AML & ABC Forum
Speaker Interview

Infoline

Brandon Daniels

President, Global Markets

Exiger

Q. What key opportunities do you think technology is bringing to the financial crime compliance space?

A: Technology has inherently been both a challenge and an enabler for the identification and mitigation of financial crime compliance in financial institutions and corporations.

Now, with the advent of both data management systems and artificial intelligence (AI) that can replicate analysts' decision-making processes, technology is affording financial institutions and corporations three key opportunities.

The first opportunity is increased efficiency by reducing false positives. Whereas in the past you had to do a blanket level of due diligence against all customers and against all transactions, AI allows for a more granular level of risk indicators. This replicates in a more nuanced way the decision-making process of a financial crime compliance expert. It relieves analysts of false positives and junk alerts, allowing them to do more complex and judgement-based analysis – the kind of work they were originally hired to do.

The second opportunity is to achieve a higher level of holistic analysis that cannot be accomplished through simple large-scale human-driven processes. Having one analyst who is only seeing their own customers or transactions and risk-ranking them gives them a skewed perspective. It doesn't allow them to see how that customer might be connected to several other high-risk customers or transactions or understand risks that have trended with that customer over time. There is no way to do a much broader analysis in which you would have to review hundreds of thousands of entities in order to appropriately calculate risk that exists in the environment. The technology, thus, serves to augment the analyst.

Finally, technology allows us to be more comprehensive in our investigations. There are limitations to what any human can do and technology allows you to go further in some of those more banal, routinized tasks. The idea is that you can go deeper and be more comprehensive if you have the system picking up the "grunt work."

In sum, the three things technology brings to the table are efficiency, holistic analysis of risk and the ability to do more comprehensive analysis which is not limited by what humans can do in a given time frame.

Q. How do you see increased digitisation changing the role of compliance practitioners?

A: The biggest change is that compliance practitioners need to be data and technology literate. There is a shift in what one is required to know and understand in terms of data literacy that will fundamentally change the compliance officer's skillset and role.

A similar change happened 20 years ago in eDiscovery when lawyers became responsible for understanding what metadata was and how databases and communications systems work. They had to come up to speed on how electronically stored information was going to change their practice.

Second, because they are going to be relying on systems more often, practitioners must become more well-versed in what those systems are doing. When that technology is replicating work that compliance officers previously did with hundreds of people, they had better know how it works.

Finally, they must also become a driver of innovation and economic resilience of the firm. The more we incorporate systems in managing financial crime compliance, the more viable each business relationship becomes. The banks have to do some degree of calculus to determine how much it costs to onboard a customer and at what financial level a customer has to generate revenue in order to offset the onboarding cost. Practitioners can help the bottom line of the company while at the same time serving the needs of regulators who hold them responsible.

Q. What do you think are the current and future challenges for the financial services sector of combating financial crime?

A: The challenge is the same as the opportunity.

There is so much information available in today's financial services market and so many systems in marketing, relationship management and trade, it is hard to prioritize. The volume of data is a major challenge to tackle.

In addition, institutions like large Wall Street or High Street banks are dealing with legacy infrastructure, technology and practices that don't fit today's digital and commercial market. Comparably, these legacy-dependent firms have to execute a much larger transition than alternative and challenger banks that can use new systems to do KYC, manage third party risk, and conduct transaction monitoring because they are not working from outdated technology which is ill-fitting with new systems.

It is becoming a competitive disadvantage in retail markets and SME markets to be an older and larger institution whereas that used to be a pillar of trust. Will those challenger banks and digital payment providers build up the compliance and regulatory infrastructure and create enough trust with the consumer to be real and formidable challengers? Or, will the established banks change their culture and infrastructure fast enough and move to a new model quickly enough to be competitive?

I don't think either party will lose, as big banks are monetary engines that will drive the smaller retail digital marketplace banks in the future. The challenge is who is going to change culture, infrastructure and perceptions faster in order to be more competitive.

Q. Do you predict further convergence of different subsets of financial crime over the next few years? If yes, what do you think is driving this trend?

A: There is convergence happening today; we just don't realize the degree to which this has occurred because of silos in banking and compliance. Trade finance is separate from markets which is separate from retail which is separate from private wealth. We don't have commonality of systems or analysis to find systemic risk. The same people who are abusing the lack of insight into trade finance transactions are the same people who are abusing a lack of insight into shell companies.

These are systemic issues where malicious actors are taking known gaps in the financial system and exploiting them across these subsets. The question is whether there will be convergence of analysis across these silos to make for better financial crime compliance policies.