ARTICLE

Financial Crime and Compliance: Responsibility Is Not Just on Banks

April 21, 2023 | 2 minutes reading time | By Samar Pratt

Lawyers, accountants and other “gatekeepers” must also be accountable

Global fines for banks that are failing to prevent financial crimes **rose 50%** in 2022, due to the tsunami of Russian and Belorusian sanctions, the Ukraine war, the economic downturn and the rise in cybercrime in general. This likely won’t be the peak; the contributing factors are likely to increase

criminal activity that banks are unlikely to detect, and we can expect further regulatory investigations and fines to come, even if those fines take several years to take hold.

Banks often face the brunt of the blame for not preventing these types of breaches – but this is an overly simplistic characterization. The global framework for combating financial crime and money laundering is fundamentally flawed, and this is the issue that must be addressed.

Why Crime Is Thriving

Financial crime thrives for many reasons, but a key cause is the ability of criminals to hide behind complex corporate ownership structures that banks can find difficult to penetrate.

Banks often use public corporate registries, such as **Companies House**, to identify the beneficial ownership of their business banking and corporate clients and help them spot criminals.

Work with trusted technology partners, Exiger's Samar Pratt advises.

However, some countries don't have publicly available corporate registries – and those that do may not verify the ultimate beneficial owners (UBOs) – so they often turn to shoddily-run registries. UBO data is not validated, so criminals can register fraudulent companies and use them to open bank accounts and use them for nefarious purposes.

Streamlining Regulations

The divergence of anti-money laundering (AML) and sanctions regulatory requirements globally can add to the confusion. With the United Kingdom, United States and European Union often requiring different compliance standards, a bank headquartered in, for example, Germany, with booking centers in London, New York, Milan and Frankfurt, needs to create a complex set of procedures to ensure compliance to all regulatory requirements. Navigating this type of complexity – and the time involved – often encourages a "tick the box" mentality for banks, which is when compliance checks can slip.

Suspicious activity reporting (SAR) must also be improved to enable more of an "intelligence-led" approach to financial crime detection and prevention. The lack of near-real-time information sharing, both domestically and internationally, is possibly the single biggest barrier to effective detection and disruption of financial crime.

Banks fail at preventing financial crime when there are issues impacting the quality and timeliness of information flow between the public and banks or private entities; between banks and the private sector, such as limited bank-to-bank information exchange; and within the same regulated entity that operates in silos.

All Hands on Deck

The fight against financial crime can't only sit on the shoulders of banks. All gatekeepers, such as lawyers, accountants and corporate service providers, need to be involved. The boards of banks are genuinely taking AML and sanctions seriously – and of course, they need to be held accountable.

However, until the other gatekeepers are held to similarly high AML standards as banks, financial crime will persist, and "dirty money" will continue to flow through the financial system.

Ultimately, like so many entities today, banks are under tremendous pressure to implement more preventative measures with fewer Know Your Customer (KYC) resources. They are struggling with backlogs of information they cannot process let alone keep pace with, putting them in a precarious position to comply with increasing regulations.

The simplest and most effective step is to leverage trusted partners that create and operate technology solutions to do just that. Working with innovative partners can help banks not only to bolster internal risk postures and stay ahead of shifting regulatory requirements, but also to help them efficiently prioritize operational resilience, report thoroughly and accurately on third-party relationships, and use innovative, AI-powered solutions to stay compliant.

***Samar Pratt** is global head of Advisory Solutions & International at **Exiger**.*

Topics: **Regulation & Compliance**

SHARE

Related Insights

ARTICLE Members Only

Penalties for Noncompliance: Don't Misread the Dip

MAY 8

The billions that the financial industry pays for anti-money launderin...

ARTICLE Members Only

Anthropic's Mythos: Frontier AI Shakes Up Cybersecurity and Regulation

JULY 2

A select group of corporations gets early access to powerful agentic s...