

FDIC New York Region Regulatory Teleconference
BSA Today – Regulatory Tips, Trends, and Hot Topics
March 3, 2015

Deputy Regional Director John Conneely: Good afternoon everyone and welcome to today's conference call entitled BSA Today – Regulatory Tips, Trends, and Hot Topics. I'm John Conneely, the New York Regional Director for the FDIC. I would like to thank you for joining us.

During today's call we will focus on recent BSA trends and hot topics from a regulatory standpoint, as well as tips to assist the Board and management in ensuring overall BSA/AML compliance. Emphasis will be on the Financial Crimes Enforcement Network's (or FinCEN's) guidance on corporate compliance, recent BSA issues and trends, and emerging hot topics. The session will also cover suspicious activity reporting, as well as common suspicious activity report (SAR) misconceptions and common causes for apparent SAR violations.

We view these conference calls as an opportunity to share regulatory guidance and discuss items of supervisory importance with a wide audience. These calls also present us with the opportunity to hear directly from you regarding any questions you may have on issues discussed.

In addition to our quarterly conference calls, the FDIC partners with various trade associations to conduct Directors' Colleges. The Directors' College is an interactive one-day seminar that provides ongoing education to bank directors on current topics in various elements of bank supervision. It is designed to help directors, both new and experienced, stay abreast of the changing regulatory and economic environment.

The FDIC also provides a Technical Assistance Video Program, which is a series of educational videos designed to provide useful information to bank directors, officers and employees on areas of supervisory focus and regulatory changes. One of the videos discusses BSA, and these videos are available on the fdic.gov website.

We very much appreciate your participation in today's call. Your confirmation email included a link to the PowerPoint slides for the various topics being covered. The PowerPoint slides should aid you in following today's presentation and can be used for future reference.

If you have any questions relating to this presentation, please email us at nycalls@fdic.gov. There will be a question and answer session at the end of the presentation. The operator will provide instructions for how to ask a telephonic question.

A written transcript and question and answer document will be posted to the same Web link you used to register for today's call.

With me today are two presenters, Special Activities Case Managers Kristi Keating and Rebecca Williams, who will discuss current regulatory guidance and helpful hints to assist your bank in developing an effective BSA/AML program.

It's now my pleasure to turn the program over to Special Activities Case Manager Kristi Keating who will begin the presentation.

Special Activities Case Manager Kristi Keating: Thank you, John. Bank Secrecy Act/Anti -Money Laundering or as we will abbreviate it today as BSA/AML, is a hot topic and high priority at institutions these days. As regulators we use various methods to communicate BSA/AML expectations to all financial institutions. Examples of this communication include the updated and revised FFIEC BSA/AML Examination Manual that was issued on December 2, 2014, as well as regulatory guidance and training on laws, regulations, and emerging issues through Financial Institution Letters, Advisories, and outreach events such as this teleconference. Today we offer BSA tips, trends, and hot topics from a regulatory perspective. We will focus on FinCEN's guidance on corporate compliance, regulatory oversight matters, BSA issues and trends in the New York Region, and an emerging wire fraud trend. We will then discuss suspicious activity matters, including reporting, board notification, and confidentiality. At the end of the presentation we will provide links to resources for additional information.

Let's get started; we are on slide 2. The overwhelming majority of banks in the New York Region are doing a good job overseeing BSA/AML compliance; however, there have been some institutions with high profile BSA/AML deficiencies that have triggered recent civil and criminal enforcement actions. While the actions are usually against the institutions, there are statutes which give certain regulatory agencies the ability to assess individual civil money penalties and removal actions. On August 11, 2014, a FinCEN Advisory was issued to U.S. Financial Institutions on Promoting a Culture of Compliance. I would like to spend a few minutes briefly reviewing the FinCEN Advisory with you today and highlight the ways that financial institutions and their leadership can improve and strengthen their organization's compliance with the Bank Secrecy Act. It is important to remember that directors and executive management set the tone for the bank – regardless of the size of the bank and business model, a bank with a poor culture of compliance is likely to have deficiencies in its BSA/AML program.

As noted in guidance, leadership should be engaged. In order for a BSA/AML program to be effective, it should have the demonstrated support of bank leadership. Leadership includes the board of directors, and senior and executive management. These leaders do not have to be involved in day-to-day operations, but generally should be well-informed. They should also have periodic training and an appropriate understanding of their bank's BSA/AML risks to make informed decisions. Further, they should ensure that the BSA/AML Officer has sufficient authority to appropriately execute his or her role without undue board and senior management influence.

This leads me to the next point. Compliance should not be compromised by revenue interests. Banks are in the business of making money, but a bank's interest in generating revenue should not compromise efforts to effectively manage and mitigate BSA deficiencies and risks, including the submission of appropriate and accurate reports such as suspicious activity reports (SARs) and currency transaction reports (CTRs) to FinCEN regardless of the impact on revenue. And it is always better for management to allocate sufficient attention and resources to the BSA/AML program up front, rather than face the much higher cost of remediation and possible penalties later.

It is also important that information be shared throughout the organization. Recent enforcement actions noted that certain departments within banks had information in their possession but did not share that information with the BSA Department.

How did that happen? There may have been lack of appropriate mechanisms for sharing, lack of understanding of the BSA implications, or it may have been intentional. It is important for all business lines to share information with the BSA Department. For example, legal should share subpoenas and law enforcement requests, consumer compliance should share public actions it may be aware of, and lenders should share loan fraud information and early-payoffs with cash. As regulators we are in regular communication with BSA Officers, who occasionally cite the reason they did not investigate potentially suspicious activity and file a SAR is that either no one communicated the suspicious activity to them, or that the BSA Officer had the information and was told by senior management not to file the SAR.

Please turn to slide 3.

Additionally, leadership should provide adequate human and technological resources. Not only should management designate a qualified BSA Officer with sufficient authority, appropriate support staff should be devoted based upon the bank's risk profile. There should be enough trained staff to review and complete all reports and suspicious activity alerts in a timely manner. Failure to do so could cause the untimely reporting of suspicious activity and result in apparent violations for your bank. Also, consider the risk profile and volume of activity of your institution when deciding the type and complexity of suspicious activity monitoring systems.

Management should ensure that the BSA/AML program is effective and tested by an independent and competent party. This should be done in conjunction with a proper ongoing risk assessment, sound customer due diligence process, and appropriate monitoring and reporting of suspicious activity. Leadership should ensure that the party testing BSA compliance is independent, qualified, unbiased, and does not have conflicting business interests. As regulators, we are finding that while banks generally contract for the requisite independent reviews, auditors sometimes do not perform adequate transaction testing or do not understand the risk profile of the bank being tested. To ensure that you are getting what you are paying for, review the scope of the audit, review the auditors' resumes, ask for references, and have a qualified individual review the workpapers.

Finally, leadership and staff should understand how their BSA reports are used. The filing of these reports, primarily SARs and CTRs, result in some of the most important information available to law enforcement and others safeguarding the nation. These reports can be used for:

- Tips for investigations;
- Expanding existing investigations; and
- Identifying significant relationships, trends, and patterns.

These six areas just discussed illustrate how financial institutions and their leadership can help improve and strengthen overall organizational compliance with BSA obligations.

Please turn to slide 4.

As regulators in the New York Region, we sometimes hear that banks are facing increased BSA/AML scrutiny, and it appears that apparent violations and enforcement actions are increasing. This is not as prevalent as you may think, as BSA enforcement actions are actually declining nationwide. In the next couple of slides I will discuss the reasons for this perception and from a regulator's view why this appears to be happening, as well as the causes for the apparent violations and potential BSA program breakdowns.

First the good news: Let me give you some BSA/AML statistics for the New York Region, which includes the Boston Area, and then the nation as a whole. As I stated before, most of the banks in the New York Region are doing a good job with overall BSA/AML compliance. In New York, we oversee approximately 500 state non-member banks. As of year-end 2014, there are only 9 banks under BSA-related Consent Orders, which is a formal enforcement action. That's less than two percent of all banks we supervise. As a nation, BSA compliance continues to improve. There are approximately 4,100 state non-member banks nationwide, and as of year-end 2014, there were only 43 banks nationwide under BSA-related Consent Orders. That's less than one percent of the state non-member banks in the nation, and also indicative of good management oversight and compliance with the Bank Secrecy Act.

So why does it appear that there is increased emphasis on BSA/AML?

One reason is the emerging and more complex products, services, and markets that did not exist ten, even five years ago. These include complex third party processing arrangements; an increase in ACH transactions; an increase in prepaid access arrangements; additional foreign correspondent account matters, including regulations relating to Iran; and monitoring and reporting obligations for bulk currency. Add to this virtual currency, human trafficking, and marijuana transactions. Then add new technologies and new ways to conduct banking, such as mobile-to-mobile, internet, and remote deposit capture, and you can understand the extra assessment by the regulators and the importance of qualified and informed BSA Officers and BSA staff in your bank. Clearly the BSA environment has changed.

When you combine all the new products, services, and markets with all the new technologies, there are endless new methods for criminals to launder money, traffic narcotics, and finance terrorist activities.

Let's move to slide 5.

Some additional reasons that it appears that extra attention is devoted to BSA/AML is that during the recent financial crisis there were instances where appropriate resources and attention were not dedicated to maintaining and sustaining the core components of the BSA/AML program, leading to gaps that regulators are seeing now. For example, BSA/AML surveillance systems may have been set up at a point in time, however, the growth and diversity of the bank's infrastructure may make these systems obsolete. As a result, there may be criticism of the suspicious activity monitoring, identification, and reporting systems.

Additionally, examiners have more sophisticated tools and comprehensive guidance today and are able to identify trends, patterns, and commonalities we could not before.

As regulators we understand that it may take time to address recommendations or deficiencies in a BSA program. When examining banks with BSA issues, we take into account how the BSA Officer and management have identified the issues that

need to be updated or changed, and any action plan developed to assist in the remediation effort that assigns accountability and reasonable time lines.

Please turn to slide 6.

Now I would like to discuss some of the more prevalent areas of internal control and other BSA/AML weaknesses noted in the New York Region. These weaknesses may result in BSA pillar and other apparent violations and are as follows:

The BSA program has not kept pace with the bank's growth and risk profile. This is the most prevalent issue we are seeing. Some banks are growing and adding new customers, products, services, and markets without adding the appropriate infrastructure along the way, often without full vetting of BSA risks through the BSA Officer, management, and the Board of Directors. There has been recent discussion as to what type of customer or business a bank may serve. As stated in the January 28, 2015, Financial Institution Letter 5-2015, the FDIC encourages a risk-based approach in assessing individual customers. As long as the bank can properly manage these customer relationships and effectively manage these risks, the bank is neither prohibited nor discouraged from providing services to any category of customer accounts or individual customer operating in compliance with applicable state and federal law.

The bank's leadership is not fully engaged as I discussed at the beginning of this presentation.

Another trend seen is the difficulty **in finding and retaining qualified BSA Officers and support staff.** Finding and retaining qualified BSA officers and staff is a concern we repeatedly hear. We often see qualified BSA Officers moving from bank to bank for a more competitive salary. We also see banks having difficulty filling lower level compliance positions such as analysts and investigators. A tool that can assist management with this issue is a BSA Officer succession plan, which includes a recruitment and training plan for entry level positions.

We are also seeing instances of **insufficient resources/training dedicated to BSA compliance** as also mentioned earlier in the presentation. Many banks have a

qualified, competent BSA Officer and staff, but the volume of work compared to the staffing resources is such that they cannot clear alerts or file appropriate reports in a timely manner, often leading to examination deficiencies or the citing of an apparent violation. We also see issues where BSA training is infrequent and has not kept pace with emerging BSA risks. Further, we see BSA staff whose BSA training is not job-specific, resulting in personnel that may not clearly understand their specific BSA/AML related duties. For example, there may be a wire room operator whose job it is to approve wires, but this person does not receive adequate training on international wires to high risk and non-cooperative countries. As a result, a wire may be released to a country of concern without completion of the appropriate due diligence.

Over reliance on third party consultants. While banks often use third party consultants to help remediate BSA deficiencies, develop BSA policies and procedures, and help fill short term gaps in BSA staffing, banks are reminded that the Board and management are ultimately responsible for the BSA/AML program and its compliance with laws and regulations. It is up to the each bank to ensure that the expertise and quality of the third party consultants is appropriate for the risk profile of their bank.

Let's go to slide 7.

Inadequate customer due diligence (CDD) and enhanced due diligence (EDD). This is an area where we often find deficiencies. The bank should have CDD policies, procedures and processes that enable the bank to understand with relative certainty the types of transactions in which a customer is likely to engage. Further, the bank should also have EDD policies, procedures, and processes for bank-identified higher risk customers. EDD procedures should outline which customers should be reviewed more closely at account opening and the frequency of review throughout the term of the relationship.

Another trend we are seeing is the **failure to identify, monitor, and/or report suspicious activity**, which may result in apparent violations. This trend occurs for a variety of reasons, including inadequate CDD/EDD, insufficient monitoring systems, inadequate training, poor communication across business lines, management's reluctance to file SARs on certain customers, and not enough staff

to properly clear alerts or conduct thorough investigations. We will discuss suspicious activity reporting issues in more detail later in the presentation.

Also remember that **cash does not and should not solely drive BSA/AML compliance programs**. Some banks mistakenly believe that BSA/AML compliance and monitoring is primarily applicable to cash-based activity. With the growth of banks without a physical presence, electronic banking, and electronic and virtual cash, banks must develop and implement effective BSA/AML policies, procedures, and processes to address all types of transactions, not just cash.

We also see issues with transaction monitoring systems such as meaningful alerts not being produced. Banks should fine tune scenarios to create effective alerts. Additionally, as previously discussed, sometimes the systems chosen are not appropriate for the bank's size, risk profile and complexity, and cannot produce the reports needed for some of the bank's products.

Finally, we are seeing **instances where the independent BSA/AML audit scope, transaction testing, and experience of auditors is not sufficient for the bank's risk profile**. It is up to management to ensure that the firm and actual auditors are qualified and the bank can rely on the findings and conclusions, including products and services which may be unique to your bank. Management should also ensure that appropriate transaction testing is conducted and documented.

Moving on to slide 8.

As discussed, there have been many new trends in money laundering and fraud, and numerous hot topics. In order to increase your awareness of one of the more prevalent schemes we are seeing, today we will focus on account take-overs through wire transfer activity. There has been a recent increase in wire fraud in the New York Region, and recently the New Jersey Department of Banking and Insurance sent guidance on this subject to its banks. The guidance, in part, stated that multiple banks have reported wire frauds that share common characteristics, including the following:

- Accounts were typically corporate accounts actively engaged in wire transfer activity, although there have been some personal accounts compromised.

- The majority of fraudulent wires were sent overseas to locations such as Hong Kong, China, and Taiwan.
- Customer e-mail accounts were apparently hacked and wire request documentation received by the bank appeared to be legitimate.
- Multiple requests were received on a customer's account.
- The fraud was identified by the customer upon reviewing account statements or bank balances.
- Bank personnel did not make calls to the customer to verify the transaction or allowed suspect transactions to occur without following bank policy.

Although controls are generally strong at financial institutions, new methods of obtaining customer information are constantly evolving. Criminals look for the weakest link in the security chain, which is often with a depositor. Various techniques are used to obtain valid online banking credentials, which include keylogging malware, e-mail phishing and exploitation of weak controls over passwords and account numbers. Typically corporate accounts are targeted due to larger balances and multiple wire transactions; however, personal accounts can also be compromised. In the New York Region, we have seen recent instances of both corporate and personal account takeovers by wire, often involving millions of dollars.

A key risk mitigation practice that can greatly increase a bank's chances of preventing fraudulent wire activity is the use of multi-factor authentication. Bank management should insist on authenticating every wire transfer, even if customers claim to have too high a volume of activity to be contacted on each transaction. A call back to verify customer wires could have saved multiple losses in recent months. Wires should be verified even if the customer is out of the country or claims to be unavailable. Management must make it clear that bank employees should never be intimidated into bypassing internal control procedures by customers who feel they are entitled to preferential treatment. Banks should also encourage customers to reconcile their bank accounts on a regular basis. A common practice amongst criminals is to repeatedly send wires from customers' accounts until the fraudulent activity is noticed.

Customer awareness and education is another key to reducing the cyber-security risk faced by banks and customers. If account holders recognize the vulnerabilities, they can increase their vigilance at protecting their account information. Certain customers may be comfortable with sending multiple wires

using abbreviated security practices; while this may have worked successfully in the past, recent events have raised the risk of fraudulent activity. Employee training and re-training is crucial to every bank's security program as bank personnel are the last line of defense against fraudulent activity. Also, management should keep in mind that the bank's insurance may not cover the loss if it can be determined there was breakdown of internal controls, or liability, on the bank's part, so it very crucial that employees are well trained on wire controls and procedures.

Moving on to slide 9. Special Activities Case Manager Rebecca Williams will now discuss suspicious activity matters, including reporting, board notification, and confidentiality.

Special Activities Case Manager Rebecca Williams: Thank you, Kristi. I'd like to turn the topic of discussion to suspicious activity reporting. This is an area in which the FDIC receives numerous questions from banks. It is also an area where examiners sometimes identify weaknesses, apparent violations, or room for improvement.

Suspicious Activity Reports, or SARs, are an important tool for law enforcement to combat crime. SARs are also an important tool to assist bank regulatory agencies in their supervisory and enforcement capacities. Part 353 of the FDIC Rules and Regulations governs when FDIC-supervised banks are required to file SARs. Slide 9 summarizes the SAR filing criteria outlined in the regulations. To help you avoid potential SAR deficiencies and apparent violations, I'd like to point out a few areas of the SAR filing criteria that are sometimes overlooked or misunderstood.

In situations where there is insider abuse, it is important for banks to remember that there is no dollar threshold requirement for SAR filing. In other words, insider abuse involving any amount should be reported in a SAR. One of the more common examples of insider abuse is embezzlement; however, insider abuse could also take the form of loan fraud, wire fraud, or any other fraud or crime involving an insider of the bank. We sometimes encounter banks that think the \$5,000 threshold applies to insider abuse situations, which is incorrect. We also sometimes encounter banks that think there has to be a loss to the institution for a SAR to be warranted, and this is also incorrect. Whenever the bank detects any known or suspected federal criminal violation or pattern of criminal violations, and

the bank has a substantial basis for identifying one of the bank's directors, officers, employees, agents, or other institution-affiliated parties as having committed or aided in the criminal violation, a SAR should be filed - regardless of the amount involved in the violation, and regardless of any loss.

Regarding criminal violations, it is important for banks to remember that they do not necessarily need to “know” a criminal violation has occurred; they merely need to “suspect” a criminal violation has occurred. We sometimes hear from bankers that they did not file a SAR because they could not “prove” or “confirm” that a crime occurred. It is important to remember that banks are not obligated to investigate or confirm a crime; criminal investigation is the responsibility of law enforcement. But it is a bank’s responsibility to report known “or suspected” criminal violations by filing a SAR.

Another common misunderstanding involves the SAR dollar thresholds. We sometimes find that banks think the \$5,000 and \$25,000 SAR thresholds pertain to the loss amount. But that is not the case. The SAR dollar threshold is considered to be met if the suspicious activity equals or exceeds the threshold, regardless of any loss.

Now I’d like to draw your attention to slide 10.

For potential money laundering or violations of the Bank Secrecy Act, it is important to remember that banks are responsible for reporting suspicious activity if the bank “knows, suspects, or has reason to suspect” that a transaction conducted or attempted by, at, or through the bank either: involves funds derived from illegal activity, or is an attempt to disguise funds derived from illegal activity; is designed to evade BSA regulations, or lacks a business or apparent lawful purpose, or is not the sort of transaction in which the customer would normally be expected to engage.

I’d like to emphasize the wording of this section of the regulation. The wording clearly demonstrates that a bank does not necessarily need to “know,” but merely needs to “suspect” or have “reason to suspect” potential money laundering or violations of the Bank Secrecy Act.

We sometimes find that banks are hesitant to file SARs because they are not sure the funds are derived from illegal activity. But banks need to remember that the regulation requires a bank to file a SAR if they “know, suspect, or have reason to suspect” the funds are derived from illegal activity. They don’t have to be sure the funds are derived from illegal activity.

We also sometimes encounter banks that have not filed SARs even though they have identified suspected structuring of cash transactions designed to evade Currency Transaction Report requirements. Their reason for not filing SARs is that they are “confident that the business’ activity is legal” or they’ll tell us “this is how the customer always transacts their business, and even though it looks like structuring, it is normal for this customer and this industry.” But banks need to remember that, suspected structuring (or any other attempt to evade BSA regulations) is cause for SAR filing, even if a bank is confident that the funds flowing through the account are from otherwise legal activity, and even if the activity is normal for that customer and for that industry. In other words, the three bullets on Slide 10 are mutually exclusive, and a SAR should be filed if any of the three criteria are met. So, even if the bank is confident that the business is legitimate, and even if the customer has been transacting its business this way for a long time, if the bank “knows, suspects, or has reason to suspect” that the customer is structuring, then a SAR should be filed if dollar thresholds are met.

Please turn to slide 11.

As summarized on this slide, the SAR rules require that a SAR be filed no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection, a bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In addition to the SAR filing timeframes prescribed by regulation, FinCEN guidance also allows an expanded filing deadline for continuing suspicious activity. Financial institutions may file SARs for continuing activity after a 90 day review, with the filing deadline being 120 days after the date of the previously related SAR.

I’d like to talk a bit about when the 30-day clock starts ticking for SAR filing, because this is sometimes a source of confusion. Often times a bank will be alerted to “unusual” activity, perhaps from an exception report or review of transaction activity, but that is not necessarily when the 30-day clock starts ticking.

It is typical and expected that a bank may need to conduct additional research upon identification of unusual activity to determine whether a SAR is warranted. The time period to file a SAR starts when the institution, in the course of its review or as a result of other factors, reaches the conclusion in which it knows, or has reason to suspect, that the activity under review meets one or more of the definitions of suspicious activity.

So the phrase “initial detection” should not necessarily be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they were inconsistent with an account holder’s normal account activity. The institution’s automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not necessarily be considered “initial detection” of potential suspicious activity. The 30-day clock does not start ticking until an appropriate review is conducted and a determination is made that the transaction under review is “suspicious” within the meaning of SAR regulations.

With that being said, an important expectation that banks should be aware of is that review should be initiated “promptly” upon identification of unusual activity. Also, the timeframe required for completing review of the identified activity may vary given the situation, but in any event, the review should be completed within a reasonable period of time. What constitutes a “reasonable period of time” will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the suspicious activity monitoring, reporting, and decision-making process of each institution. One key factor is that an institution has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed. Additionally, banks should have policies, procedures, and processes to ensure the timely generation of, timely review of, and timely response to reports used to identify unusual activities.

So just to recap, appropriate review of unusual activity should be initiated promptly and take a reasonable period of time, and only when the bank determines that the activity is suspicious within the meaning of SAR regulations, does the 30-day clock start ticking.

Let's move to slide 12.

These are some of the more common causes examiners have identified that led to untimely SAR filing or failure to file SARs.

Resource issues sometimes identified during examinations include over-burdened or not enough staff assigned to review potential suspicious activity incident reports, or to complete potential suspicious activity research. The result of such resource issues is often that incident reports are not reviewed timely, and research is not completed within a reasonable period of time. Banks should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the bank's overall risk profile and the volume of transactions. Staffing levels should be sufficient to review reports and alerts timely, and appropriately investigate items. It is also important for banks to remember that the volume of system alerts and investigations should not be tailored solely to existing staffing levels.

Red flags that examiners sometimes identify during examinations that indicate there may be a resource issue includes: significant backlog of suspicious activity alerts in need of review or investigation, investigations taking unreasonable periods of time, incomplete investigations, and unreasonably high monitoring system settings.

Suspicious activity monitoring weaknesses can also result in failure to file SARs because they can prevent banks from identifying or reporting suspicious activity. For example, if a bank is not adequately monitoring for structuring, perhaps due to a system setting issue, suspicious activity could go undetected and therefore unreported. Also, if a particular area of the bank is not adequately monitored for suspicious activity, such as a specific business line or a specific product or service, suspicious activity could go undetected. Additionally, if a bank does not have an adequate secondary review process to ensure SAR decisions, including decisions not to file a SAR, are reasonable and supported, suspicious activity could go unreported. Those are just a few examples of monitoring weaknesses that can lead to failure to file SARs.

Inadequate unusual activity referral procedures can also result in failure to file SARs or untimely SARs. During the course of day-to-day operations, employees

may observe unusual or potentially suspicious transaction activity. Banks should implement appropriate training, policies, and procedures to ensure that personnel adhere to the bank's internal processes for identification and referral of potentially suspicious activity. Banks should have procedures in place for staff to report unusual activity through appropriate designated channels for SAR consideration. Also, banks should have policies, procedures, and processes in place for referring unusual activity from all areas of the bank and all business lines to the personnel or department responsible for evaluating unusual activity.

Examiners sometimes discover there are no formal referral procedures, which can lead to potential suspicious activity not being properly reported to bank personnel for SAR consideration purposes. Procedures should be in place to guide bank personnel on what to do when they identify potentially suspicious activity. Bank staff from all areas of the bank should be familiar with the procedures and aware of their referral responsibilities.

Examiners also sometimes see too many levels in a bank's referral process, which can either result in unusual or suspicious activity not being brought to the attention of the ultimate SAR filing decision-maker, or can result in untimely SAR filings. For example, if a bank's internal process for referral of unusual activity identified by a loan originator includes referral to the loan officer, then to the Vice President of Lending, then to the Senior Vice President, and then to the BSA Officer, there is a chance that anywhere along that referral chain someone, perhaps someone who is not knowledgeable of the SAR rules, may decide the matter does not warrant referral to the next person in the chain. If that happens, the bank's designated SAR decision-maker may never even be alerted to the potential suspicious activity, and will not have had the opportunity to determine if a SAR should be filed. In this same example, even if the referral ultimately makes it to the BSA Officer, an unreasonable amount of time may have passed due to the number of referral layers, causing an untimely SAR.

Misunderstanding of SAR Regulations is also a common cause for failure to file SARs. For example, examiners commonly identify apparent violations for failure to file SARs involving insiders when banks mistakenly think the activity was too small to warrant a SAR filing. As I mentioned earlier, SARs should be filed on insider abuse involving any dollar amount, because there is no dollar threshold for insider SARs. Examiners also commonly identify apparent violations for failure to file SARs when banks mistakenly think, because there was no loss associated with

the suspicious activity, a SAR was not required. As mentioned before, SAR dollar thresholds are not tied to the loss amount, but rather pertain to the suspicious activity amount. To clarify this point, let me give you a specific example. If a \$30,000 fraudulent check is deposited at the bank, but the bank recognizes the check is fraudulent and therefore returns it and does not sustain a loss, a SAR would be warranted because the SAR dollar threshold has been met even though the bank did not sustain a loss.

Training weaknesses are also a common cause for untimely SARs or failure to file SARs. Examiners sometimes find that bank staff is not properly trained on SAR regulations, bank policy, suspicious activity identification, or the BSA/AML risks presented by the bank's products, services, or relationships.

Training should be commensurate with the risk profile of the bank. For example, if the bank has identified high-risk products, services, or relationships, it is critical for BSA staff to be adequately trained regarding the BSA/AML risks posed by these products, services, and relationships. Additionally, BSA staff and relevant department staff should be properly trained to recognize and report red flags and potentially suspicious activity in these areas.

It is important for all bank staff to receive appropriate training in order to be able to recognize and report potentially suspicious activity. Suspicious activity training should be provided bank-wide, to all business lines and departments. To be most effective, it is recommended that suspicious activity training be tailored to the employee's function or department. For example, training could include discussion of different red flags to be aware of in various areas of the bank, such as the teller area, wire transfer area, and loan department.

Next, let's turn to slide 13.

Examiners often receive questions from banks on how much detail can and should be provided to the board of directors regarding SARs. So I want to speak to you about certain requirements and options that banks have in this regard.

Banks are required by SAR regulation to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations

do not mandate a particular notification format. So banks have flexibility in structuring their format. Banks may provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide redacted SARs, or SAR summaries, or tables of SARs filed for specific violation types, or other forms of notification.

Regardless of the notification format used by the bank, management should provide sufficient information regarding SAR filings for the board or committee members to fulfill their fiduciary duty. Also, because board members are being notified of SAR filings, board members should be aware and mindful of the confidential nature of SARs. Therefore, periodic board training regarding SAR confidentiality is an important control that every bank should implement; and training is particularly important for banks who provide actual copies of SARs to board members, because in general, the more information and detail provided to board members regarding SAR filings, the more important it is they understand the SAR confidentiality rules.

This segues nicely to our next topic, SAR confidentiality. **So please turn to slide 14.**

As slide 14 highlights, no bank, director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Also, a SAR and any information that would reveal the existence of a SAR are confidential, except as necessary to fulfill BSA obligations and responsibilities.

SAR confidentiality issues periodically come to the FDIC's attention. For example, we sometimes see instances of unauthorized SAR disclosures, such as SARs mentioned in local newspapers, SARs provided or their existence disclosed to unauthorized parties, or SARs provided in response to a subpoena from an unauthorized agency. Directors, officers, employees, and agents with knowledge of or access to SARs should be familiar with regulations covering SAR confidentiality. Training is important, as are controls that help maintain SAR confidentiality and minimize the risk of unauthorized disclosure.

That being said, certain SAR disclosures are allowed, and some are necessary to fulfill BSA obligations and responsibilities. Probably the most common example

of authorized SAR disclosure is providing SARs, or SAR information, to law enforcement or the bank's regulatory agency, upon request.

Slide 15 lists some outstanding guidance on SAR confidentiality that I'd like to briefly discuss, so **let's move on to slide 15.**

Whenever banks have questions about SAR confidentiality or questions on how to respond to law enforcement requests for SAR information, I usually refer them to one or all of these documents, as the answers to their questions can usually be found in this guidance.

The 2007 guidance, issued by FinCEN, discusses bank responsibilities regarding providing SARs and SAR supporting documents to appropriate law enforcement and appropriate supervisory agencies upon request.

FinCEN's 2010 guidance discusses expectations, reinforces the requirement to preserve SAR confidentiality, and clarifies the agencies that banks are authorized to provide SARs and SAR supporting documents to, upon request. Specifically, the guidance states that banks are authorized to provide SARs and SAR supporting documents to FinCEN; to federal, state, and local law enforcement; and to federal and state regulatory agencies that examine the bank for BSA compliance.

The 2012 FinCEN guidance is a reminder of the importance of maintaining SAR confidentiality, and it discusses the kinds of controls a bank can implement to help maintain SAR confidentiality.

If your institution receives a request for SARs or SAR supporting documents, please refer to the guidance listed on slide 15. If you are at all in doubt whether you are authorized to provide SAR information to the requesting agency, you can always contact FinCEN or your federal financial regulator for additional guidance and clarification.

Next, let's turn to slide 16.

One common question the FDIC receives from banks involves continuing suspicious activity on the part of a bank customer. Banks periodically ask if they are required to close accounts after filing a certain number of SARs on a customer.

The answer is that there is no specific rule or expectation for whether or when to close an account due to SAR filings. Ultimately, the decision to maintain or close an account should be made by the bank in accordance with its own standards and guidelines. However, there is an expectation that banks have policies and procedures in place to at least consider whether account closure is appropriate due to repeat SAR filings. Specifically, the bank should develop policies, procedures, and processes indicating when to escalate issues identified as a result of repeat SAR filings on accounts.

At a minimum, the bank's procedures should include the items listed on the next slide, so **let's continue on to slide 17.**

So for continuing SAR situations, bank procedures should include: review by senior management, such as the BSA 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; and criteria for when to notify law enforcement.

That concludes our prepared remarks.

For your information, **slide 18** includes Internet links to some of the guidance we've referenced today.

At this time, I'd like to turn the presentation back over to Deputy Regional Director John Conneely for closing comments.

Deputy Regional Director John Conneely: Thank you, Kristi and Rebecca. The purpose of today's call was to discuss recent BSA trends and hot topics, and provide you some BSA compliance tips. We hope you found the information in this afternoon's teleconference relevant and useful. Contact information for today's presenters is included on slide 19. Please feel free to contact any of us with

questions specific to your institution. At this time, we would like to open the discussion for questions and comments.