CORPORATE COUNSEL
An ALM Website
corpcounsel.com | February 13, 2015

# Money-Laundering Risk: It's Not Just for Banks Anymore

## From the Experts

*Douglas Greenburg, Bob Sims and Eric Volkman*

Photo by TaxRebate.org.uk, via Flickr

In recent years, banks and other financial institutions operating in the United States have faced unprecedented scrutiny from prosecutors and regulators for allegedly failing to meet their legal obligations to detect and report criminal activity taking place through their accounts. This scrutiny has direct and potentially far-reaching consequences—not only for financial institutions, but for their customers who are commonly seeing the risks and burdens of anti-money laundering (AML) compliance passed on to them. These customers increasingly should expect the institutions to scrutinize their accounts and report suspicious transactions to law enforcement. And, as financial institutions seek to "de-risk" their customer base, they increasingly will close customer accounts and deny other privileges, such as the ability to make payments to account holders at the bank or execute international wire transfers that use the bank as an intermediary.

This article identifies the potential implications for nonfinancial institutions, and also offers strategies to mitigate the risks.

### Government Efforts to Prevent Money Laundering

The U.S. approach to preventing criminals from taking advantage of the financial system relies on the basic premise that financial institutions themselves are in the best position to detect money laundering and other illicit transactions. Thus, the Bank Secrecy Act (BSA) and its regulations require institutions to implement policies and procedures to detect suspicious activity and to report it to the government. The USA PATRIOT Act, passed in the wake of the 9/11 terrorist attacks, dramatically expanded the scope of entities deemed "financial institutions" subject to suspicious activity reporting. These institutions now include a myriad of entities beyond banks, such as securities broker-dealers, casinos, money-service businesses and insurance companies.

Although the AML requirements in the BSA do not apply to companies other than financial institutions, all companies operating in the U.S. must comply with the principal U.S. AML laws, 18 U.S.C. §§1956 and 1957. These apply broadly and can potentially result in severe penalties against companies and individuals who knowingly, or with "willful blindness," handle "dirty money" generated by a wide variety of illicit activity. U.S. laws can reach companies that engage directly in the criminal activity that generates the illegal funds, companies that use otherwise untainted funds for some illicit purpose, and even companies unconnected to the original crime that knowingly conduct financial transactions involving tainted funds.

### Financial Institutions in the Crosshairs

"The BSA is not a tip; it is not a suggestion," cautioned Preet Bharara, the U.S. attorney for the southern district of New York, in January 2014. "It is a legal require-

ment, enforceable through criminal sanction," he continued." Financial institutions need to take it seriously because we are deadly serious about enforcing it."

As Bharara's warning suggested, prosecutors and regulators have pursued financial institutions for AML and related violations with a vigor never seen before. The result has been a large number of high-profile prosecutions, often ending in nine- or even 10-figure criminal penalties. Since 2012, financial institutions have paid out over $4 billion in penalties and forfeitures to settle cases brought in whole or in part under the BSA.

The costs of these enforcement actions have extended beyond the direct financial penalties the government has assessed. In the last three years alone, BSA actions were responsible for billions more spent in compliance and legal costs, dramatic losses of shareholder value in public banks under investigation, multiyear delays in corporate transactions and, in one case, the revocation of a bank's charter, ultimately leading to that institution's dissolution.

Banks have responded to these developments in a number of ways. First, banks have dedicated a tremendous amount of resources to AML compliance, both in terms of financial resources and manpower. As a result, banks are prioritizing this issue and scrutinizing the sources of their customers' funds to a far greater degree. "Know Your Customer"—the catchphrase that traditionally summarized a financial institution's AML obligations—has in many cases been replaced by "Know Your Customer's Customer." This evolution has resulted in increased demands on nonfinancial institutions to keep informed about their customers' identities and businesses.

Second, the rise in the number and magnitude of BSA enforcement actions has predictably caused a surge in Suspicious Activity Reports (SARs) filed by financial institutions with the Financial Crimes Enforcement Network (FinCEN), the bureau within the U.S. Department of the Treasury primarily responsible for collecting and analyzing SAR data and making it available to law enforcement and for intelligence purposes. Between 2012 and 2014, SARs filed by depository institutions (banks, thrifts, savings and loans, and credit unions) increased by a factor of nearly 25, from 35,736 to 886,927. In that same period, money laundering-related SARs filed by depository institutions rose from 14,396 to 672,136.

Faced with rocketing compliance costs and the specter of billion-dollar penalties, banks have chosen in some circumstances to "de-risk" by cutting ties with certain customers if they believe that the costs and risks exceed the value of those customers' business. Data regarding the prevalence of "de-risking" is anecdotal, but FinCEN viewed it as sufficiently widespread in the case of money-service businesses (MSBs) to issue a formal statement in November 2014 urging financial institutions to "assess the risks of customers on a case-by-case basis" rather than indiscriminately terminate accounts. (MSBs include dealers in foreign exchange, check cashers, issuers and sellers of traveler's checks or money orders, and the like.)

## Implications for Nonfinancial Initiations

The banks' responses to the increase in BSA enforcement activity have significant practical implications for their customers. For example:

### Increased Risk of Investigations

Most obviously, in a climate in which banks are taking a broad view of what constitutes "suspicious activity" and erring on the side of reporting, customers face a greater risk of investigation. Not every SAR leads to an investigation, and FinCEN has been reluctant to quantify the frequency with which this occurs.

However, a review of FinCEN's archive of law enforcement cases involving SARs suggest that the frequency of such investigations has increased as the number of reports have risen. Moreover, such investigations are not limited to potential money-laundering violations. SARs data has been used to investigate a number of different crimes, including corruption, fraud, sanctions violations and tax evasion. Similarly, a wide variety of law enforcement agencies—both federal and state/local—have initiated or supported investigations based on SARs.

### Increased Administrative Burdens in Maintaining Banking Relationships

As wary banks aggressively seek to manage their risks, nonfinancial institutions should be prepared for greater scrutiny regarding their customers and business operations. Interactions with banking partners can be arduous and time-consuming. In the AML context, these dealings may be further complicated by the fact that nonfinancial institutions rarely encounter the BSA and, in many cases, do not have systems in place to supply their banks with the information they may be seeking easily and efficiently. Even a slight delay in payment processing can have damaging consequences for a company's operations—impacting cash flow and their ability to pay vendors and suppliers.

### Risk of Being "De-Risked"

The termination of a banking relationship raises a host of problems for any bank customer. In addition to the disastrous short-term effect such an action has on a company's ability to generate and collect revenue, being "de-risked" also impacts the company's access to capital, including loan facilities, credit cards and letters of credit. Moreover, a risk-averse bank may not only close a company's accounts, but deny that customer the right to transact with the bank at all. The denial of banking privileges could extend even to making payments, and the de-risked party may not be able to pay suppliers or other creditors who hold

accounts at the bank.

So, even if a company has alternative banking partners on which to fall back, the denial of the ability to transact with a significant financial institution presents practical and reputational concerns to the de-risked party.

### Practical Strategies for Nonfinancial Institutions

In this era of enhanced AML scrutiny, bank customers should take three practical steps to protect themselves:

**1.** They should enhance their own AML compliance so that their own financial transactions do not trip banks' AML detectors. Nonfinancial institutions are, of course, not subject to the BSA AML regime, but every company doing business in or through the U.S. is subject to the more broadly applicable prohibition on laundering money or transacting in the criminally derived proceeds. To minimize the risk of such illicit activity, which banks will be looking to detect, companies should adopt appropriate controls over payments and be extremely sensitive to red flags of potential money laundering. Some common examples of these are:

- Inexplicable third-party payments from sources other than the party owing the money.
- Requests from counterparties for unusually complex deal structures or structures with no apparent business purpose.
- Requests by counterparties that funds be delivered to apparently unconnected accounts.
- Payment of one invoice or group of invoices with multiple instruments.
- News reports or rumors indicating that a counterparty is engaged in criminal or regulatory violations or is under government investigation.
- Transactions involving jurisdictions known for smuggling or lawlessness, or jurisdictions cited for substantial money laundering concern by U.S. or international authorities.

These red flags should be investigated and resolved before a particular relationship continues. Fixing issues before they are flagged by a financial institution will go a long way toward mitigating risks.

**2.** Companies should enhance compliance in other areas where violations may trigger bank scrutiny, such as the Foreign Corrupt Practices Act (FCPA) or the economic sanctions enforced by the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC). The monitoring that sophisticated financial institutions commonly undertake can potentially flag indications of FCPA or OFAC violations, such as questionable payments to offshore "agents," or transactions with potential fronts for sanctioned parties. A SAR filing on such issues easily could trigger a government investigation, which can be very expensive and disruptive, regardless of the outcome.

**3.** Companies should be prepared to deal with questions from financial institutions about potential compliance issues by promptly investigating a bank's concerns and responding with timely, accurate information. Companies should designate an appropriate person as a point of contact for dealing with questions from financial institutions that may implicate legal compliance, and develop procedures for quickly elevating the inquiry to the right legal and/or compliance personnel to ensure an appropriate response. At times, a bank's concerns may be addressed easily with readily available information. At other times, companies may need to conduct an investigation and consider sharing the results with their financial institution to address any concerns.

Every such situation is, of course, unique and must be addressed on its own facts and circumstances. The key, however, is to implement appropriate procedures so that responsible persons within the company learn of the financial institution's concerns in time to address them. False or inaccurate information provided to a financial institution in these circumstances can result in severe consequences. Such information can jeopardize the company's relationship with the bank, prompt the filing of a SAR, or lead to a government investigation and criminal prosecution.

### The Bottom Line

Today's heightened AML scrutiny of financial institutions has major potential consequences for their customers as well. Nonfinancial institutions can protect themselves by enhancing their own compliance—particularly in areas like AML, FCPA and OFAC, which might raise red flags with banks—and by appropriately handling inquires and concerns that their financial institutions may raise.

*Douglas Greenburg, Bob Sims and Eric Volkman are partners in the white-collar defense and investigations practice group at Latham & Watkins. They regularly represent clients in U.S. government investigations and counsel clients worldwide on compliance with U.S. laws. Greenburg serves as a vice-chair of the firm's global litigation department and, with Volkman, is based in the firm's Washington, D.C., office. Sims is based in San Francisco.*

Reprinted with permission from the February 13, 2015 edition of CORPORATE COUNSEL © 2015 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-02-15-02