

# SARs

**Imagine working overtime yet again to add important detail to a suspicious activity report (SAR), making sure that law enforcement gets the entire picture of the activity that you are observing. Also imagine this activity is related to a well-known, high-ranking government official. You submit the report and continue to monitor the activity and go on with your business ...**

# after Spitzer

BY MAUREEN E. CAROLLO, CRCM

**W**EKS LATER, YOU RECEIVE A PHONE CALL FROM LAW ENFORCEMENT OFFICIALS, who visit your bank to discuss the SAR and obtain the supporting documentation you referenced. Of course you go through the steps to verify law enforcement authority before handing over the information. You feel secure and confident about doing so because everyone knows that the SAR won't be disclosed because you and the bank are protected by the safe harbor provisions of the Bank Secrecy Act (BSA) regulations. And then you see it: the news media is reporting that your bank has been named as one of several that filed SARs in the same high-profile case, and now specific details are being disclosed by an "anonymous" agent of the IRS, the very agency you provided the information to. Would your head be spinning and would your heart skip a beat?

It probably did for the management of HSBC Bank and North Fork Bank, both located in New York, who will forever be linked to former New York Governor Eliot Spitzer's case for allegedly filing SARs.<sup>1</sup> The details disclosed in the various media outlets refer to structuring and other activity that could only have come from a source that had access to the information.

If you are a BSA officer, you might have participated in the collective gasp in mid-March as national media outlets publicized the SAR filing details surrounding the Spitzer case. The comments in the media varied, with some attributing information to an "unnamed source in the IRS"<sup>2</sup> and others claiming high-level knowledge of the contents of those filings. Obviously, we could surmise that the disclosures must have had some merit as they provided the level of detailed information that makes law enforcement officials rub their hands together with glee when they comment that the bank "did the right thing"<sup>3</sup> and then with even more glee, say "We got lucky."

As bankers, we have the right to inquire upstream about what went wrong and why information such as the very fact that a SAR was filed—much less the name of the bank, the name of the suspect, and the nature of the activity—was disclosed. The outcry in general from bankers has been shock and anger. Because the very nature of banking involves maintaining mountains of confidential customer information, we are regularly reminded that we are not only required to keep our customer data secure, but also required to have a formal incident response plan in place in the event this data is compromised while in our control or in the control of a service provider. The Federal Financial Institutions Examination Council (FFIEC) and other federal regulators provide guidelines for dealing with these all-too-common breaches, but what if information as sensitive and privileged as SAR data is disclosed? What

guidance is out there for bankers to turn to then?

Unfortunately, not much can be done by the bank other than verifying that a disclosure didn't come from an internal source. In any situation like this, legal counsel should be notified and an internal investigation should be conducted to identify the source of the leak. The penalties for disclosure apply to anyone with the knowledge that a SAR was filed and the seriousness of this issue is why banks should establish a "need to know" basis when investigating and researching this type of data. This is a standard practice for most banks, but this approach may be more challenging depending on the structure of the organization, the number of AML department personnel involved, and employee access to monitoring software that tracks such data.

The response outside the bank's walls can vary depending on the situation. There have been many cases in which a private litigant, usually a customer or former customer, felt that the information related to suspected SAR filings should be available to him or her in a court of law. One such example is the Planters National Bank<sup>4</sup> case, in which BizCapital filed a request with the Office of the Comptroller of the Currency (OCC) for information on SARs filed related to Media Direct and its principal, Raymond Reggie. The reason for the request was based on a civil action being taken against the bank in state court and the OCC stated that the facts withstanding, the SAR information was still precluded from being released. The landmark case that is cemented in most of our minds was the *Whitney National Bank v. Karam* in Texas in 2004<sup>5</sup> when individuals filed suit against the bank for defamation, claiming that the bank had "wrongfully accused them of illegal lending activity when it filed a SAR." This was the case that most clearly drove home the fact that the prohibition from disclosure applies to a party requesting information they simply don't have legal access to, regardless of the reason and regardless of what legal avenue may be used to pursue it.

Most of these cases appear to be similar claims of unlawful release of customer information or alleged libel. This case reaffirmed the basis for the safe harbor that was created by the Annunzio-Wylie Anti-Money Laundering Act and was codified at 31 USC Section 5318(g)(3) and simply states that the bank and its employees are protected from any civil liability for following the law and filing a SAR.

In *Whitney*, the court ruled that the bank must not produce documents that provided even the very evidence of the following:

- the fact that a SAR even existed or of its contents
- any communications regarding a SAR or its contents
- any communications with law enforcement that may have been the basis for the filing or that assisted in the filing of a SAR
- any communications that follow the filing of a SAR, aimed at clarifying information in a report
- any records or documentation of any conversations with law enforcement, whether in writing or in oral discussion, that ultimately did *not* end in filing a SAR

**Let me be clear:  
There is no acceptable  
release of SAR data.**

—Steve Hudak,  
chief of public affairs at FinCEN

This case noted that although specific items may not be disclosed, other documents and information regularly obtained in the ordinary course of doing business were *not* prohibited from being disclosed as

long as their existence didn't confirm a SAR filing.<sup>6</sup>

We have discussed what a banker or other related party who may be involved with filing a SAR can't disclose; now let's address the other players. The BSA very simply prohibits anything related to a SAR from being disclosed by bank personnel or agents such as legal counsel. This prohibition also applies to law enforcement, and 31 USC Section 5318(g)(2) states that the disclosure can't be made to anyone involved in the transaction(s) in question. This would quite clearly appear to include the media. The regulation specifically speaks to law enforcement, too, stating that these officials including "an officer or employee of the Federal Government ... who has **any** knowledge that such report was made may [not] disclose to **any** person involved in the transaction that the transaction has been reported."<sup>7</sup>

Because the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) has final authority and interpretation of the BSA, it is also the leader in pointing out proper protocol when it appears not to have been followed. Steve Hudak, chief of public affairs at FinCEN, stated that in

any case, the network can never confirm or deny any rumors of filings in the media but that it takes a very interested viewpoint whenever such breaches are publicized: "We take any unauthorized SAR disclosure very seriously and we take our responsibility to guard this sensitive data very seriously as well. Let me be clear: There is no acceptable release of SAR data. Law enforcement agencies who have access to this type of data also should be reminded of their responsibility to protect both the banks who report this information and those individuals who are reported from any negative effect of the filing itself. The penalties (for disclosure) are severe and FinCEN will take appropriate action if we become aware that a SAR filing has been leaked."

All law enforcement officials contacted had similar responses. One of the most interesting, considering that the alleged leak has been attributed to the IRS, is from Robert G. Brannum, special agent with the IRS Criminal Investigation Division, who reiterated those comments on behalf of the IRS: "CI (Criminal Investigations) has recently taken several actions pertaining to the issue of nondisclosure of SAR data. First, CI's intranet, CI Connections, ran a headline reminding employees that it is a 'violation of the law' to disclose SAR information. Second, this same message was also included in CI's weekly electronic newsletter to all CI employees. This weekly newsletter is also sent to the Association of Former Special Agents to remind our retired special agents that they must also continue to abide by the disclosure laws. Third, any incident where CI suspects the release of unauthorized disclosure of data is reported to the Treasury Inspector General for Tax Administration (TIGTA) for thorough investigation."

The FBI stated that its compliance posture regarding the SAR disclosure issue is also communicated throughout the agency. An FBI special agent, who requested anonymity and who ironically has banking experience, commented that part of any law enforcement training, especially while new agents are enrolled at the FBI Academy, includes specific formal training on confidentiality protocol. The SAR issue is addressed in great detail there and he also said this issue is reiterated to agents on special assignments.

Every BSA and AML seminar, compliance school, and conference across the country strives to provide top-notch instructors and many include former and current law enforcement officials. These folks always plead with their captive audiences to pass along as much detailed information as possible in the narrative section when filing SARs. Some bankers file as automatically as breathing and others seriously consider and discuss in a committee format before making the decision to file and possibly commit to long-term monitoring and to accept the understood "deal" of repeat filing. Most large regional banks have sophisticated AML software that helps to identify those patterns of activity to take the guesswork out of the analysis, and these days, many mid-size and smaller community banks are also jumping on the bandwagon of purchasing

## Challenges to the SAR Safe Harbor Provisions

Case	Year	Court
<i>Merrill Lynch v. Green</i>	1996	Florida
<i>Lee v. Bankers Trust Co.</i>	1999	2nd Circuit
<i>Weil v. Long Island Savings Bank</i>	2001	New York
<i>Cotton v. PrivateBank and Trust Co.</i>	2002	Illinois
<i>Dupre v. FBI</i>	2002	Louisiana
<i>Gregory v. Bank One, Indiana, N.A.</i>	2002	Indiana
<i>United States v. Holihan</i>	2003	New York
<i>Bank of China v. St. Paul Mercury Insurance Co.</i>	2004	New York
<i>BizCapital Business and Industrial Development Corp. v. OCC</i>	2005	Louisiana
<i>FDIC v. Flagship Auto</i>	2005	Ohio
<i>United States v. Bortnick</i>	2005	Pennsylvania
<i>Whitney National Bank v. Karam</i>	2004	Texas
<i>Wuliger v. OCC</i>	2005	Ohio

such software. For smaller banks that are not in the position to have dedicated BSA officers, the challenge can be even greater in identifying this activity, but the responsibility to provide the same quality and quantity of data remains the same.

We think we know what may be taking place when we identify what appears to be suspicious activity, and frequently we are dead-on correct. We either get those long-awaited grand jury subpoenas or a visit from law enforcement flashing a shiny badge, and we mutter to ourselves, “Yes, we were right, they *are* doing *that!*” Or, as is more often the case, we file, and we file, and we file, and we get no response at all.

Several years ago, law enforcement agencies would send notices letting banks know that they received the filings and there would be “no action taken at this time.” It was comforting to know that the SAR got to its final destination, but it was also sometimes disappointing knowing you slaved over something that received such scrutiny by auditors and examiners but just didn’t amount to much according to law enforcement. And then 9/11 happened and our favorite read, the *FFIEC BSA/AML Examination Manual*, was born.

On the confidentiality issue, bankers are all aware that the very fact that a SAR was filed on an individual or entity can-

not be disclosed to the suspect, but what public knowledge or basis is there for the media to use as a guide on presenting something as juicy as a SAR? This is better information than anything someone got to the courthouse to find first because it is not public knowledge. Although the Spitzer case is the first time in recent memory anyone of such public stature had this type of information released in the media, the issue was already in the works of being addressed by the American Bankers Association (ABA). This recent event has only elevated the priority of the project for obvious reasons. A media toolbox would be a great resource for bankers to be able to have at their disposal to be able to better address those concerns raised by customers and citizens in the community in general, and one may be on the way. The public's concern of the "big brother" concept is already bad enough in an election year, and with the subprime mortgage mess, bankers don't need any more bad press from skeptical customers and the public at large.



**The public's concern of the "big brother" concept is already bad enough in an election year, and with the subprime mortgage mess, bankers don't need any more bad press from skeptical customers and the public at large.**

In short, a response to customers who inquire about what you, as a banker, report to law enforcement should be comforting: if there is nothing to hide, there should be nothing to fear. This is obviously easier said than done because most consumers and even more sophisticated business customers don't always get the correct and most current information from their legal and accounting sources. The professional service providers for our customers mean to do a good job and provide accurate information, but all too often we hear of cases in which an accountant provided faulty or outdated information to a customer or even more often, the customer simply misunderstood. When customers act on misinformation it often leads to unusual activity that may appear suspicious. This issue was communicated in May 2007 by the ABA's Megan Davis Hodge in testimony to Congress.<sup>8</sup> She also reiterated the concern over reported instances of IRS-CID officials directly contacting suspects related to structuring and then the suspects returned to their banks demanding to know who reported them. This is neither effective nor helpful if law enforcement agencies wish to continue the strides on gathering much-needed information from banks.

Good communication before this type of situation occurs is not always practical, especially with multiple branch locations or where a customer does not have a specific account officer relationship.

All in all, law enforcement and bank regulators truly want to do the right thing and the vast majority would never disclose, intentionally or unintentionally, the fact that a SAR was filed or the underlying details. Just like other items of interest found in the media, we need to view these items carefully and not jump to conclusions that any particular media outlet has all of its facts in order. Bankers should continue to comply with their current risk management practices regarding BSA regulations and they should also continue to rely on the safe harbor provided to them.

Not everyone feels that the recent disclosure was completely negative. Tim R. White, national risk specialist with Bankers Toolbox, commented that the recent disclosure was actually indicative that the BSA works: "It will certainly raise the eyebrows of any public official that is currently involved in criminal activity, money laundering, or political corruption," he said. He went on to say that although the system works, it is "unfortunate that the SAR was actually disclosed

because it compromises the secrecy of the system. It could raise doubts in the mind of a potential SAR filer (about his or her) ability to remain anonymous. SARs are to be confidential for the protection of the bank employees or others working on the case."

Another angle to this story is whether the politically exposed person (PEP) issue is one that bankers should be more mindful of. Because Spitzer was technically not a PEP, according to the FFIEC exam manual,<sup>9</sup> this would not have been

as much of a concern, but some in the industry think that it should be, regardless of what the U.S. definition is. Alan Abel, global AML practice leader for Crowe Chizek, feels that banks should ask whether a customer is related to any government, domestic or foreign, to determine whether they should be included in additional monitoring efforts. "The institution has to ask what definitions they are going to abide by and to decide what their risk appetite will be and then to have greater controls in place," Abel said. "Banks should decide if just foreign officials should be covered, as indicated in the U.S. definition, or to take a more conservative approach and follow what other countries have done and that is to include domestic officials as well." Abel also said that even if banks don't want to formally track these customers as true PEPs, they should at least internally designate them as high-risk customers who require additional due diligence and monitoring because this "is simply the right thing to do."

In the U.S. version of the definition,<sup>10</sup> only those who are current or former *foreign* political figures, and their immediate families and close associates, are included, but in Great Britain for example, the definition covers local governmental officials too. For their regulation, a PEP includes "individuals who are or have been entrusted with prominent public functions."<sup>11</sup>

On the issue of the SAR disclosure, Abel commented that “the sheer volume of law enforcement agencies who have access to the SAR data is enormous and the relatively few leaks that have occurred are better to deal with here than a similar situation in another country where there is no expectation of safe harbor or no enforcement of disclosure prohibitions.” Although other countries have a more encompassing definition of PEP, the United States is the leader in affording the protections to those involved in filing the SAR.

One avenue that is being utilized to communicate the need for vigilance for the protection of SAR confidentiality is the Bank Secrecy Act Advisory Group (BSAAG). This group was organized by the Department of Treasury, is headed by FinCEN Director James H. Freis Jr., and includes representatives from federal regulatory and law enforcement agencies, financial institutions, and trade groups. Its primary goal is to offer advice on administering BSA regulations.<sup>12</sup>

Sepidah Behram, general council, Banker’s Association for Finance and Trade (former ABA senior compliance counsel), pointed out that the ABA is actively involved as a participant in this organization and has addressed the SAR confidentiality issue in this and other forums: “Through the subcommittees we have raised concerns over disclosure of SAR information and FinCEN has been working on developing an informative brochure for consumers to inform them of the obligations of BSA reporting. There is no set time frame for the release of the brochure and we have as a committee agreed to a final version.”

The efforts of the ABA were also described by Richard Riese, senior vice president, ABA’s Center for Regulatory Compliance. “ABA has stressed this point (of SAR confidentiality) and IRS’s problematic approach to handling SARs in Congressional testimony, to IRS and Justice Department officials directly and in other government forums,” Riese said. “There is an ongoing interagency project that ABA has urged move more quickly to come to a consensus about what can be said about the process that leads to SARs on structuring generally.”

In June 2006, the ABA filed an amicus brief on behalf of the OCC regarding the BizCapital case. The heart of this SAR disclosure controversy is simple and is described in the BizCapital amicus brief as follows: “Permitting the release of any SAR through civil discovery could harm the law enforcement interests the [Annunzio-Wiley Anti-Money Laundering] Act was intended to promote. Release of a SAR could compromise an ongoing law enforcement investigation, tip off a criminal wishing to evade detection, or reveal the methods by which banks are able to detect suspicious activity. Furthermore, [a] bank may be reluctant to prepare a SAR if it believes that its cooperation may cause its customers to retaliate. Moreover, the disclosure of a SAR may harm the privacy interests of innocent people whose names may be contained therein.”<sup>13</sup>

Aside from the fact that the BSA basically deputizes every bank employee into being an extension of the long arm of the law, generally speaking, the vast majority of bankers

simply want to do the right thing. Doing the right thing is continuing to file the SARs when there is apparent or suspected illicit activity and enhancing AML programs to prevent the abuse of the U.S. banking system. Of course we all want to do the right thing, but if the general media and the occasional purported law enforcement leaks continue, the fears of possible legal action and retaliation from the loss of confidentiality and possible jeopardy to the safe harbor protection will only increase. If we allow this to happen and don’t speak out to legislators and the media, law enforcement and the general public could suffer a great disservice committed in the fight against financial crime. **BC**

#### ABOUT THE AUTHOR

**Maureen E. Carollo, CRCM**, serves as vice president, compliance and BSA officer for NBanC in Oklahoma City, Okla. NBanC is a multibank holding company that owns NBC Bank and operates nine locations in Oklahoma. Carollo has 20 years of experience in the banking industry in the deposit operations, loan administration, compliance, and audit areas and holds the Certified Regulatory Compliance Manager (CRCM) designation through the ABA’s Institute of Certified Bankers. She holds an associate’s degree in finance and is a graduate of the Southwestern Graduate School of Banking at SMU in Dallas, Texas. She serves on the ABA Bank Compliance magazine editorial advisory board and is active in the Oklahoma Bankers Association, where she has served on the Compliance School Board of Regents for several years and is currently serving on the OBA’s Women in Banking Board. Reach her via e-mail at mcarollo@nbcok.com.

#### Endnotes

<sup>14</sup>“How Spitzer Got Stung,” CBS News, March 11, 2008; and “Why Spitzer’s Banking May Have Tripped Him Up,” *U.S. News and World Report*, March 12, 2008.

<sup>24</sup>“The Reports That Drew Federal Eyes to Spitzer,” *The New York Times*, March 12, 2008.

<sup>34</sup>“Banking Activity Drew Attention to Spitzer,” *Dallas Morning News*, March 12, 2008.

<sup>4</sup>Brief of Amicus Curiae filed in U.S. Court of Appeals for the Fifth Circuit, ABA in support of defendant-appellant Office of the Comptroller of the Currency of the United States, June 1, 2006.

<sup>54</sup>“Federal Court Reaffirms Protections for Financial Institutions Filing Suspicious Activity Reports,” Interagency Advisory, May 24, 2004.

<sup>6</sup>FDIC Financial Institution Letter No. 6704, May 24, 2004.

<sup>7</sup>*William T. Wuliger vs. Office of the Comptroller of the Currency and J. Katz*, Case No. 3:05 CV 108, Amended Memorandum Opinion, United States District Court for the Northern District of Ohio, Western Division.

<sup>8</sup>Testimony of Megan Davis Hodge on Behalf of the American Bankers Association before the Subcommittee on Oversight and Investigations, Committee on Financial Services, United States House of Representatives, May 10, 2007.

<sup>94</sup>“Politically Exposes Persons-Overview,” *FFIEC BSA/AML Examination Manual*, August 24, 2007, pg. 264.

<sup>10</sup>FFIEC BSA/AML Infobase, www.ffiec.gov/bsa.

<sup>11</sup>The Money Laundering Regulations 2007 No. 2157, www.english-legislation.hmso.gov.uk/si/si2007/ukSI\_20072157\_en\_8.

<sup>12</sup>“FinCEN Director James H. Freis, Jr. Hosts BSAAG Plenary,” FinCEN Press Release, May 17, 2007.

<sup>13</sup>Brief of Amicus Curiae filed in U.S. Court of Appeals for the Fifth Circuit, ABA in support of defendant-appellant Office of the Comptroller of the Currency of the United States, June 1, 2006.