REGTECH

Banks feel more pressure to upgrade AML tech after 'Fincen Files'

By Penny Crosman September 23, 2020, 3:24 p.m. EDT 7 Min Read

Banks have long needed to strengthen their efforts to catch money launderers, which they mostly attempt to do with anti-money-laundering software. New revelations of financial crime taking place under bankers' noses only add to the pressure to do so — quickly.

This week, journalists from BuzzFeed and the International Consortium of Investigative Journalists began publishing their analyses of a trove of 2,100 suspicious activity reports leaked from the Financial Crimes Enforcement Network, a unit of the Treasury Department.

The journalists say five large banks — JPMorgan Chase, HSBC, Standard Chartered Bank, Deutsche Bank and Bank of New York Mellon — allowed $2 trillion of laundering to take place through their institutions after they had been fined by regulators for AML compliance violations.

"This leak will be a wake-up call for financial services firms and their regulators," said Guy Harrison, general manager at Dow Jones Risk and Compliance, who pointed out that the $2 trillion in suspicious transactions were flagged in 2,000 SARs from 2011 to 2017, which were only 0.02% of the total SARs filed in that period. So the scope of the problem could be much larger.

Inadequate technology

Most SARs are generated by AML software.

"The situation further brightens the spotlight on technology in the AML world," said Jo Ann Barefoot, CEO and co-founder of the Alliance for Innovative Regulation. "I have been one of the many people saying for a long time that we need to upgrade it. Most banks have been working with antiquated technology and struggling with the difficulty of sharing information."

Banks are required to file SARs whenever they suspect some kind of financial crime, and they do file them by the thousands. But about 90% of the time, the suspicious activities don't prove to be criminal, according to Barefoot.

"We also must have a high false-negative rate where we're not finding money laundering," she said.

One challenge is that banks often don't know exactly who is behind the transactions they process. Though each new customer is put through know-your-customer vetting, money launderers use shell companies and other forms of obfuscation.

Vishal Gossain, vice president of Scotiabank in Canada, said his $1 trillion-asset company has been working on this in three ways. First, it's bringing in data from third parties to supplement its customer data, to get a more complete picture of customers. Second, it's using more advanced machine learning models to detect criminal behavior.

“Only a few cases actually get prosecuted,” Gossain said. “So to know the bad actors becomes a challenge because of limited data size. Advanced machine learning really helps.”

This is an industry trend, according to Harrison.

"Banks and regulators will embrace new [artificial-intelligence] powered technologies to be able to analyze vast amounts of data and be able to identify and manage the associated risks,” he said. “We may see regulators put more pressure on banks to identify trends or patterns within their SARs to help them deal with the volumes of SARs filed."

Third, Scotiabank has been improving network analytics and entity resolution to detect shell companies and individuals who may be transferring funds to third parties.

“Once you plot a network on a graph and connect all the companies or individuals in it with account numbers, telephone numbers and transactions, it becomes very clear how this entire network is operating,” Gossain said. “We have uncovered illicit cannabis and human trafficking networks worth millions in transactions, through a combination of these three techniques.”

Barefoot says identity verification and know-your-customer technology is on the verge of getting better. There's work being done in Washington to help determine the true ownership of the entities that are transacting. Real-time money laundering detection would be a big step forward.

“That is coming at the large banks, but we're still in early days,” Barefoot said. “That's exactly where we need to go.”

Need for banks to share data

Many in the industry believe money laundering could be caught more effectively if banks could share data about suspicious activity.

“The fundamental problem that we are facing is that each bank is only able to look at data for their customer base,” said Gossain, who leads the AML analytics practice for Scotiabank. An analyst at Scotiabank, for instance, has no visibility into a Canadian customer’s transactions at Royal Bank of Canada or TD Bank.

“That creates a blind spot,” Gossain said. “I cannot understand the customer and his transactions overall.”

Banks use rules to monitor every transaction. For example, a bank might set a rule that any transaction over $10,000 triggers the filing of a SAR report. But a customer might withdraw $5,000 from Scotiabank, $5,000 from TD and $5,000 from RBC.

“In Canada, human trafficking and sex trafficking is a significantly increasing problem,” Gossain said. “The same is true in the U.S. and in the world.”

Criminals use a lot of email money transfers for this purpose.

“If a pimp has 10 customers who email money to him, we could potentially link all the email money transfers and realize this is a hub and report that to" the Financial Transactions and Reports Analysis Centre of Canada.

But because those customers have accounts at different banks, Scotiabank can only see a small part of the spoke, not the entire hub and spoke.

The problem with data sharing among banks is privacy: Transaction data is sensitive customer data that banks have to protect.

Homomorphic encryption is one technology that could facilitate data sharing without violating privacy rules. It lets users apply analytics to data without seeing all the underlying data itself.

“You can imagine it as locking data in a box,” said Alon Kaufman, CEO of Duality Technologies, a provider or homomorphic encryption for data sharing for money laundering investigations and other purposes. “The data stays intact, totally accurate, and you don't delete any fields, but everything's locked in a box. You can apply accurate analytics to the data in the box without ever opening it.”

A bank might identify a suspicious customer and that person’s pattern of cash transactions. Then the bank could ask its peers if they have seen the same kind of pattern from that customer. The name, address, date of birth and cash transaction data would all be encrypted in the query.

Other banks would apply the query to their databases and send back encrypted data about the customer’s cash transactions.

“The other banks do not get tipped on which customer I’m inquiring about, and everything remains encrypted, so nobody could see each other's data,” Gossain said.

Homomorphic encryption technology is standardized and open source, so banks could be using different software but still be able to make such handoffs. Law enforcement agencies and regulators could also use it in their work.

Need for feedback from regulators

Barefoot pointed out that filing SARs is a blind process.

“When a bank files a SAR, it doesn’t get feedback about it unless there is a further inquiry from Fincen or law enforcement,” she said. “They don't know if the SAR was useful. They know that they had a suspicion and had reason to file a suspicious activity report. They don't know how the users of the report have valued it and what they have done with it.”

Barefoot and others have been advocating for a better feedback loop.

“Fincen has some very sophisticated technology, but it's a small agency, and it’s overwhelmed with reports, including false-positive reports,” she said.

Whether or not to file a SAR is a judgment call, Barefoot said.

“Suspicion is a subjective matter,” she said. “But if they suspect money laundering, they have to file a SAR. I've seen some commentary suggesting that banks consider the high penalties that occur in the AML space are a cost of doing business and they don't care. I don't agree with that. These are very high penalties and reputation damage.”

Need to do the right thing

Obviously, sometimes banks don’t catch money laundering because they don’t want to. The customers doing it are highly profitable and well connected, so it makes business sense to turn a blind eye.

“There are some situations where someone in the bank is actively colluding and being rewarded for it,” Barefoot said. “My view is that that is rare, but it undoubtedly happens. And there are some situations that the bank is just not able to catch; they don't have the tools. And then in the middle, you've got gradations of people who maybe are not being aggressive enough in checking it out and getting to the bottom of what is happening.”

On the other hand, banks do spend tens of billions of dollars a year on AML compliance.

“It's the most expensive and most risky compliance area of all,” Barefoot said. “The penalties and the costs of compliance are the highest. So it's definitely not the case that the industry is shrugging off. But if we really want to shut down the terrible kinds of crimes that happen, the whole industry needs to go on to modern, digitized technology that can gather information in a digitized form so it can be analyzed with AI and you can find these suspicious patterns.”

Penny Crosman Executive Editor, Technology at American Banker and Arizent, American Banker

Regtech AML Money laundering Scotiabank FinCEN

By Brendan Pedersen September 23

AML

Will 'Fincen Files' give banks opening to push for AML reform?

The news media investigation of transactions by nefarious actors puts certain large banks in a negative light, but it also points to inefficient use of suspicious activity reports and other anti-money-laundering issues that the industry has decried for years.

By Neil Haggerty September 23

COMMERCIAL REAL ESTATE LENDING

CRE concerns intensify as stimulus programs expire

Commercial real estate loans are vulnerable as financial assistance for tenants winds down and might not be fully renewed. Late rent payments could rise, leading lenders to press landlords to pay up.

By Jim Dobbs September 23

M&A

Sandia Laboratory FCU to expand footprint with merger

A pending combination with Animas Credit Union will broaden the Albuquerque-based institution's reach in northern New Mexico.

By Aaron Passman September 23

DIVERSITY AND EQUALITY

Truist commits $40M to loan fund aimed at closing racial wealth gap

The fund will support Community Development Financial Institutions that lend to minority- and women-owned businesses. The Charlotte, N.C., company is the latest big bank to make a large dollar commitment focused on alleviating racial and economic inequality.

By Laura Alix September 23

DIVERSITY AND EQUALITY

acknowledging that his words reflected his own "unconscious bias" and vowing to improve diversity in the bank's leadership.

By Kevin Wack September 23

Reputation Rebound

Never let a good crisis go to waste — the pandemic is giving banks the opportunity to create goodwill with consumers and our annual survey of bank reputations offers some insight on how to keep the positive momentum going