The Impact of SARs Disclosures on Financial Institutions

NOVEMBER 2020

Julie Copeland
Partner, StoneTurn
jcopeland@stoneturn.com
+1 212 430 3439

by Julie Copeland

There has been a great deal written over the past several weeks about the surprising—and some might say, shocking—releases of information from Suspicious Activity Reports (SARs) that were filed with the Financial Crimes Enforcement Network, an arm of the U.S. Treasury Department. Under the Bank Secrecy Act (BSA), financial institutions are required to file SARs when activity by customers, counterparties, even employees, meets a set of pre-established criteria, specifically:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through a covered financial institution (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect the transaction.

The stated purpose of these reports is to help law enforcement identify and prosecute criminal activity relating to a variety of crimes, including money laundering, tax fraud and terrorist financing. It is important to note that a SAR often contains unproven statements regarding a transaction that may have an

innocent explanation; it is not necessarily a final assessment regarding a transaction's legality or illegality. Moreover, it may reflect account activity at a point in time, after which additional facts may become known. As such, these reports are intended to be confidential and it is, in fact, a crime for a financial institution to divulge the existence of a SAR or the mere fact that one is being drafted.

It is yet to be determined how BuzzFeed and the International Consortium of Investigative Journalists received access to SARs. Notably, both of these organizations have been careful not to reproduce the entire contents of the SARs, but to describe the content or publish select excerpts. These recent SARs leaks reveal deficiencies within law enforcement, as well as within individual banks.

One example involved a task force recommendation that the Treasury Department designate a Dubai-based gold trading and refining company, as of "primary money laundering concern" under the USA PATRIOT Act. This is a seldom-used measure known as the financial "death penalty" because it can freeze a firm out of the international banking system. According to reports in the press, the Treasury Department did not take action, saying a decision on whether to move ahead was deferred for fear of angering the United Arab Emirates, a key U.S. ally in the Middle East.

The leaked documents also contain examples of failures by major U.S. and international financial institutions to file complete SARs. According to reports, multiple SARs were missing crucial information that would enable law enforcement to follow the trail of potentially illicit funds. Some reports were filed without naming or verifying the source of funds and the beneficiary of those funds. In some examples, financial institutions failed or were unable to obtain the necessary information from the relationship manager in order to file complete information on the customer.

Finally, there have been multiple examples cited of banks failing to take proactive action regarding customers on whom they have filed SARs and/or against whom they have suspicions of illegal activity. Filing a SAR—depending on its nature, the nature of the customer and the transactions being conducted—is only the beginning of a process that should lead to a conclusion to maintain the client and continue to monitor the activity or to exit the relationship. Many financial institutions have policies that if multiple SARs are filed on a customer, the relationship should be exited after a certain threshold has been reached.

The unintended consequences of these leaks are troubling, since they are largely not being addressed. SARs are supposed to be confidential documents, so these leaks may impact when and how financial institutions file SARs and, in the process, further limit law enforcement's ability to uncover terrorist financing and other financial crimes. The disclosure of SARs could also reveal the methods by which banks are able to detect suspicious activity and could harm the legitimate privacy interests of innocent persons whose names may be contained in the report.

If SARs do not remain confidential, banks, broker/dealers and other financial institutions may require double layers of approval before a Suspicious Activity Report can be filed. This could lead to delays in filing, as well as shape the content of the report to protect the institution, should the report become public, which could deprive law enforcement of much-needed facts.

Of course, there is no way financial institutions can stop the publication of SARs by those not required to keep them confidential. So, how should financial institutions adapt their SARs protocols in light of the recent disclosures? Perhaps, it is time to perform a "health check" on your SAR process:

- Educate SAR preparers on the implications of the recent leaks, emphasizing that what they report may become public information, and the need to fully document in a timely manner any suspicious activity.
- If SARs are risk-ranked—and if your organization doesn't follow this practice, you might want to start—in terms of frequency, nature of the underlying suspicion, dollar amount, choose a sample to review to determine that the decision to maintain/ exit the account relationship was properly made or should be changed in light of new information. The SAR process must be an ongoing and dynamic one that considers new information as it becomes available.

Third-party experts can be extremely helpful in performing an objective and holistic review of your institution's SAR processes, from assessing the quality of the reports to training SAR professionals, as well as reviewing and remediating transaction monitoring systems. The key is to be proactive and continually strengthen your SAR protocols, ideally well before any leak occurs.

This article originally appeared as an Op-Ed in **Banking Exchange, November 2020**.

About the Author

Julie Copeland, a Partner with StoneTurn, brings over 20 years of experience advising the world's largest financial institutions on anti-money laundering controls; issues related to economic sanctions, anti-bribery and corruption; as well as multi-jurisdictional business disputes. She provides clients across a range of industries with pragmatic insights into launching and maintaining effective compliance programs worldwide.