The Truth About Suspicious Activity Reports

September 22, 2020

On Sunday, September 20th the International Consortium of Investigative Journalists and BuzzFeed released a report on thousands of illegally leaked Suspicious Activity Reports (SARs). The report titled "FinCEN Files" is based on limited information and lacks a full understanding of the AML framework, so it provides a skewed and misleading perspective of AML enforcement efforts. In particular, the report disregards the purpose of SARs and demonstrates an uninformed view of how they are generated by banks and used by law enforcement.

This report has led to considerable confusion about the anti-money laundering regime in the United States, and the global system of correspondent banking. Here is a quick Q&A that we hope will provide useful background.

What is a Suspicious Activity Report, or SAR?

As the name suggests, it is a report filed by a bank with a government database operated by the Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department.

What is the standard for filing a SAR?

The activity need only be suspicious, and the SAR does not reflect any finding by the bank that a crime has been committed. It's a lead – akin to seeing someone suspicious in your neighborhood and calling the police to check it out.

Who at the bank files the SARs?

Each bank has an independent unit, generally in the Compliance Department, who file the SARs. The largest banks employ thousands of such people; regional banks hundreds or dozens. Many of the staff are former law enforcement, national security, or military.

How are the SARs generated?

Most SARs come through a two-stage process. The bank runs rules-based algorithms against transaction systems to generate alerts. The algorithms look for anomalous behavior -- e.g. a large volume of cash transactions; large transfers to a country where the customer does not do business.) At this point, a Compliance staffer investigates the alert and decides whether the activity is "suspicious" or not. A computer algorithm monitoring customer behavior triggers an alert if certain parameters are met. Since banks are subject to enforcement action if they fail to file a SAR when they should have, but suffer no sanction if they file a useless SAR, the general presumption is to file the SAR.

How many SARs would a large bank file in a year?

A BPI study found that, in 2017, a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent.

How many of these SARs are really illegal activity versus false positives?

Our data indicate that about 4 percent of SARs result in any follow-up from law enforcement. A tiny subset of these results in an arrest and ultimately a conviction.

Isn't law enforcement overwhelmed by the number of SARs being filed by the banks?

Not exactly. Law enforcement uses computer searches to mine the database, so extra data is not necessarily a problem. Generally, law enforcement already has suspicions about someone and then goes to the SAR database to gather evidence and find other suspects.

What if a bank concludes that a SAR almost certainly reflects actual criminal behavior, as opposed to suspicion?

In those cases, someone at the bank will call law enforcement directly to flag the SAR.

Why would a bank identify a suspicious transaction for law enforcement and continue to bank that client?

There are several reasons:

- In most cases, an institution may see something anomalous for a client and file a SAR, but continue to monitor the customer in case additional transactions prove their suspicions correct rather than immediately exiting the customer when a SAR is filed. Furthermore, in the great majority of cases, the bank hears nothing back from law enforcement. In some cases, a case of suspicious behavior – e.g., cash transactions – turns out to be a one-time thing. Absent any evidence of actual criminality, the bank may elect to keep the account open.
- BPI's research found that a median of 40% of member SAR filings were so-called structuring SARs – basically, cases where there were a lot of cash deposits that might indicate that transactions were being structured to avoid detection. Research showed that roughly 28% of SAR filings resulted in account terminations due to multiple filings; so, when patterns persisted, banks frequently closed accounts.
- Relatedly, there are cases where a bank is subject to contractual relationships with a client, which could be implicated if they abruptly closed the account; therefore additional legal diligence is required by the bank prior to any formal action, and real evidence is necessary to support a closing decision.

- Banks frequently receive "keep open" letters from law enforcement, requesting that they work with investigators to track and report the flow of potentially suspicious funds. These requests are similarly subject to strict confidentiality provisions and time limited. However, once they expire it is at the bank's discretion to continue to bank the customer or close the account, which is a difficult decision to make if law enforcement has not formally brought charges against the individual during the keep open letter's period. In most cases, absent formal charges, institutions are unaware whether the covered individual has been cleared of suspicion or if the investigation is proceeding but in a different vein. There is no legal requirement to close the account once the keep open letter expires.
- Lastly, it is worth noting that in the case of the recent reports, which are based solely on leaked SARs, the bank in many cases may have subsequently closed the account – perhaps after further investigation or monitoring, or after hearing from law enforcement. A partial leak of SAR filings does not reflect the whole history of an account.

Aren't banks simply deciding for monetary reasons to keep banking customers who they have filed SARs?

Recall that SAR investigations and filings are conducted by Compliance teams generally made up of former law enforcement. In all cases, they have no connection to the business unit, and their compensation is unaffected by whether an account is kept open or closed. They are at personal risk of enforcement action if they mistakenly decide to keep open an account, so all their incentives are towards closing accounts. Indeed, diplomatic and development officials have criticized banks for closing too many overseas accounts.

Much of the reporting focuses on U.S. banks acting as "correspondent banks." What does that mean?

Because the dollar is the world's reserve currency, foreign banks frequently transfer dollars between each other. To do so, they need a U.S. bank, transacting in dollars, in the middle.

How does AML monitoring work in such a situation?

Suppose a company in Spain wishes to transfer dollars to a company in Argentina. The Spanish bank is responsible for monitoring its customer's behavior, and the Argentinian bank is responsible for monitoring its customer's behavior. The U.S. bank that stands in the middle of the transaction will monitor it for suspicion, but is limited in its ability to do so because it does not have the same knowledge of the companies' transaction history.

Why not just ban U.S. banks from correspondent banking, as some of the reports imply should be done?

Such action would come at massive costs.

- Correspondent banking is a crucial linchpin in global trade.

- Correspondent banking is necessary to continue the dollar's status as the global reserve currency, which has massive benefits for the U.S. economy and its geopolitical power.
- Correspondent banking is vital to foreign aid. A February 2017 report released by the Charity and Security Network found that two-thirds of U.S. non-profits that work internationally have difficulties obtaining or maintaining banking services, with delays in wire transfers, documentation requests, and increased fees topping the list of discrete concerns as well as account closures and refusals to open accounts by financial institutions.

Well, then, why not just require the U.S. bank to do the same monitoring as the two other banks?

This is practically impossible. It would slow global trade to a halt, as every transfer was re-investigated, and would require U.S. banks to gain access to all the customer data at all global banks, which will never happen for innumerable reasons, including privacy and national security concerns.

Why aren't the banks explaining themselves in this case?

SARs are subject to statutory and regulatory "tipping-off" provisions, which generally stipulate that "[a] SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities." Law enforcement insists on secrecy for three general reasons: (1) to protect the reputations of many innocent people and companies where the suspicious activity turns out not to be criminal; (2) to prevent the banks from failing to file SARs for fear of being criticized or sued by the subject of a SAR; (3) to prevent criminals from learning about the SAR process at the bank.

How would legislative efforts to reform BSA/AML affect the requirements of banks to provide SARs to law enforcement?

Members of both parties in the House and Senate have worked for several years to reform and modernize the BSA/AML framework. Nothing in the bill lowers the expectations for banks or the penalties associated with failure to properly carry out BSA/AML compliance. Law enforcement and national security experts have endorsed the legislation as a meaningful step in improving the prevention of money laundering and illicit activities. Provisions in the bill that encourage law enforcement to set and share priorities and information with banks, and push banks to adopt technology will move our system forward.

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.