that was provided was that this resource is helpful, FinCEN representatives are knowledgeable, and calls are returned in a timely manner, within 24 hours or in the same day.

In addition to contacting the Regulatory Helpline directly, the Helpline posts "Hot Topics" on the FinCEN Web site which provides answers to their most frequently asked questions.[86] FinCEN explained that this functionality was one example of how FinCEN analyzes incoming questions from financial institutions to help determine areas that may benefit from additional clarification or guidance.

Guidance/Advisories

One institution noted that it found FinCEN's January 2009 ruling of the Application of a Section 311 Special Measure to Payments under a Stand-By Letter of Credit very informative,[87] as well as the update on this issue included in the 2010 FFIEC BSA/AML Examination Manual.[88]

Another institution commented that FinCEN's recent guidance with respect to identity theft was also particularly useful.[89]

A few institutions use FinCEN publications for training purposes.

The SAR Activity Review, Trends, Tips and Issues and By the Numbers

Institutions found both publications to be useful, and one institution noted that the *SAR Activity Review – By the Numbers* is useful on a local level and validates the institution's BSA compliance efforts.[90] A number of institutions regularly compare the suspicious activity within their respective institutions with the broader industry and regional trends detailed in that report.

85. FinCEN's Regulatory Helpline can be reached at 1-800-949-2732.
86. See http://www.fincen.gov/hotTopics.html
87. See http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-r001.pdf
88. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf
89. See http://www.fincen.gov/news_room/rp/reports/pdf/ID%20Theft.pdf
90. See http://www.fincen.gov/news_room/rp/sar_by_number.html

Another institution noted that it has incorporated case examples from the *SAR Activity Review – Trends, Tips and Issues* into its annual BSA/AML training program.[91]

Some institutions noted that more information on terrorist financing, in terms of what to look for in transaction monitoring, and when to consider filing a SAR, would be helpful in future issues of these publications.

One institution indicated that the *SAR Activity Reviews* are useful (particularly the trends, charts, and graphs), but that there often isn't enough time to read a 25-page document.

MSB Examination Manual

Analogous to the FFIEC BSA/AML Examination Manual for depository institutions mentioned earlier, FinCEN released the *Bank Secrecy Act/Anti-Money Laundering Examination Manual*[92] for Money Services Businesses in December 2008, to provide guidance that would assist in examinations of MSBs for compliance with the BSA, and to provide the MSB industry with information about BSA requirements and examination practices.[93] The manual includes input from a wide variety of sources, including FinCEN, the IRS in its role as delegated compliance examiner, the State agencies regulating MSBs under State law, the Money Transmitter Regulators Association (MTRA), and the Conference of State Bank Supervisors (CSBS).

The Manual is intended to enhance BSA examiners' ability to perform risk-based examinations of MSBs, provide a resource to enhance the consistency of BSA examination procedures, and facilitate the efficient allocation of examination resources between Federal and State BSA examiners.

While the Manual is focused on MSBs, one institution that has an MSB subsidiary noted that the manual was very helpful guidance and has participated in FinCEN outreach efforts to educate institutions about the manual.

91. See http://www.fincen.gov/news_room/rp/sar_tti.html
92. See http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf
93. See http://www.fincen.gov/news_room/nr/pdf/20081209.pdf

Issues Specific to Credit Unions

Credit unions offer many of the same financial services as banks, often using a different terminology; common services include: share accounts (savings accounts), share draft accounts (checking accounts), credit cards, share term certificates (certificates of deposit), and online banking.

In FinCEN's outreach visits and town hall meetings with credit unions, the vast majority of the issues discussed, as well as credit union observations on individual issues, were very similar to the observations of other depository institutions participating in the outreach events. Hence, observations by credit unions are mentioned throughout this report among the individual examples from "institutions" as well as in the overall observations. Nevertheless, FinCEN representatives sought to increase their understanding of changes affecting the business of credit unions as well as specific issues unique to credit unions.

Many of the participating credit unions had undergone growth in recent years, either organically or through merger with other institutions or both. The growth in many institutions was facilitated by changes to their membership policy, in particular having evolved beyond the original affiliation that the credit union was formed to serve — for example, a specific corporate or government employer, school district, profession, or immigrant group — to welcoming members, for example, residing within the credit union's geographical area.

Some credit unions discussed how they now advertize publicly to bring in new members, and some of the variety they increasingly see as they collect customer information and assess product needs. Furthermore, a number of credit unions described with pride how they retained most members over long time periods, while also acknowledging that over time this contributed significantly to the increase in diversity of the member population as members or their family moved out of the local region, took new jobs, or otherwise changed aspects that had led them to the initial affiliation with the credit union.

A number of credit unions described how the services to members had evolved over time to not only provide share accounts and share draft accounts to support the individual member, but in cases involving professionals and small businessmen, to accommodate the small business needs. Almost all of the participating credit unions — regardless of asset size or location across the country — had some international activity, usually in the form of wire transfer activity related to customers or members

who had established relationships locally and later moved overseas, processing remittances, or import and export activity. A few of the participating credit unions had very large portions of international business, due to the nature of their membership affiliations.

The following issues were identified by multiple credit unions as unique to credit unions (without distinction as to Federal or State charter).

Shared Branching

Shared branching extends the credit union's ability to provide expanded access or offer more complex and competitive financial services to their memberships.[94] Shared branching and the provision of remote services such as through the internet were also noted as facilitating the ability of individual credit unions to service more varied and geographically diverse memberships. FinCEN discussed the issue of shared branching with the credit unions that participated in the outreach initiative, including how shared branching may also introduce additional challenges or risks from an AML compliance perspective. By nature, in shared branching one credit union is relying on another credit union to help serve a member, and there must be an understanding of the appropriate division of responsibilities.

A possible money laundering risk with respect to shared branching is whether it is possible or feasible for institutions to aggregate multiple transactions at different credit unions within the network for CTR purposes. When asked about this issue, one credit union explained that network-wide transaction information is fed into the credit union's software. However, since different credit unions use different coding systems, compliance personnel are still required to review each shared branching transaction manually. This issue has been raised by the shared branching boards on which credit union personnel participate, though it has yet to be resolved.

One credit union characterized shared branching, from a compliance perspective, as a "nightmare." The credit union is hoping to receive "bright lines" from the National Credit Union Administration (NCUA) regarding who is responsible for what. Another credit union states that it feels the AML responsibilities are appropriately placed on the credit union that opened the account, as the aggregated accounts can only be seen by that credit union, not the shared service center.

94. See http://www.fincen.gov/news_room/rp/files/sar_tti_12.pdf#page=21.

Another credit union mentioned that shared branching is a critical service for its members that are not conducting business at their headquarters, however, it is difficult to get CTR and other BSA-related information from shared service centers. The credit union expressed an interest in receiving assistance from the NCUA in this regard.

Another credit union stated that shared branching is very important for helping the un-banked and under-banked. Shared branching provides a benefit to members through MSBs, which provide "point-of-banking" terminals at check cashers that enable credit union members to make deposits and withdrawals. Through shared branching, the credit union has 130 deposit locations for its members. The credit union notes that BSA compliance requirements at the State and Federal levels are very strong.

One credit union asked about accepting deposits of agents of money transmitters in the shared branching context. The credit union suggested that there needs to be more education on the responsibilities of shared service centers, and that FinCEN should issue guidance on the subject.

While some states have the ability to examine the practices of cooperative services providers to ensure that credit unions are getting information that they need relevant to their compliance, FinCEN will continue discussing this issue with the NCUA and the National Association of State Credit Union Supervisors (NASCUS), including the possible need for more guidance to industry and/or examiners on this issue. FinCEN has asked credit union associations for their views on shared branching, and welcomes further insights and suggestions in this area.

Membership

As mentioned earlier in the report, there were discussions regarding the challenges of exiting relationships after a certain number of SAR filings. For credit unions, you are not a customer; you are a *member* and co-owner of the institution, which makes ending that relationship much more challenging.

In order to expel a member when necessary, some credit unions spoke of restricting services when an account was deemed suspicious, ultimately resulting in the member incurring fees that if left unpaid would allow the account to be closed by default. The credit unions that "fee out" members they wish to expel explained that they are either never challenged for taking these measures or that such challenges are easy to deflect.

The credit unions stated that that if they identify suspicious activity involving possible violations of law, they would not wish unwittingly to continue such relationships. They suggested that it might be helpful for FinCEN and/or their regulators to provide further guidance in this area.

Additional Issues

Enterprise-Wide Risk Management

One institution noted its strong support of a move toward enterprise-wide risk management (ERM). The institution's representatives believe that ERM will be very useful to institutions if they can implement this type of program. The institution noted that ERM is a large effort, and some small institutions may find it to be cost-prohibitive, but in the long run, ERM would be well-worth the implementation costs. The biggest problem is to automate an integrated system. The cost of technical expertise is great. The institution has been working on implementing an ERM system for 3 years and it does not expect to fully implement the system for at least 2 more years. The institution's representatives are not aware of any processor that can currently accommodate a comprehensive ERM system.

Jewelers

FinCEN issued an Interim Final Rule requiring AML programs for dealers in precious metals, precious stones, and jewels ("covered goods"), on June 9, 2005.[95] Most retailers in this industry are not required to establish anti-money laundering programs. The Interim Final Rule applies to "dealers" that have purchased *and* sold at least $50,000 worth of "covered goods" during the preceding year. The dollar threshold is intended to ensure that the rule only applies to persons engaged in the business of buying and selling a significant amount of these items, rather than small businesses, occasional dealers and persons dealing in such items for hobby purposes.

The Interim Final Rule requires dealers, among other things, to implement an anti-money laundering program that includes policies, procedures, and internal controls to prevent themselves from being used to facilitate money laundering or terrorist financing. In order to develop an effective program tailored to their business, dealers are required to assess the vulnerabilities of their operations to money laundering and terrorist financing, thus emphasizing a risk-based approach to AML program management.

One of the institutions FinCEN met with has a branch located in New York City's "diamond district." The institution currently has about 70 accounts with jewelers and conducts a semi-annual account review to look at all checks and deposits.

95. See http://www.fincen.gov/news_room/nr/pdf/20050603.pdf

When the institution opens a new account, one of the questions it asks is whether the individual is in the jewelry business. If the business is a jeweler, the institution shows them the AML requirements (covering dealers that have purchased and sold at least $50,000 worth of "covered goods" during the preceding year) and asks the business to certify whether it is covered by the requirement.

The institution asked for guidance on its AML obligations when providing services to a jewelry business. For example, if the customer says that it is not covered by the rule, is the institution ultimately responsible for ensuring that the jeweler has an AML program in place? FinCEN acknowledged the complexity of the issue depending on the specific facts and circumstances and analogized the approach to reasonable steps taken by depository institutions in serving other types of customers (such as MSBs or casinos) that have independent BSA obligations.[96]

To date, no customers have closed their accounts when questioned if they are covered entities. The institution has one customer that it mandated developing an AML program and conducting an internal audit due to the volume of activity. The institution paid for half of the cost of the internal audit.

The institution does not offer bulk cash service to jewelers. These clients fund their accounts with the institution through check deposits and funds transfers. At one time, the institution was looking at all activity on jeweler accounts, but the institution has more recently moved to risk rating the account at opening. The institution notes that it has filed some SARs on these customers, mostly structuring activity to avoid the requirement to file a report of cash transactions on Form 8300 (which is analogous to CTRs for depository institutions). The institution was curious why jewelers are not required to file SARs under FinCEN regulations.

Observations on Certain Accounts

One institution noted that at one point it maintained accounts for corporate check cashers, however, it closed these accounts after noticing an increase in suspicious activity. In addition, State authorities were very slow to license these entities. Another area noted by one institution involves the growing number of charity accounts, some of which raised questions for the institution as to whether the charity was fully engaged in charitable activities, including activities consistent with its preferred tax status.

96. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf (p. 307)

Armored Car Ruling

On July 2, 2009, FinCEN issued a ruling titled *Treatment of Deposits by Armored Cars for Currency Transaction Report (CTR) Purposes*.[97] The intent of this ruling was to clarify that armored cars that are conducting transactions on behalf of bank customers should be treated differently from armored cars that are conducting transactions on behalf of a bank.

FinCEN discussed a few institutions' concerns with this guidance during the course of our outreach, and is also aware of concerns that have been put forth by other representatives of both the banking and armored car industries. FinCEN continues to review this subject, and in deciding what additional steps may be taken, FinCEN will balance both the obligations that this ruling may place on the affected industries against the benefit that law enforcement will receive in having this CTR information available.

Money Laundering Pattern Recognition

Institutions requested general guidance on how to identify transactions involving schemes such as internet gambling, corporate takeovers, Ponzi schemes, "secret shopper" scams,[98] and other transactions. As one institution explained, employees routinely see money moving within the institution, making it difficult to know when certain transactions should trigger an investigation and/or a SAR.

FinCEN mentioned that sometimes the best source for information on what constitutes a suspicious transaction comes from customers who complain that they have been the victim of a scam. However, FinCEN also recognizes there is an interest from institutions to receive more guidance on money laundering pattern recognition.

97. See http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-r002.pdf

98. "Secret shopping" is a tool used by legitimate market research companies to measure the quality of retail service and to learn other information about the experience of purchasing specific products. In some instances, the "secret shopper" is instructed to purchase products to be sent to a market research company, which later reimburses the "secret shopper." However, sham market research companies provide "secret shoppers" with fake reimbursement checks. One institution indicated that it sometimes holds certain checks for 180 days as an anti-fraud mechanism when it suspects a "secret shopping" scam. For more information, see http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf.


FINANCIAL CRIMES
ENFORCEMENT NETWORK