CLIFFORD

CHANCE

AI AND RISK FOR FINANCIAL INSTITUTIONS

— THOUGHT LEADERSHIP

MARCH 2019

AI AND RISK FOR FINANCIAL INSTITUTIONS

Artificial intelligence (AI) has the capability to unlock huge volumes of data and is revolutionising the financial services industry. It creates huge opportunities for both established and disruptive fintech businesses, but with rewards, comes risk.

This year, we are likely to see existing law and regulation (and those who enforce it) adapting to address AI, alongside the implementation of new, standalone, AI regulation. In this article, which was first published by the International Financial Law Review, we highlight the legal, ethical and reputational risk that UK financial institutions face when using AI and suggest the steps that they should take now to minimise them.

AI data and behaviours

AI, in its simplest form, represents "data inputs" which, when overlaid with digital/computer code, train the AI to achieve a particular intelligent behaviour as an "output."

In 2018, the General Data Protection Regulation (GDPR), implemented via the UK Data Protection Act 2018 (DPA 2018) led to a focus on financial institutions' use of personal data. However, the potential scope of data inputs used by AI is significantly broader and includes, for example, customer data, structured market data, or unstructured big data (such as news reports and social media).

To fully understand their AI exposures, firms need to understand (and ensure that their systems and controls address) how all of this data is used.

Existing law and regulation applicable to AI

Regulators and law enforcement agencies have already demonstrated their willingness to apply existing legislation to new digital markets and technologies. As they do so, financial institutions may also be exposed to parallel (or standalone) civil claims in the English courts. Here are some of the risks:

- **Misuse of data:** Under GDPR, individuals have the right to know how their personal data is being used by AI. GDPR promotes fair and transparent processing by requiring firms to provide individuals with meaningful information about the logic involved, as well as the consequences of the processing. As well as the risk of enforcement action, Financial institutions should be aware that GDPR (and section 168 of the DPA 2018) gives individuals the right to bring civil claims for compensation, including for distress, for personal data breaches. In relation to big data, the Financial Conduct Authority (FCA) signalled in its 2018/19 business plan that it would "review the use of data by financial services firms, including machine learning analysis of big data pools, algo trading and wider artificial intelligence… to assess harm and where we may need to intervene."
- **Fairness, discrimination and bias:** There is an inherent risk of AI incorporating biased datasets and creating biased outcomes, which can lead to unfair or discriminatory decision making. In July 2018, Charles Randall, FCA and Payment Systems Regulator (PSR) chair, highlighted several examples of AI in financial services which risked exacerbating social exclusion, such as credit card companies cutting credit limits when charges appeared for marriage guidance counselling (since marriage breakdown is highly correlated with debt default). Financial institutions need to monitor such usage of AI to avoid potential breaches of FCA Principle 6 and facing discrimination claims in the English courts.
- **Anti-competitive conduct:** Financial institutions need to ensure that their use of AI is not anti-competitive. For example, complaints may be made where financial institutions implement algorithms (including those procured from external suppliers), which could drive common customer outcomes

across the industry (for example, where a certain class of customer is at risk of foreclosure from products or services). The UK Competition and Markets Authority (CMA), has already used its powers to restrain technology with an anti-competitive objective. In August 2016, it fined Trod, an online seller of posters and frames, for using software to implement an agreement with a competitor not to undercut each other's prices. Margrethe Vestager, European Commissioner for Competition, has specifically identified the misuse of algorithms to fix prices and has highlighted how EU regulation is evolving to tackle the issues. Again, firms face the parallel risk of follow-on civil claims.

- **Systems and controls:** The Prudential Regulation Authority (PRA) and FCA have both shown their willingness to apply existing regulatory principles to AI, meaning that firms need to be mindful of an overreliance on automation, insufficient oversight and ineffective systems (as for any existing processes). In the context of reviewing automated investment services (or robo-advice), the FCA noted that firms should… "ensure clear oversight over the auto advice proposition, as well as clear allocation of responsibilities". The FCA has also reported on the supervision of algorithmic trading in wholesale markets. Firms should be aware that the FCA can require them to produce a description of their algo-trading strategies within just 14 days, and that it recommends that firms have a detailed "algorithm inventory" setting out coding protocols, usages, responsibilities and risk controls.
- **Market abuse:** The FCA is particularly focused on procedures countering the risk that AI is used to further financial crime, including the testing of algorithms to assess the impact they may have on market integrity, alongside post-trade monitoring. If trading on the basis of big data analysis, firms need to be sure that datasets do not contain confidential information (whether from within the firm or elsewhere) that amount to inside information. If using algorithms to make or determine orders, firms to be sure that the algorithm will not behave in a manipulative manner, whether immediately or later through iterative "learning". Where AI is used in generating published or disseminated information (for example in generating published research), firms need to be sure that such information is not misleading. Julia Hoggett, Director of Market Oversight at the FCA, said in a recent speech: "I can see a world where seemingly 'rational' AI, unconstrained and exposed to certain markets and data, would deem it entirely rational to commit market manipulation. Now, the FCA cannot prosecute a computer, but we can seek to prosecute the people who provided the governance over that computer." Firms also need to have systems in place to prevent and detect such forms of market misconduct by their clients.
- **Liability in contract and tort:** AI usage (whether by a firm's suppliers or by the firm with its customers) may give rise to unintended consequences and may expose institutions to claims for breach of contract or in tort, and test the boundaries of existing exclusion clauses. Firms need to assess whether their existing terms and conditions remain fit for purpose, where AI is concerned.
- **Product liability:** AI or robots, as physical products, can also be covered by the EU's product liability laws (such as the Directive on Liability for Defective Products and the Product Safety Directive), which provide for strict liability.
- **Further exposures:** Breaches of FCA Principles in relation to AI also give rise to further exposures for financial institutions' senior managers (under the Senior Managers and Certification Regime (SMCR)), and to additional potential civil liabilities under the Financial Services and Markets Act 2000, which allows private persons a right to sue the firm in respect of losses suffered as a result of FCA or PRA rule breaches.

Ethical use of AI

As well as the legal risks, financial institutions need to focus on managing the ethical issues of AI. The public debate is now on how firms should behave, rather than simply complying with the law. Technology companies (such as Facebook and Google) have been under political scrutiny and we expect the financial services sector to be next.

A challenge for global firms is to identify a consistent set of ethical standards and

> “The public debate is now on how firms should behave, rather than simply complying with the law.”

“Financial institutions may wish to reflect on how their own core values are reflected in their firm’s use of AI.”

values, across multiple jurisdictions where there may be cultural variations, in circumstances where the capabilities of the AI are constantly evolving.

Singapore was one of the first jurisdictions to focus on the ethical use of AI. It announced the Singapore Model Artificial Intelligence Governance Framework at Davos, in January 2019. This is a living document, designed to help organisations ensure that decisions made by or with the assistance of AI are explainable, transparent and fair to consumers and that AI solutions are “human-centric”. This framework builds on the earlier publication in November 2018, by the Monetary Authority of Singapore (which regulates financial institutions in Singapore) of its fairness, ethics, accountability and transparency principles to promote the responsible use of AI and data analytics and to assist firms in contextualising governance of such technologies in their own business models and structures.

UK and EU bodies are currently consulting on ethical guidelines applicable to AI. Whilst they are doing so, financial institutions may wish to reflect on how their own core values are reflected in their firm’s use of AI, particularly given the FCA’s continuing focus on firms’ culture. As Charles Randall highlighted in a speech on Big Data and AI in 2018: “Firms need to anticipate the effect that more technology will have on their culture, and design systems to maintain good judgment.” Accordingly, financial institutions need to buy and build their AI with ethics in mind.

2019 – the year of standalone AI regulation?

We expect to see increasing standalone regulation of AI at a UK and international level in 2019.

Among the initiatives supporting this view are the UK Government’s establishment of an industry-led AI Council, a new Government Office for AI and a new Centre for Data Ethics and Innovation (CDEI) to strengthen the existing governance landscape and ensure ethical and innovative uses of data and AI.

In 2018, the House of Lords Select Committee (HoLSC) on AI, and the House of Commons Select Committee on Science and Technology (HoCSTC), published reports exploring the lawful and ethical use of AI. The HoLSC recommendations included establishing a cross-sector AI code, to preserve the intelligibility and fairness of AI and protecting the privacy and data rights of individuals.

Roger Taylor, chair of the CDEI, told the HoCSTC that the CDEI was “listening to the public” about the use of AI. It will work with consumer associations, civil society organisations and use social media to ensure their voices are heard (cognisant of the fact that often those most at risk of harm by AI are often those most ignored). The CDEI anticipates reports into micro-targeting (and its regulation) and algorithmic bias.

In 2018, both the FCA and the PRA recognised the potential benefits of machine learning and AI as supervision tools, on the basis that “much regulation is ultimately about recognising patterns in data”. As Stefan Hunt, head of behavioural economics and data science at the FCA, has highlighted: “Using data science, we can understand the markets we regulate, the players within them, and the relationships between those players. We can move from a deluge of data to a nuanced overview.”

Finally, the European Commission’s High Level Expert Group on Artificial Intelligence (AI HLEG) is due to publish the final version of its AI Draft Ethics Guidelines in March 2019. Similar to the Singapore Model Framework, it focusses on fundamental rights, regulation and core principles (such as “ethical purpose” and “trustworthy AI”) but also highlights that AI should be technically robust and reliable. The AI HLEG will put forward policy recommendations with respect to AI in May 2019. Regardless of whether the UK remains in the EU, firms will need to consider HLEG’s recommendations.

Practical issues for financial institutions

AI is typically used across business lines and technology teams’ responsibilities, areas of legal coverage and across different geographies. This dispersion creates risk for institutions.

The very nature of AI's functionality, embedded in computer code, means that it is not necessarily accessible to those with the usual control functions in institutions (such as legal, compliance and internal audit). That needs to change. Firms need to focus on understanding how their AI technology works, and how they would explain it in an accessible and transparent way to build trust with customers and employees (and to the regulators and judges, who will require such explanations).

Those explanations might take the form of pre-approval processes for AI; consideration of the data inputs; requirements for those programming AI to maintain a living manual; and/or testing or reverse-engineering AI's decision making and behavioural outputs. The objective is to translate computer code and its decisions into descriptive text.

In our experience, the starting point for proper governance of AI is clear leadership, with firms' boards and general counsels overseeing AI risk management and embedding a culture of transparent, ethical use of AI.

In this context, the approach of many leading firms to human rights can provide a practical roadmap. Institutions who are signatories to the UN Global Compact will have already undertaken diligence and active monitoring to ensure their businesses are compliant. One option for firms is to mirror that top-down and end-to-end approach regarding AI.

We recommend that financial institutions consider the following issues. First, due diligence of AI usage: financial institutions that wish to minimise AI risk, need to assess their use of AI from supply chain to clients, encompassing AI technology that has been bought (from suppliers or via M&A) or built in-house. This diligence needs to consider:

- Dataset cleanliness: Where does the data come from? Does the firm have consent/the right to use it? Is bias in the data inputs to AI being addressed?
- Transparency: How is data being used and decisions made? How is that communicated to stakeholders, whether suppliers, employees or customers?
- Control: When can the firm's customers opt-out? Does the firm have control of the AI it uses?
- Explanations: Can the firm identify a written explanation of the AI's functionality? How and where is it documented and is it up to date?
- Review: Is the firm monitoring and/or testing the AI's decision making? To what extent is there human oversight?
- Limits: Have boundaries been set regarding use of AI? Who could be harmed by its use? Are there uses that the firm will not countenance? Is there an off-switch?
- Liability: What is the contractual framework for the use of AI? How is liability apportioned between the firm and its suppliers on the one hand, and the firm and its customers on the other?
- Third parties: Which third parties is the firm comfortable working with and transferring/selling data to? How will the firm audit and check this shadow AI infrastructure?

A second consideration would be any existing policies/control frameworks, for example: GDPR compliance, human rights policies, competition policies, codes of conduct and new product approvals. To what extent do these procedures already contemplate AI use? If they do, are they consistent?

A third important issue is management responsibility. Firms need to determine and document management responsibility for a business' use of AI, with a consistent approach taken across the firm. Senior managers need to understand the technological capabilities of AI and how to challenge its operation.

For many financial institutions, a standalone AI framework will be appropriate, and should be a priority. This framework may well be the first document requested by regulators, litigants and politicians, if any AI issues should arise. Such a framework can also help demonstrate a firm's proper understanding of its AI use and its active management of AI risk.

AUTHOR

London

Kate Scott
Senior Associate
T: +44 20 7006 4442
E: kate.scott@
cliffordchance.com

CONTACTS

Dubai

Jack Hardman
Senior Associate
T: +97 14 503 2712
E: jack.hardman@
cliffordchance.com

Hong Kong

Ling Ho
Partner
T: +852 2826 3479
E: ling.ho@
cliffordchance.com

London

Jonathan Kewley
Partner
T: +44 20 7006 3629
E: jonathan.kewley@
cliffordchance.com

Nelson Jung
Partner
T: +44 20 7006 6675
E: nelson.jung@
cliffordchance.com

Sam Ward
Partner
T: +44 20 7006 8546
E: samantha.ward@
cliffordchance.com

Peter Chapman
Senior Associate
T: +44 20 7006 1896
E: peter.chapman@
cliffordchance.com

Oliver Pegden
Senior Associate
T: +44 20 7006 8160
E: oliver.pegden@
cliffordchance.com

Stephen Reese
Partner
T: +44 20 7006 2810
E: stephen.reese@
cliffordchance.com

Laila Wood
Senior Associate
T: +44 20 7006 5696
E: laila.wood@
cliffordchance.com

Milan

Andrea Tuninetti Ferrari
Senior Associate
T: +39 02 8063 4435
E: andrea.tuninettiferrari@
cliffordchance.com

Paris

Dessislava Savova
Partner
T: +33 1 4405 5483
E: Dessislava Savova@
cliffordchance.com

Singapore

Paul Landless
Partner
T: +65 6410 2235
E: paul.landless@
cliffordchance.com

Lena Ng
Partner
T: +65 6410 2215
E: lena.ng@
cliffordchance.com

US

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon@
cliffordchance.com

Steven Gatti
Partner
T: +1 202 912 5095
E: steven.gatti@
cliffordchance.com

OUR INTERNATIONAL NETWORK
32 OFFICES IN 21 COUNTRIES

Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

Riyadh*

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

CLIFFORD
CHANCE

This publication does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street,
London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571
Registered office: 10 Upper Bank Street,
London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications.

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or contact our database administrator by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ.

Abu Dhabi • Amsterdam • Barcelona
Beijing • Brussels • Bucharest
Casablanca • Dubai • Düsseldorf
Frankfurt • Hong Kong • Istanbul
London • Luxembourg • Madrid
Milan • Moscow • Munich • Newcastle
New York • Paris • Perth • Prague
Rome • São Paulo • Seoul • Shanghai
Singapore • Sydney • Tokyo • Warsaw
Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.