ANALYSIS: FinCEN leaks highlight fundamental flaws in AML regime — survey

Published 15-Oct-2020 by
Nathan Lynch, Regulatory Intelligence

Two-thirds of practitioners in the financial crime compliance field believe the leaks from the U.S. financial intelligence unit (FIU), the Financial Crimes Enforcement Network (FinCEN), have exposed fundamental flaws in the international anti-money laundering regime.

A live poll of more than 120 compliance practitioners from around the world found that just 8% believed the regime was functioning effectively in the wake of the FinCEN Files. A total of 68% of respondents said the leaks had highlighted fundamental problems within the anti-money laundering/counter-terrorism financing (AML/CTF) regime, while 24% were still undecided.

The poll took place during a live webinar on the FinCEN Files involving members of the RAW Compliance AML/CTF community. Respondents included bank financial crime compliance staff, regulators, consultants and government officials from around the world.

The webinar explored the costs and benefits of high-profile leaks of suspicious activity reports (SARs) from FinCEN.

Only 6% of participants said the banks had breached their regulatory obligations in the cases exposed by members of the International Consortium of Investigative Journalists (ICIJ). A total of 44% of practitioners said the banks involved had fulfilled their duties by reporting intelligence and waiting for law enforcement agencies to take further action. Half of the respondents said there was not enough information in the reports to make a clear determination either way.

Small slice of the big picture

Oonagh van den Berg, founder of the RAW Compliance community platform, said the 2,100 files released to the ICIJ only showed a small slice of the picture.

"What the SARS don't show is the follow-up action that's been taken by the banks subsequent to the submission of the SARs," she said.

"The SARs are 0.002% of the SARS that were submitted over a 20-year period. Is that a fair representation of what's happening in the background?"

The leaks also highlighted the need for FIUs to provide more detailed information to reporting entities about their expectations with regard to account closures.

"One of the challenges I've had when working in-house is what we call the 'black abyss' of SAR submission. When you submit a SAR you don't ever know what happens with it. For instance, if you submit a SAR and then you say to your regulatory contact, 'what do you want us to do?', the response is, 'just follow your internal controls and we'll be in touch if there's anything further that we expect from you'," van den Berg said.

Risk tolerance

The FinCEN Files highlighted numerous cases where banks had reported suspicions but continued to provide services to those customers. This has prompted mixed reactions from within the AML/CTF community. Linda Lacewell, superintendent at the New York State Department of Financial Services, said in a recent "op ed" that the reporting regime was acting as a cover to allow banks to continue to work with suspicious customers.

"The SAR — originally intended to alert law enforcement to potentially criminal activity — has become a free pass for banks. The report itself is frequently riddled with the names of anonymous shell companies that make it practically impossible to determine the identity of the perpetrators," she wrote.

Every organisation will have a unique risk tolerance, customer base and financial crime compliance framework, van den Berg said. As a result, there is no single policy on account closures.

"As an organisation you have to have your internal risk appetite, so there are clients you're going to offboard if you see any illicit activities. But there are other situations where you submit SARs that are just indicators of things like tax evasion and you may have submitted it because you're just not 100% certain," she said. "So there is this 'black hole' of SAR submission. The question we always ask ourselves as an industry is, 'what is actually being done with these SAR submissions?'"

FinCEN in the crosshairs

Speakers at the event said FinCEN had failed to communicate well with its stakeholders throughout this crisis. The agency issued a brief media statement on September 1 but has not commented publicly since the ICIJ members began publishing their reports.

Julian Dixon, chief executive at Napier in London, said FIUs around the world had a responsibility to "get on the front foot" and respond to the industry's concerns about data security. He said FIUs should seize the opportunity to close down a lot of the speculation on unanswered questions, such as the source of the leaks.

"They should really be wholly prepared for things like this. Leaks like this appear to be becoming more prevalent in society generally. There's a honeypot of information here that is interesting to journalists and criminals," Dixon said. "In terms of cyber protection, I would hope that FinCEN and other agencies who have this data have got the highest levels of protection."

The big questions

Dixon said some of the questions that need to be answered include: Who has access to the data? What levels of authority do they have? When users want to download large volumes of data, can they do it on their own or do they need authorisation?

"With all these things, prevention is better than the cure. So disabling the agency's computer USB ports to prevent the downloading of files is something that I would think most financial organisations have done probably 10 years ago. It's a serious thing that [FinCEN] hasn't done that," Dixon said.

Reluctance to report

Speakers at the webinar also said leaks from FIUs would have a "chilling effect" on the financial crime compliance community. The webinar heard that SARs had information that could even place individuals at risk of harm in some jurisdictions.

One-quarter of poll participants said the FinCEN Files would lead to a reduction in the volume or quality of SARs that banks file. A total of 41% of respondents said reporting rates would continue at the existing levels.

Van den Berg said that FIUs around the world have a responsibility to protect the identity of SAR filers.

"There are people who are exposed as a result of these leaks. People are in danger now because of the exposure of their names in these SARs and also the people whose names are in the submissions," she said. "The fact that these have now been published into the public domain is a big concern because the people who have submitted it have done so with the expectation that it remains anonymous."

Improving technology

The case has shone a light on the importance of investing in better systems and controls — in both the private sector and within the FIUs themselves. Three-quarters of respondents said technology would play a key role, provided the available solutions continued to improve. A total of 17% said good technology existed but organisations were unwilling to make the necessary investments.

"Technology is at the forefront. The banks need better systems, which we're all aware of, but the FIUs, how many of them are working through data manually? How many of them are trying to find the wood for the trees, because of the amount of submissions they're receiving?" van den Berg said.

Dixon said the FinCEN leaks demonstrated that the AML/CTF regime needed to be built on a foundation of mutual responsibility between regulators, FIUs and reporting entities.

"The banks and other institutions are held to such high standards, and I think in most instances adhere to those standards, but the gamekeepers here don't actually seem to have the same standards employed," he said.

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 16-Oct-2020