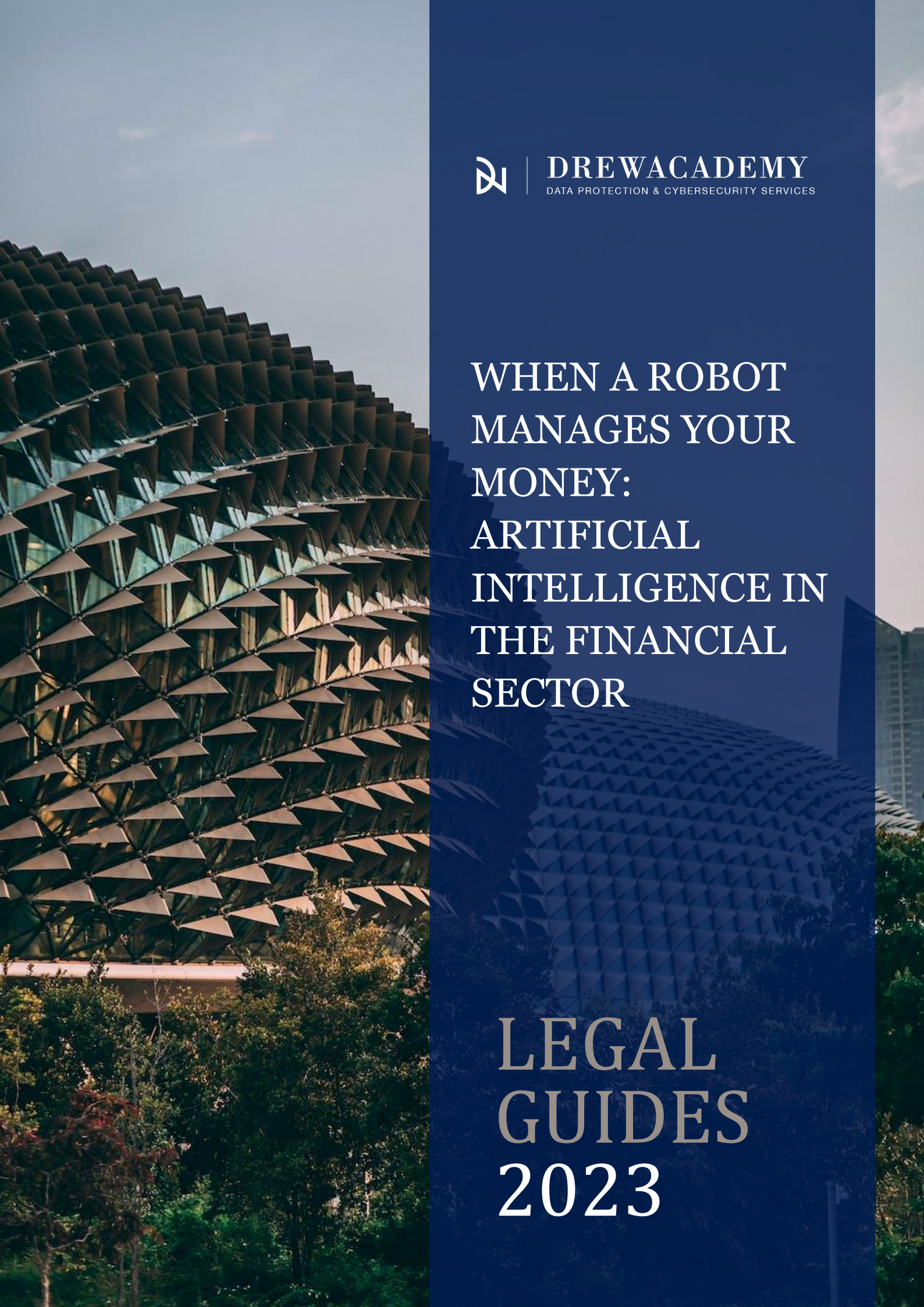

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

WHEN A ROBOT MANAGES YOUR MONEY: ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SECTOR

LEGAL GUIDES
2023

CONTENTS

Developments as of 11 April 2023

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

WHEN A ROBOT MANAGES YOUR MONEY: ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SECTOR

In 2018, the Monetary Authority of Singapore ("**MAS"**) published the *Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector* (the "**FEAT Principles**") to provide guidance to firms that use artificial intelligence ("**AI**") and data analytics to offer financial products and services.[1]

AI systems may bring about ever-increasing processing capabilities and value to data-driven decision-making processes. However, certain elements of AI deployments raise legal and regulatory questions. Without careful design and control, these systems can also bring new risks and unprecedented harms. This article will discuss the importance of the FEAT Principles in practice, as well as various countries' regulatory approaches in implementing similar principles.

Accountability

The question of who is responsible when AI makes a 'mistake' features in every industry. The financial sector is not an exception.

The case of *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02 ("***Quoine***") is the first-ever Singapore decision that ruled on the applicability of contractual principles in the context of algorithmic trading of digital tokens. Central to the case was the question of whether contracts formed through "deterministic" algorithms (i.e. algorithms that given a particular input will always produce the same output) are valid and if so, whether such contracts can be cancelled on the ground of unilateral mistake.

The Court of Appeal in *Quoine* confirmed that agreements formed purely through the operation of algorithms can be considered a binding contract. In deciding whether there was a unilateral mistake, the majority were of the view that reference should be made to the state of mind of the programmers of the algorithms at the time of the programming, up to the point that the relevant contract is formed. On the facts, because the programmer did not design the trading software to exploit any glitches on the other party's platform, nor did the programmer have any knowledge of the glitches occurring on the other party's platform until after the trades were made, the Court of Appeal upheld the contract.

The natural follow-up question is this: will the outcome be the same in the case of an AI system that is not considered "deterministic", in the sense that it "learns" to make decisions independently of its programmer(s) and it is programmed to continually "improve" and modify its behaviour based on new data inputs? As AI becomes increasingly autonomous and removed from human decision-making, would it still be appropriate to impute the programmers' knowledge for decisions made by a system whose parameters they did not set? In such scenarios, it can be difficult to prove the chain of causation and establish who will be at fault. This is exacerbated by the complex multi-party ecosystems in which AI systems are likely to be deployed: from developers, to data providers, and users.

Similar issues have also arisen in other jurisdictions. Up until the parties settled, the English courts had to consider for the first time who (if anyone) is liable when an AI-powered trading system causes substantial losses for an investor. In 2019, Hong Kong real estate tycoon Samathur Li Kin-kan sued a company that used trade-executing AI to manage his account, causing more than US$20 million in losses. Central to the parties' dispute was that Li claimed the company had exaggerated what the AI system could do and the returns it could make, where it would purportedly scan through online sources (news and social media) to gauge investor sentiment and predict US stock futures.[2]

The issue of accountability also throws the spotlight on the "black box" problem: if people don't know how the computer is making decisions, who is responsible when things go wrong? Members of the Financial Stability Institute of the Bank for International Settlements have commented that central to tackling the AI "black box" problem are concepts like "human-in-the-loop" (human intervention in the decision cycle of the AI) and "human-on-the-loop" (human intervention during the design cycle and

[1] While not the focus of this article, it is worth noting that the MAS also leads an industry consortium, Veritas, which is a multi-phased collaborative project that operationalises frameworks for financial services institutions based on the FEAT Principles.
[2] https://www.insurancejournal.com/news/national/2019/05/07/525762.htm

subsequent reviews), so that regardless of the inner workings of the AI system, the decisions it produces do not result in unfair or unethical outcomes.[3] Human interventions are required to the extent that humans must correct mislabelled data, override erroneous system decisions and feed updated data into the AI system.

Jurisdictions around the world are recognising that the adoption of systems centred on AI or machine-learning technologies should not reduce the existing accountability burden on humans. In response, countries are ramping up regulatory efforts in ensuring that there is sufficient human oversight in the deployment of AI systems. For instance, the Singapore regime under the *MAS Guidelines on Individual Accountability and Conduct*, which applies to regulated financial institutions, is intended to promote senior managers' individual accountability, strengthen oversight over material risk personnel and reinforce standards of proper conduct among all employees. Each senior manager's areas of responsibility must be clearly specified to ensure that relevant persons are held accountable over AI systems.

Transparency

Ancillary to the issue of accountability is the concept of transparency. The growing ubiquity of AI applications means that consumers need greater assurance in knowing that their personal data is adequately safeguarded, and that the organisation's use of AI to process their personal data is fair, explainable, and safe. This includes ensuring that data subjects are aware that AI is being used to make a decision in respect of them and have channels to inquire about and challenge those decisions.

The FEAT Principles state that financial institutions that use AI should provide data subjects (e.g. prospective financial customers) with channels to inquire about, submit appeals for, and request reviews of AI-driven decisions that affect them; and take into account verified and relevant supplementary data provided by data subjects when performing reviews of AI-driven decisions.

Similarly, the *MAS Guidelines on Provision of Digital Advisory Services* provide that as a general disclosure principle, digital advisers (also known as robo-advisers) which provide advice on investment products through their clients accessing automated, algorithm-based tools with limited or no human adviser interaction, should provide minimally, the following information to their clients: assumptions, limitations and risks of the algorithms; circumstances under which the digital advisers may override the algorithms or temporarily halt the digital advisory service; and any material adjustments to the algorithms.

Singapore also launched AI Verify, the world's first AI governance testing framework and toolkit, for organisations who want to be transparent about the performance of their AI systems through a combination of technical tests and process checks.

Of course, transparency is not a foreign concept in other jurisdictions. The European Union's General Data Protection Regulation ("GDPR") gives individuals a right of access to the personal data collected on them, so that they know how the data is used. More importantly, where automated decision making takes place, there is a "right of explanation" in Article 22 of the GDPR. Individuals must be informed of the fact of automated decision making, the significance of the decision on the individual, and be given an explanation of the automated decision after it has been made (i.e. meaningful information about the logic involved in the automated decision-making process). In combination, this provides data subjects with the ability to address any issues arising from the processing of their personal data, especially where the AI system is using data scraped from social media or other non-official sources to derive vital consumer information or make a decision in respect of the consumer.

In the US, certain algorithmic or AI-based collection and uses of data are subject to the Fair Credit Reporting Act, which is designed to ensure that the data collected by credit rating agencies is accurate

[3] https://www.bis.org/fsi/publ/insights35.pdf

and up to date. Consumers have the legal right to ask for their credit report, which includes all the information that goes into their credit score, and to have them fixed if there are mistakes.

Fairness & Ethics

Many jurisdictions have laws that aim to ensure fairness in the provision of financial services. For example, in the US, the Equal Credit Opportunity Act prohibits discrimination in access to credit based on protected characteristics such as race, colour, sex, religion, age and marital status. In Australia, federal anti-discrimination laws cover a wide range of grounds broadly including race, sex, disability and age. However, despite these measures, discrimination can still creep into the system if the data used to train the AI system is flawed.

Unintended biases and discrimination, particularly in the credit and insurance sectors, are often sources of controversy. For example, insurance companies have been accused of giving higher premium quotes to drivers named 'Mohammed' than 'John', all else being equal.[4] In 2019, gender discrimination complaints arose when entrepreneur David Heinemeier Hansson went public on Twitter stating that the Apple Card algorithm gave him a credit limit 20 times higher than his wife's despite the fact that she had a higher credit score and they filed joint tax returns.[5]

It appears that while the use of AI can help insurers assess risk, detect fraud and reduce human error in the application process, it can also perpetuate discrimination. For instance, insurers' decisions can be based on misleading or unrepresentative data or historically biased data, which can lead to unfair outcomes for clients.

In the credit scoring sector, there are concerns that AI models may contain hidden biases against disadvantaged communities, limiting their access to credit. For example, predictive algorithms (such as for a loan approval) may favour groups that are better represented in the training data. In fact, studies have shown that credit score algorithms are less accurate in predicting creditworthiness for lower-income families and minority borrowers, often because these groups have limited credit histories.[6]

Cybersecurity

Finally, the increased adoption of AI systems also exposes financial institutions to greater operational vulnerabilities. This was demonstrated in 2013 when hackers took control of Associated Press' Twitter account and propagated false claims of explosions at the White House.[7] The US stock market was sent into freefall, spotlighting the vulnerability of high-frequency trading algorithms (that predict sentiments in the financial markets based on social media data and thereafter execute trades) to fake news.

The susceptibility of AI systems to external threats like cyber attacks (e.g. data poisoning attacks) and technology failures underscores the importance of strengthening operational resiliency within the financial sector. Operational resilience is the ability of an institution to continue delivering its critical operations through disruption, as well as its ability to identify and protect itself from threats, and learn and recover from disruptive events.[8] The Basel Committee on Banking Supervision has issued principles for operational resilience to help coordinate national approaches in this area.

In Singapore, MAS imposes requirements it considers necessary for the management of technology risks, including cyber-security risks. For example, financial institutions are subject to MAS' *Technology Risk Management Guidelines*, as well as Notices on Cyber Hygiene. In response to an increasing reliance on third-party outsourcing and non-outsourcing arrangements, MAS also recently issued an Information paper on *Operational Risk Management - Management of Third Party Arrangements*.

[4] https://www.thesun.co.uk/motors/5393978/insurance-race-row-john-mohammed/
[5] https://www.washingtonpost.com/business/2019/11/11/apple-card-algorithm-sparks-gender-bias-allegations-against-goldman-sachs/
[6] https://hai.stanford.edu/news/how-flawed-data-aggravates-inequality-credit
[7] https://www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html
[8] See "*Principles for Operational Resilience*" by Basel Committee on Banking Supervision, https://www.bis.org/bcbs/publ/d516.pdf

With the proliferation of AI and big data, the dissenting judge in *Quoine* is right in pointing out "[t]he law must be adapted to the new world of algorithmic programmes and artificial intelligence, in a way which gives rise to the results that reason and justice would lead one to expect." Given the importance of good AI governance in the financial sector to ensure that the use of AI is fair, explainable, accountable and transparent, development of international standards or guidance in this space should be encouraged and embraced.

Drew Academy wishes to acknowledge our Associate Zhu Zhuohui for assisting in the preparation of this article.

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Benjamin Gaw
Director, Corporate and
Merger & Acquisitions;
Head, Healthcare & Life Sciences
(Corporate & Regulatory)

T: +65 6531 2393
E: benjamin.gaw@drewnapier.com

David N. Alfred
Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head and Programme Director,
Drew Data Protection &
Cybersecurity Academy

T: +65 6531 2342
E: david.alfred@drewnapier.com

Cheryl Seah
Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152
F: +65 6535 4864
E: academy@drewnapier.com

In association with

DREW & NAPIER