Financial IT
Innovations in FinTech

Financial IT Digital Reprint

Richard Price,
Head of Financial Services Practice – UK&I, TIBCO

FCA SHIFTS STANCE ON ML AND AI

The Financial Conduct Authority (FCA), the UK's banking watchdog, has signalled a new and much more positive attitude to the use of artificial intelligence (AI) and machine learning (ML) in the fight against crime.

It has long been the policy of the FCA to demand maximum transparency from banks in their use of AI and machine learning algorithms. Its position has been to demand that banks justify the use of all kinds of automated decision making, clearly fearing that the interests of customers are at risk from poorly deployed automated solutions.

While not softening its demands that technology be applied intelligently, the FCA has clearly moved forward in its approach to AI and ML, recognising them as crucial weapons against criminals whose own use of automation techniques has become vastly more sophisticated. The FCA accepts what we in the AI and ML development community have long been saying – that purely manual approaches to crime busting are as ineffectual as they are wasteful. It is time, says the FCA, for software to augment human efforts.

The FCA's head of regtech and advanced analytics Nick Cook says the regulator is now proactively running sandboxes and hackathons to encourage the development and refinement of AI and ML solutions. In this respect the FCA is following the lead of other progressive regulators, such as Singapore's MAS which has been investing to encourage local AI solution providers.

This change of heart can only be a good thing. The advantages of automation, not just as a tool to satisfy regulators and beat crime but as a positive and transformative benefit for a range of banking processes, are too clear to be ignored.

The way that many banks monitor transactions in the search for instances of fraud or money laundering involves human investigators manually sifting through suspicious transactions. Intelligent technology could be used to augment this activity, improving and speeding up the process of identifying suspicious transactions.

Machine learning and streaming analytics tools, such as TIBCO's, can instantly monitor transactions across vast amounts of data. They can identify subtle patterns and filter transactions more accurately. At the same time, they will be learning in real-time to identify new patterns of fraud as they occur. All of this helps them to intercept new attacks before they impact the customer or the bank.

Crime fighting needs forensic levels of detail too. So these systems will have ingrained model management capacity which exposes and traces all data sources and versions. This is not easy to achieve on the grand scale of a banking enterprise, so the administration and ease of deployment of these systems are as important as raw power needed to process all the instant 'real time' queries.

In this context, the ability of the cloud to create a perfect elasticity of supply for computing power is crucial. This is why the 'big compute' execution capability, associated with Cloud infrastructure, is becoming an industry standard.

Modern analytics techniques can work on multiple data sources concurrently to support automated fraud identification, accelerating the investigation process and automating regulatory reporting. These methods apply equally to payments, insurance claims, new customer applications, money laundering, cyber security and many other financial services activities.

As for transaction monitoring, so too for risk assessment. The way many banks currently model risk involves analysing changes to perhaps thousands of economic variables and their impact upon the bank. These results are then integrated into larger models reflecting performance under a variety of scenarios. Machine learning simplifies this by highlighting key variables while removing redundant data.

The right AI and ML-driven modelling tools are designed with real business decision makers in mind, building on what data scientists are able to deliver by themselves and driving their value further into the business. Such tools ensure the full transparency that both you and the regulator demand and they deliver the results right where they are needed – in the frontline in the battle against crime and fraud as well as the quest to control and manage terabytes of sensitive customer data.

Don't throw good money after bad with any more investment in old school reporting and surveillance solutions. Instead choose something that gives you better augmented intelligence and helps you make better and faster decisions.