Ubiquitous BSA/AML

regulatory risk management BSA-AML

Summary: Anti Money Laundering Suspicious Activity Alerts at banks are soaring, almost doubling since 2013. We bring you the latest updates on this hot topic.

Sadly, Pew Research finds a whopping 59% of teens in this country say they have been bullied or harassed online and have experienced abusive online behaviors. The top three forms of cyber bullying include offensive name calling (42%), spreading false rumors (32%) and receiving explicit messages they did not ask for (25%). Be alert parents!

Social media has become ubiquitous in everyone's lives and BSA/AML has done the same in the lives of bankers. We have mentioned this before, but it is worth repeating - thanks to advanced technology and rising government mandates for fighting money laundering, Anti Money Laundering (AML) Suspicious Activity Reports (SAR) at banks are soaring. They have almost doubled in the past 5Ys to more than 2mm annually.

Unfortunately, most of those alerts associated with monitoring for suspicious activity are just flagging business as usual at banks, as research finds more than 90% are false positives. While there may be ways to tweak the technology that generates SARs to reduce the number of false positives, the issue remains a big one for community banks.

After hefty spending on AML technology, it is no doubt disheartening to learn that such technology generates so many false-positives. But, here's some more bad news: research also shows conventional AML solutions may not be doing a very good job of weeding out more sophisticated international crooks like terrorist groups and drug cartels either. Failing to detect one of these money laundering schemes can pose significant problems for community banks.

The issue at hand is that community banks, like much of the financial world, have focused on transactional data in their AML defenses. These systems use rules-based approaches to search for suspicious activities, like a series of deposits or transfers between bank accounts. As reports of money laundering schemes rise, the tendency is to work with technology vendors to update and improve those transactional-based AML systems.

However, money-laundering operations are much more sophisticated these days and often employ technology experts with deep knowledge of AML systems. As such, it should be no surprise that they have developed ways to work around rules-based AML solutions.

Further compounding the issue is that since transactional AML technology doesn't know a good guy from a bad guy, a bad guy who understands the rules and sneaks around them has a chance of avoiding detection. In some cases, the crooks will even hijack an account of a bank's legitimate customer and then use it to launder money. It's a global cat-and-mouse game, and the bad guys still win too often.

So, what can community banks do? One new strategy is to adopt an "actor-centric" approach to AML detection that looks not just for suspicious transactions, but also for suspicious actors. One way to do this is to use big data solutions that vacuum up massive amounts of data from sources like news feeds, and name and address files, and then try to find matches in bank transactions. No matter what, the AML threat facing community

banks remains a significant and evolving risk, so defending against this risk may require new and creative solutions.

WEBINAR: LEVERAGED LENDING

GETTING COMFORTABLE WITH A LOAN

OCT 10 | 10:00AM PT | Registration

Join us for a 30-minute webinar where we introduce you to one of the loans on our Shared National Credit Pipeline. Could this loan be the answer to your loan growth needs?