REPRINT

R&C risk & compliance

THE EMERGENCE OF AI REGTECH SOLUTIONS FOR AML AND SANCTIONS COMPLIANCE

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2017 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

WHITE & CASE

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

PERSPECTIVES

THE EMERGENCE OF AI REGTECH SOLUTIONS FOR AML AND SANCTIONS COMPLIANCE

BY **KEVIN PETRASIC, BENJAMIN SAUL AND MATTHEW BORNFREUND**
> WHITE & CASE LLP

Innovations in financial technology (FinTech) are rapidly changing the global banking system, not only from the consumer perspective but also in ways that are hidden from view. While FinTech startups and existing technology firms work to improve how consumers interact with the financial system, banks themselves are pouring billions of dollars into developing faster and more efficient methods for meeting their regulatory compliance obligations. In a post-crisis environment which has seen significant new regulations and restrictions placed on activities and operations, as well as record-breaking enforcement penalty amounts, reducing the cost of regulatory compliance is an attractive means of increasing margins.

Regulation technology (RegTech) is the branch of FinTech that focuses on improving financial services providers' compliance and internal control systems. Among other things, RegTech applications automate risk management processes, facilitate regulatory reporting, prevent fraud, enable companies to stay abreast of regulatory changes around the world and support strategic planning.

RegTech, as a field, is not new. Banks and other financial service companies were early adopters of computers and business process automation. But the RegTech applications being developed in connection with the recent wave of FinTech are utilising the latest computer science breakthroughs, such as Big Data analytics, cloud computing and

machine learning. Since 2010, the pace of innovation has accelerated rapidly, paving the way for RegTech systems to incorporate artificial intelligence (AI).

AI basics

Underneath all computer programmes are algorithms, which are the instructions that control their operation. Designed to follow a set of discrete steps from beginning to end, early algorithms were able to act based only on clearly defined data and variables. These algorithms were inherently limited by the availability of digitised data and the computing power of the systems running them. The breathtaking expansion of digital data – from email and the early web, to social media and streaming entertainment – required data scientists to develop new techniques to store, categorise and analyse the information.

The development of Big Data, machine learning and AI, combined with hardware advances and

distributed processing, have enabled engineers to design algorithms that are no longer strictly bound by the parameters in their code. Although current systems are still far short of general AI – the kind that appears to be sentient and displays human characteristics such as improvisation – specialised AI systems using narrow AI have become remarkably adept at independent decision-making. The key to developing narrow AI is using systems that are trained by recursively evaluating the output of each algorithm against a desired result, allowing the machine to 'learn' by making its own connections within the available data.

This process of building up AI, called supervised learning, requires systems to be fed labelled data followed by training cycles where results of the analysis are repeatedly judged by the programmers. For example, to train AI to be able to identify pictures of cats, researchers provide the AI access to a database with thousands of pictures of cats. After the AI builds a baseline model, it is tested against a new database of pictures – some of cats but many of other animals or objects – and the AI is asked to identify whether each is or is not a cat. Both right and wrong answers allow the AI to learn the characteristics of a cat without ever being programmed with specific rules, for example, 'cats have whiskers' or 'cats have sharp claws'.

AI in RegTech for AML and sanctions compliance

Supervised learning has successfully created AI for many specific tasks, including playing chess (trained not by programming in the rules of chess but by allowing it to study millions of actual past games) and translating languages (trained not by programming grammar rules but by allowing the machine to learn from billions of conversations). Similarly, systems are being developed to train AI to work within a bank's computer systems to identify everything from fraud and inadequate internal controls to money laundering and terrorist financing.

> "By automating many compliance tasks, RegTech has already helped reduce costs for banks."

By automating many compliance tasks, RegTech has already helped reduce costs for banks. However, when it comes to anti-money laundering (AML) requirements (including anti-terrorist-financing) and

obligations to comply with sanctions implemented by the Office of Foreign Assets Control (OFAC), the issue for banks is not only cost, but also significant legal and reputational risk. The challenge is magnified because AML and OFAC compliance is difficult to achieve through existing instructional algorithms and rules-based systems.

A rules-based approach to AML would, for example, flag cash transactions over a certain currency amount, block transactions to certain countries, use customer data to select accounts for additional monitoring, and categorise merchant accounts based on prior transactions. These types of systems are already widely used, but they require a significant amount of bank resources to review the transactions that are flagged or blocked to weed out false positives. In addition, a rules-based approach to AML will be unable to adapt to changes in criminal behaviour designed to evade detection.

An AI approach to AML, by contrast, does not require developers to establish rules that identify potentially criminal transactions. Instead, the system would be trained to identify such transactions over time by analysing a staggering array of factors. These could eventually come to include where a customer opens an account relative to their home address, what time of day an account was opened, duration between transactions, patterns among the merchants where a customer makes transactions, relationships between other customers of those same merchants, whether a customer uses a mobile telephone, what communication channel a customer uses to contact the bank and even changes in a customer's social media presence. The factors that AI can evaluate are limited only by the available data.

AI can identify patterns and connections among the data that humans cannot hope to recognise. Using this information, the AI would then monitor every transaction processed by a bank and predict whether each one is or is not criminal. The accuracy of such a system would be significantly higher, and the resources needed to monitor the output significantly lower, than with a rules-based system. Importantly, an AI system would continually improve its accuracy automatically.

For OFAC compliance, as with AML systems, AI would drastically improve detection. This is particularly important because banks are strictly liable for any transaction involving an entity on the OFAC sanctions lists. It has long been routine for bank systems to block attempts by persons on these lists to open accounts or by existing account holders to initiate a transaction with such people. But it is far more difficult for a bank to detect when OFAC controls are intentionally circumvented or the counterparties of transactions are obscured. An AI-based system, however, would be able to prevent these transactions specifically by not relying on defined rules.

Acceptance of AI

In addition to general resistance to the use of AI – there are innumerous articles and books detailing how people remain uncomfortable with thinking machines and the use of vast troves of digital data (citing, among others, privacy concerns) – using AI in RegTech faces two main hurdles: the potential for algorithmic bias and regulatory hesitation for a full embrace.

Algorithmic bias occurs when a system incorporates existing human biases into its relationship model and generates discriminatory outcomes. This can occur in a number of ways, including through input bias (source data are flawed or prejudiced), training bias (training or teaching incorporates flawed or prejudiced baseline assumptions) and programming bias (the algorithm learns bias as it reviews and analyses data). Although these biases are often inadvertent, the potential risk for banks is significant. Consider an AI-based AML system that eventually starts to reject all new account applications from people of a particular race. Such a system would not only present fair lending risk in the context of credit products, but also pose significant liability and reputation risk issues for the institution in failing to maintain a reasonably designed AML programme that incorporates a risk-based approach to meet legal requirements. Moreover, the potential risks for an institution in the AML and sanctions context are magnified given the potential civil and criminal consequences for noncompliance, not to mention the public safety issues arising from the criminality of the conduct sought to be deterred. Thus, the accuracy, transparency, functionality and continuing reliability of an AI system is imperative.

So far, regulators are taking reactive stances and proceeding with caution in evaluating and adopting new methods, particularly when it comes to AML regulations. The bedrock of AML is the 'know your customer' (KYC) regime, requiring institutions to verify the identity of customers, clients and business partners, including their beneficial owners if they are legal persons. KYC, to a large degree, depends on customers telling a bank that they themselves are a high risk. Even though an AI-based system would be more effective at preventing actual money laundering and terrorist financing, banks must still use a traditional KYC approach because the regulations focus on the process, not the results.

Recently, regulators have signalled a growing openness to FinTech and RegTech. In late 2016, the Office of the Comptroller of the Currency announced it is considering granting new special purpose national bank charters for FinTech companies, and the Federal Reserve System published a paper detailing how FinTech could improve the payments and settlements systems. In the hope that proven results will motivate regulators to act, many banks are running AI-based RegTech solutions in parallel with traditional KYC and AML systems. Given the

current rate of development of AI, it is likely that this last hurdle of regulatory uptake will happen soon, with 2017 the year that AI begins to assume primary responsibility for AML and OFAC compliance. R&C

Kevin Petrasic
Partner
White & Case LLP
T: +1 (202) 626 3671
E: kevin.petrasic@whitecase.com

Benjamin Saul
Partner
White & Case LLP
T: +1 (202) 626 3665
E: benjamin.saul@whitecase.com

Matthew Bornfreund
Associate
White & Case LLP
T: +1 (202) 637 6258
E: matthew.bornfreund@whitecase.com