The Tide is Turning: Using Technology Against Criminals

JUNE 19, 2018

On 22 May 2018, Megan Butler, Executive Director of Supervision – Investment, Wholesale and Specialists at the Financial Conduct Authority ("**FCA**"), delivered a speech on the use of technology to detect and counteract criminal activity in the financial services industry. Throughout the speech, she encouraged the adoption of such technologies, emphasising that the FCA will, above all, consider the efficacy and outcomes of new systems. While it is clear that new technologies could bring substantial benefits, there will likely be significant hurdles to overcome in their implementation.

There are two major reasons why using technology and improving automation in compliance and detection of crime would be beneficial, particularly to the financial services industry: to cut costs and to create more efficient and effective systems.

Taking the issue of cost first, it is clear that compliance costs, particularly in the financial services industry, have sky-rocketed in recent years. As banks and other financial institutions scramble to increase their compliance headcount, employing more experienced professionals and launching specialised regulatory projects, costs have soared into the billions. While such a commitment to compliance is, of course, laudable, this rate of increase will ultimately prove untenable. Businesses are, after all, designed to make a profit – sooner or later, spiralling compliance costs will come under heavy scrutiny. Compliance is often process-driven and could benefit greatly from cost savings associated with automation.

Efficacy and efficiency are the other main driver of change in compliance and detection of criminal activity. As Butler points out, almost 50% of reported crime in the UK is cybercrime, and major threats such as phishing scams are deeply rooted in automation. Human checks and investigation simply cannot keep up with the volume of material to be reviewed, while human error and limitations must always be accounted for. Fire needs to be fought with fire: to turn technology against criminals could not only dramatically improve the speed with which data is reviewed but would likely also bring to the table skills which no person would be capable of possessing (for example, identifying patterns across swathes of data too massive for a human mind to comprehend).

Of course, as with any advancement in technology, the pitfalls in its application to compliance are numerous and could be potentially be very deep. Three key issues which institutions are likely to

face are costs, an enduring need for human judgement, and inconsistency across jurisdictions.

The first issue will be to convince businesses and their shareholders that, despite the necessary initial capital outlay, cost savings, along with the other benefits associated with new technology, will be realised within a short period of time. New and effective systems, especially for complex institutions such as banks, are expensive to create. Institutions are largely operating in the unknown and may be blindly throwing money at new systems which could ultimately prove useless. Butler encourages banks to “move first”, and to tell regulators about new innovations they have devised – but which institutions will be willing to go out on a limb, pouring money into new systems and risking having to absorb the costs of failure if the FCA, or another regulator, deems them to be unfit for purpose? The risks of investment in new compliance technologies could prove off-putting.

A second problem to grapple with is that, although compliance is often process-driven, there can be great benefit in having human judgement involved in the process. While technology is a hugely useful tool in sifting through vast quantities of data to help in identifying red flags, manual review, with the experience and insight it brings, would ultimately still be a necessary component of the compliance process. Butler suggests that the next step would be for artificial intelligence (“**AI**”) to provide such judgement. This, however, creates its own problems: technology cannot be reasoned with, and does not provide explanations or justifications for decisions made. Indeed, many proprietary learning algorithms, which learn from their past experience, develop in such a way that even the people who created them cannot understand why they begin to behave in a certain way. In such cases, where would liability lie for mistakes or poor decision making by AI?

The final problem is one which dogs all aspects of compliance for global institutions: differing regulations around the world and the often-divergent attitudes of regulators. From a business perspective, a streamlined and consistent compliance approach in all jurisdictions is the most effective and efficient approach. Unfortunately, it is almost always a pipe dream. What is deemed acceptable by the FCA may not pass muster with the US Securities and Exchange Commission, and vice versa. The incentive to invest heavily in new technologies is greatly diminished if it can only be used selectively across the world. A consistent approach from major regulators will be key to developing long-term technology driven compliance solutions.

It is clear that implementing technology in the compliance field has the potential to shake up the industry, providing long-term cost efficiencies and enabling the swift detection of criminal activity. However, such benefits need to be carefully weighed up with the potential issues that new technologies would face and, ultimately, with how realistic their implementation will be.