ARTIFICIAL INTELLIGENCE APPLICATIONS IN FINANCIAL SERVICES

ASSET MANAGEMENT, BANKING AND INSURANCE

CONTENTS

AUTHORS

Hermes Investment Management
Chi Chan, Dr Christine Chow, Janet Wong, Nikolaos Dimakis

Marsh
David Nayler, Jano Bermudes

Oliver Wyman
Jayant Raman, Rachel Lam

Bryan Cave Leighton Paisner LLP
Matthew Baker

FOREWORD

This paper is a very valuable guide to the uses, opportunities and pitfalls behind the deployment of Artificial Intelligence (AI) in the Banking, Insurance and Asset Management industries. It should be required reading for all boards of directors involved in these businesses. The paper is simply structured by topic with helpful end of section questions that boards might think about and ask their relevant management teams to answer.

Most importantly the paper highlights that AI should not be thought of simply as a business tool but rather as a transformative business philosophy that needs to be considered in a very broad, multi-dimensional context. The deployment of AI within financial services raises many questions around regulation (still developing and changing quickly), data protection, security and most importantly, the ethical use of insights gained from personal data. Boards need to consider deeply the moral and legal consequences of their usage of AI. These are not simple subjects, and nor have they been dealt with previously – so we are all feeling our way. But the authors provide a very readable, easy to digest guide to these issues with many source reference works that will help all interested parties navigate their way successful through these uncharted waters.

Paul Smith
Advisor; Former President and CEO, CFA Institute

EXECUTIVE SUMMARY

Artificial Intelligence (AI) is a powerful tool that is already widely deployed in financial services. It has great potential for positive impact if companies deploy it with sufficient diligence, prudence, and care. This paper is a collaborative effort between Bryan Cave Leighton Paisner LLP (BCLP), Hermes, Marsh, and Oliver Wyman on the pros and cons of AI applications in three areas of financial services: asset management, banking, and insurance. It aims to facilitate board-level discussion on AI. In each section, we suggest questions that board directors can discuss with their management team.

We highlight a number of specific applications, including risk management, alpha generation and stewardship in asset management, chatbots and virtual assistants, underwriting, relationship manager augmentation, fraud detection, and algorithmic trading in banking. In insurance, we look at core support practices and customer-facing activities. We also address the use of AI in hiring.

There are many benefits of using AI in financial services. It can enhance efficiency and productivity through automation; reduce errors caused by psychological or emotional factors; and improve the quality and conciseness of management information by spotting either anomalies or longer-term trends that cannot be easily picked up by current reporting methods. These applications are particularly helpful when regulations, such as the European Union Markets in Financial Instruments Directive II (MiFID II), increase senior management's level of responsibility to review and consider higher-quality data generated by the firm.

However, if organisations do not exercise enough prudence and care in AI applications, they face potential pitfalls. These include bias in input data, process, and outcome when profiling customers and scoring credit, as well as due diligence risk in the supply chain. Users of AI analytics must have a thorough understanding of the data that has been used to train, test, retrain, upgrade, and use their AI systems. This is critical when analytics are provided by third parties or when proprietary analytics are built on third-party data and platforms.[1] There are also concerns over the appropriateness of using big data in customer profiling and credit scoring. In November 2016, for instance, a British insurer abandoned a plan to assess first-time car owners' propensity to drive safely – and use the results to set the level of their insurance premiums – by using social media posts to analyse their personality traits.[2] The social media service company in question said that the initiative breached its privacy policy, according to which data should not be used to "make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan."[3]

These concerns often have legal and financial implications, in addition to carrying reputational risks. For example, the General Data Protection Regulation (GDPR) gives EU citizens the right of information and access, the right of rectification, the right of portability, the right to be forgotten, the right to restrict the processing of their data, and the right to restriction of profiling. However, it is unclear how easily individuals can opt out of the sharing of their data for customer profiling. It is also unclear whether opting out will affect individuals' credit scorings, which in turn could affect the pricing of insurance products and their eligibility to apply for credit-based products such as loans.

There have already been fines and legal cases related to discrimination and the opacity of AI applications. In October 2018, a leading insurer in the United Kingdom was fined £5.2 million by the Financial Conduct Authority (FCA)[4] for poor oversight of a third-party supplier – one of the largest fines for a failure in an outsourcing relationship. FCA said that the insurer's overreliance on voice analytics software led to some claims being unfairly declined or not being investigated adequately. Separately, a trial is scheduled for May 2020 in what is believed to be the first lawsuit over investment losses triggered by autonomous machines. An investor made a claim against a UK-based investment advisor, alleging misrepresentation and breach of contract in relation to a supercomputer purported to use online sources to gauge investor sentiment and make predictions for US stock futures.

Calls for the ethical and responsible use of AI have also grown louder, creating global momentum for the development of governance principles, as noted in a 2019 paper by Hermes and BCLP.[5] However, the real challenge is to shift from principles to practice.

QUESTIONS FOR BOARDS

Given the financial implications, companies should ensure that senior management and the board have sufficient understanding of AI and other technology used in the business to provide proper oversight. This is particularly important given the increasing expectations for board directors to oversee material issues that affect a company's long-term value. The board is "responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives," according to the UK Corporate Governance Code.[6] It "should maintain sound risk management and internal control systems"[7] to ensure that the risk framework is sufficiently up to date, and that the entity's risk appetite is appropriately set, monitored, and communicated. The decision making, implementation, and use of AI must take place within a risk management framework that captures changes to the business. Whether the framework follows the International Organization for Standardization (ISO), the Committee of Sponsoring Organizations (COSO), or another model, it will cover four main activities: risk identification, risk assessment, risk mitigation, and risk monitoring. These will be complemented by early intervention, incident preparedness, crisis response plans, and training.

In addition to the specific questions on AI applications outlined in "How is AI applied in financial services?", we would expect board directors to address the following questions:

- What is the company's AI footprint?
- Does the board have any oversight of the company's use of AI?
- If yes, what is the specific expertise that will enable the board to oversee the use of AI?
- How does the board oversee the use of AI? What are the related documents that the board reviews? What questions does the board pose to the management team?
- Does the company have a set of AI governance principles? If so, how are these implemented? How does the board assure itself that these principles are fit for purpose and actually implemented?
- Does the board have the appropriate skills and expertise to oversee the risks and opportunities arising from AI? If not, does it at least have access to such skills and expertise?
- Does the company engage with policymakers and other relevant stakeholders on AI governance?
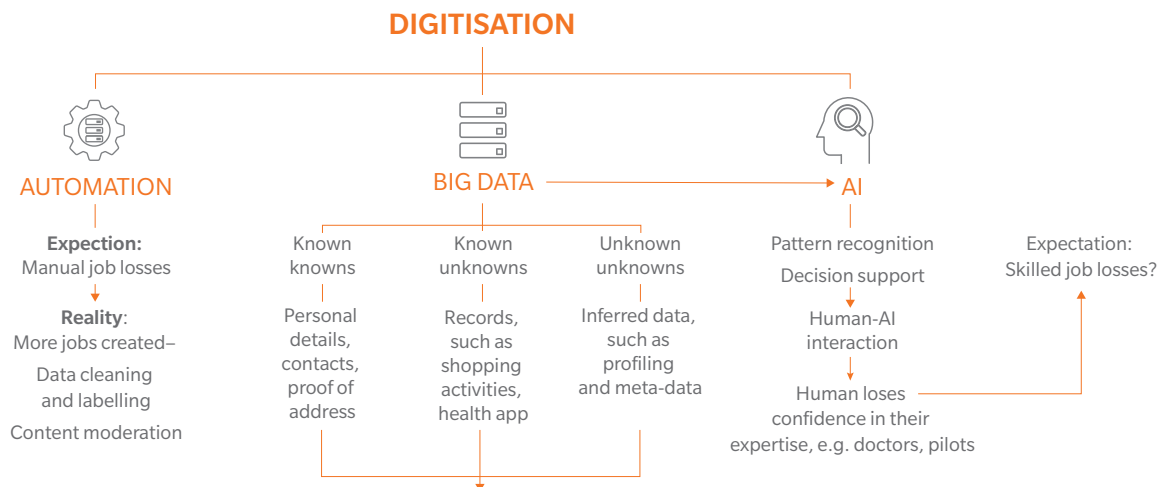
WHAT IS ARTIFICIAL INTELLIGENCE?

AI NEEDS TO BE CONSIDERED IN THE CONTEXT OF TRENDS SUCH AS DIGITISATION, AUTOMATION, AND BIG DATA

Artificial Intelligence (AI) consists of the use of computers and algorithms to augment and simulate human intelligence. AI enables adaptive pattern recognition using large volumes of data and modern statistical methods to give the 'best guess' answer to any narrowly defined and definitive problem set. Essentially, it is an optimisation machine. The analysis is based on the data provided to a computer program, rather than the innate intelligence of the machine. We explain below why it is important to consider AI as part of wider industry trends instead of as an isolated topic:

Digitisation is an overarching industry trend, driven by automation's promise of greater effectiveness and cost efficiency. (See Exhibit 1.) However, the process of digitisation is showing signs of being more complicated than expected. For example, the UK government started the GOV.UK Verify project in 2011, with the aim of providing users with a single login to verify their identity for all UK government digital services. This turned out to be a colossal task involving the combination of several processes: the standardising of data input configurations, the categorisation of data types, managing historic or legacy data,

EXHIBIT 1: CONCEPTUAL MAP OF DIGITISATION, BIG DATA AND AI

DIGITISATION

AUTOMATION

BIG DATA

AI

Expection:
Manual job losses

Reality:
More jobs created–
Data cleaning and labelling
Content moderation

Known knowns

Personal details, contacts, proof of address

Known unknowns

Records, such as shopping activities, health app

Unknown unknowns

Inferred data, such as profiling and meta-data

Pattern recognition
Decision support

Human-AI interaction

Human loses confidence in their expertise, e.g. doctors, pilots

Expectation: Skilled job losses?

Big data impact comes from the combination of the different types of data as described above, giving rise to the following issues with impact on individuals as well as corporates:

• Data privacy
• Pricing differentiation
• Service quality discrimination
• Segmented product offering
• Historical bias – sample vs. population (identifiable and diversifiable)
• Embedded bias - cultural/religious/political (debatable and undiversifiable)

and harmonising standards for various other kinds of data. According to a UK parliamentary update in May 2019, the project was delivered years later than the target date and the performance standards did not meet expectations.[8] This is only one example of the challenges of digitisation in a government project, yet digitisation is taking place across different industries and sectors.

Automation and straight-through processing (STP) have sparked societal concerns of job losses. However, data preparation is messy, and new jobs are created as data need to be tagged, checked, cleaned, formatted, and labelled. These steps are essential for AI, as it relies on good quality datasets for training, testing, and delivering consistent performance. Moreover, AI algorithms need to be retrained intermittently, as new data become available and competitors create more sophisticated analytics.
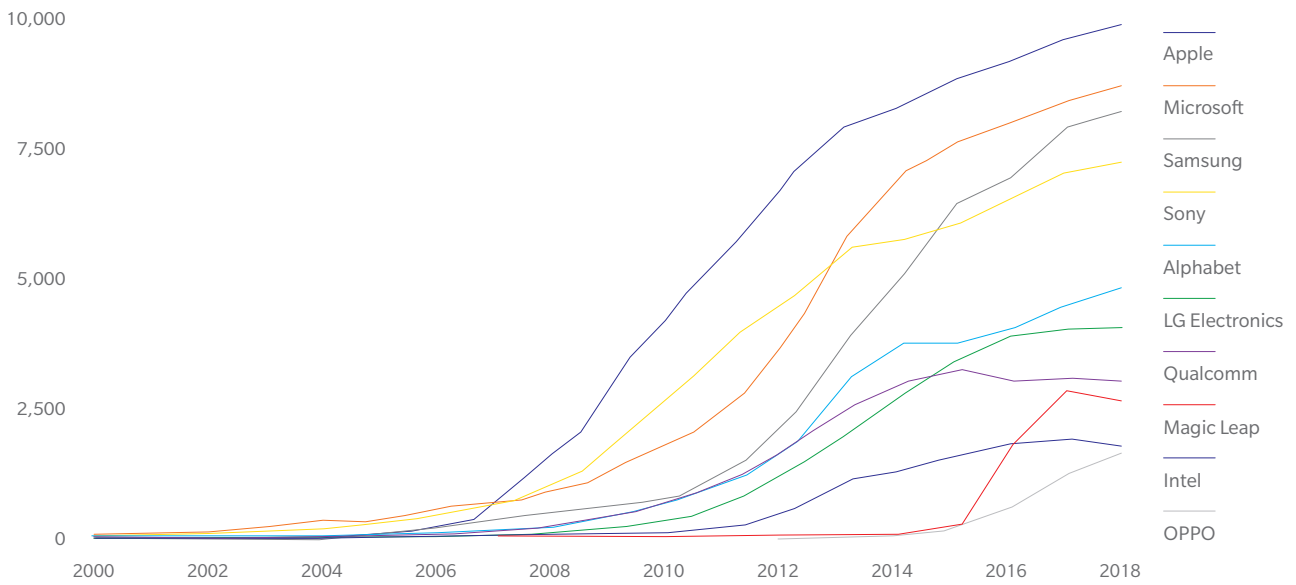
Digitisation and AI both harness **big data** on people and their behaviour. Our understanding of what data are requires some rethinking. To borrow the words of former United States Secretary of Defense Donald Rumsfeld, people's data can be categorised into three main categories:

- **"Known knowns"** are data that we know exist and that we know. For example, someone who opens a bank account provides their name, address, telephone number, gender, date of birth, and so on. These are hard data that we can check and validate and for which evidence can be provided to prove their authenticity.

- **"Known unknowns"** are data that arise from people's activities. They include health data recorded on digital health apps and fitness wearables, as well as data recorded during online shopping. We know that such data exist,[9] but we do not know how they are packaged, anonymised, and used – or how they may be sold to data brokers.[10] Even anonymised data can be reengineered if specific personal data such as post codes, locations, and medical information are known.

- **"Unknown unknowns"** are data that are created without our knowledge. People have few – or no – opportunities to validate such data and whether they accurately describe them and their behaviour. For example, companies may have created a digital profile of each customer based on online behaviour such as YouTube searches and Netflix accounts. Increasingly, companies are using eyeball tracking, gesture tracking, and facial recognition to create metadata based on how a user interacts with their mobile devices. (See Exhibit 2.) However, people do not know what profiling buckets have been created to represent their digital attributes. As with the known unknowns, these inferred data may be packaged and sold onto data brokers after they have been anonymised.

EXHIBIT 2: PATENT ASSET VALUE[11] BASED ON FACIAL AND GESTURE RECOGNITION TECHNOLOGIES AND EYEBALL TRACKING

Patent Asset Index™

Development of the active portfolios of the top 10 companies in Eye Tracking, Iris Verification, Facial Recognition, and Gesture Recognition. Data as on 17th October 2019.

Academics have argued that customers' identities can be revealed if data are aggregated and powerful analytics such as AI are applied. This gives rise to new data privacy issues. Bias can potentially result from differentiation in pricing and service quality resulting from aggregated data and customer categorisation processes. Against the backdrop of these trends in digitisation and big data, we now evaluate the value that AI applications can add in financial services.
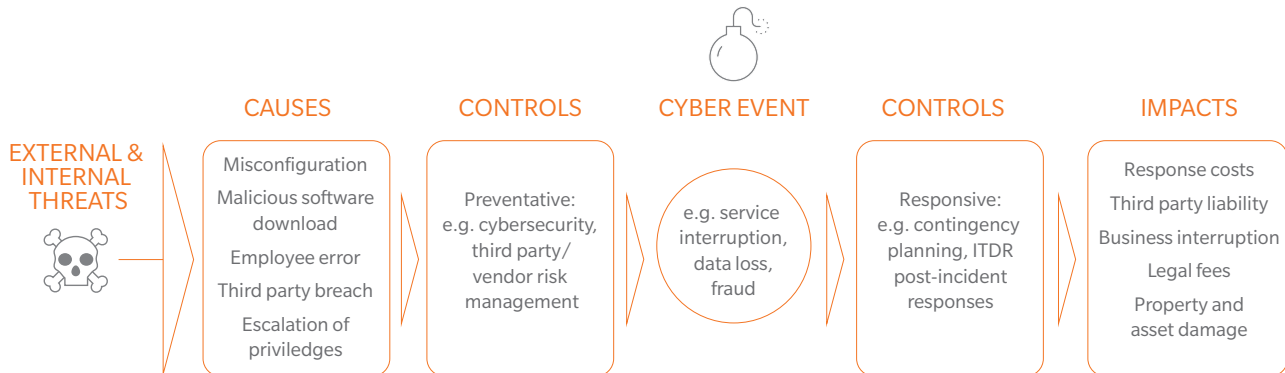
AI AND CYBERSECURITY

Two key aspects of cybersecurity in the context of AI are the following:

1. **The function of cybersecurity in securing all aspects of digital and data transformation and resilience.** This includes the confidentiality of sensitive information; the integrity of processing, which is of particular concern for AI implementation; and the availability of systems, data stores, and networks that are essential for ongoing service provision. The challenge is that technology continues to advance and transform. So an organisation's cybersecurity function must keep abreast of business changes in order to continue to develop effective approaches to protection and security. In addition, there is significant development and innovation in the security industry, making it challenging for professionals to keep up – and even just to assess the effectiveness of two alternative solutions, both of which promise a significant reduction in threat.

2. **The disruption of the cybersecurity industry itself. This is happening because of advances in adversarial threats that leverage AI to render accepted methods of protection ineffective.** This evolution has come about through automation, which makes possible complex attacks that could previously only be carried out by advanced, state-level actors with significant resources. These advances are then industrialised by creating malware or fraud-as-a-service models, enabling criminals with lower skills to monetise cybercrime.

In many ways, making bots secure is little different to making traditional IT services secure. In both cases, the first step is to consider various threats and potential causes and the second is to consider actual cyber events – such as a business interruption, data breach, or even physical damage. Finally, the potential implications and impact of a cyber incident are examined. This process allows for a holistic analysis of the problem and a layering of controls, whether these be technical, procedural, or process-oriented. They can be aimed at preventing an event from occurring, at responding to an event, or at mitigating or reducing impact to an acceptable level for the business. There are several established approaches to layering controls. Basic control frameworks include ISO27. More-advanced approaches, such as the US National Institute of Standards & Technology (NIST)'s cybersecurity framework or the MITRE framework, analyse cyberattacks differently. They layer preventative, detective, and responsive controls in order to disrupt or intelligently minimise the impact of attacks.

EXHIBIT 3: HOLISTIC ANALYSIS OF THE PROBLEM AND A LAYERING OF CONTROLS

EXTERNAL & INTERNAL THREATS	CAUSES	CONTROLS	CYBER EVENT	CONTROLS	IMPACTS
	Misconfiguration Malicious software download Employee error Third party breach Escalation of priviledges	Preventative: e.g. cybersecurity, third party/ vendor risk management	e.g. service interruption, data loss, fraud	Responsive: e.g. contingency planning, ITDR post-incident responses	Response costs Third party liability Business interruption Legal fees Property and asset damage

There are in fact some advantages related to the implementation of advanced automation, primarily that the human element, which is prevalent in cybersecurity attacks today, becomes much less of a risk. In addition, the operating parameters of systems are more predictable than those of humans, making it possible to implement more widely means of securing an environment such as whitelisting*, which had previously been less effective. This could reduce the cost of compliance.

Bots also come with disadvantages. Consider the implementation of third-party software in an environment that has been set up to support a highly regulated control regime such as the US Sarbanes Oxley Act 2002 (SOX), Payment Cards Industry Data Security Standards (PCI DSS), or another regime such as the General Data Protection Regulation (GDPR). Third-party software could impact the integrity of those systems, leading to a loss of confidentiality, an interruption of service, or impacts on the integrity of data stores or processing mechanisms. Such software could even lead to compliance violations.

Systemic cyber risk across all industries is rising with the use of automation. The ubiquitous evolution from cloud to mobile, followed by digital transformation and the use of AI, means that successful cyber exploits are likely to be effective across a broad range of industries and applications. In addition, digital economies are increasingly interconnected; regulation and the implementation of controls have become harmonised; and data formats have been standardised. As a result, events such as WannaCry** and NotPetya*** will become more likely and have greater impacts.

* Whitelisting is not a new concept in enterprise security. In contrast to blacklisting, application whitelisting is a proactive approach that allows only pre-approved and specified programs, tasks, or users to operate on the network. Any activity or user not whitelisted is blocked by default. Whitelisting controls can be implemented at the network, application, or user level. https://digitalguardian.com/blog/what-application-whitelisting-application-whitelisting-definition

Platforms that support these controls typically initially deploy machine learning to examine an environment and 'learn' what standard operation looks like. Once this phase has been completed, the system is changed to whitelist mode, where it blocks anything outside the standard operating baseline.

** The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm. It targeted computers running the Microsoft Windows operating system, by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

*** Petya is a family of encrypting ransomware that was first discovered in 2016. This malware targets Windows-based systems, where it infects the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. A variant used ransomware that did not have a decryption key. That meant it was a destructive attack rather than an extortion attack and was referred to as NotPetya. https://en.wikipedia.org/wiki/Petya_(malware)

HOW IS AI APPLIED IN THE CONTEXT OF FINANCIAL SERVICES?

APPLICATIONS IN ASSET MANAGEMENT

According to the 2018 Growth Readiness Study, asset managers who are embracing big data and analytics are found to be growing their revenue 1.5 times more quickly than the rest of financial services.[13] Pillars of AI transformation include generating alpha, enhancing operational efficiency, improving product and content distribution, and managing risk.[14] We focus on alpha generation and risk management in this section, as their applications tend to be specific for different sectors.
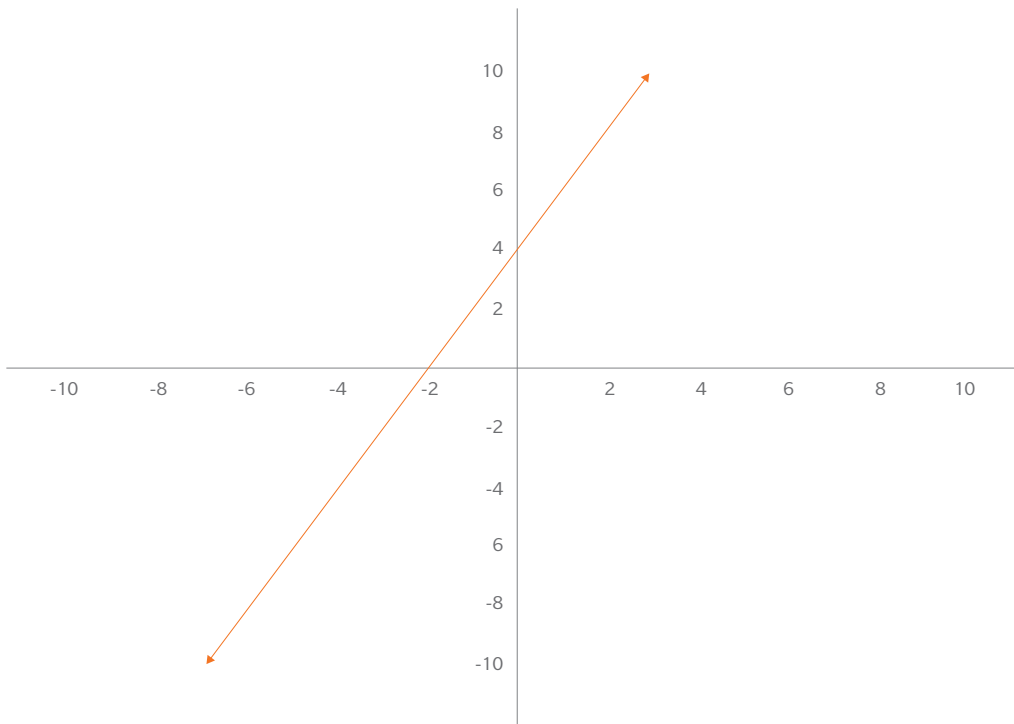
RISK MANAGEMENT

AI CHANGES RISK MANAGEMENT BY ENABLING THE INVESTIGATION OF NON-LINEAR RELATIONSHIPS

Developments in AI will rewrite the future of asset management globally, according to two-thirds of the respondents to an industry survey participated in by 45 chief investment officers and investment professionals in 16 countries.[15] A poll by industry data firm BarclayHedge[16] found that 56 percent of respondents were using these tools in their investment processes, while 33 percent were using machine learning for risk management.

Current challenges: Conventional risk models assume markets behave in linear relationships. (See Exhibit 4.) For example, stock prices are treated as a variable dependent on factors such as liquidity and macroeconomic conditions, as well as a company's profitability, debt-to-equity ratio, and net cash position. Multicollinearity is tested and factors are adjusted to minimise correlations amongst factors.

Each factor that contributes to risk gets a weighting, and those weightings do not tend to change. There is model risk arising from tail risks[17] – that is, the risk of idiosyncratic or extreme events that have a fundamental impact on the underlying assumptions that govern the distribution of data.[18] Value at risk (VaR), a widely used measure of the risk of loss for investments, is exposed to model risks and so applications are known to be limited to normal market conditions.[19]

EXHIBIT 4: LINEAR RELATIONSHIP MODEL

AI technology as an enabler: As traditionally taught and applied, statistics tends to assume normal distributions of data and to use significance testing methods from the 1930s. However, since the 1990s, more statistical methods have been established to address the non-linear nature of real-world events. One is machine learning, or AI, where data samples are weighted and applied to a specific architecture to make the machine intelligent.

How it works: The AI risk model can be used to challenge traditional risk-factor regression analysis and so demonstrate the pros and cons of each type of decision-support tool.

Added business value: Companies can use AI to model complex risks and carry out stress tests beyond business-as-usual scenarios.

Measurable results: Systematically better-managed downside risks and improved performance by investments and in environmental, social, and governance (ESG) factors.

ALPHA GENERATION

NEW FACTORS FOR ALPHA AND NEW INSIGHTS FROM BIG-DATA CORRELATION ANALYSIS

Current challenges: Fund managers and analysts face the 21st century challenge of data overload and fake news. Data analytics providers integrate Twitter and other social media feeds from selected corporates and influencers. But many professionals find that they are overwhelmed by the amount of information available, and there is an urgent need to establish a systematic way to organise and analyse large quantities of data.

AI as an enabler: AI technology helps draw correlations out of 'big data' and offers decision support. For example, financial institutions increasingly use AI in ESG evaluation. But ESG data often come in large quantities and are unstructured. To achieve consistency and comparability across companies, AI providers such as RepRisk, Truvalue Labs, and Arabesque S-Ray use proprietary algorithms to quantify ESG risks.[20] MioTech, a Hong Kong-based AI platform provider, derives one third of its revenue from ESG-related work, which includes using big-data correlations to spot ESG patterns.[21]

How it works: For AI to be useful to investors, analysts need to establish hypotheses on the possible relationships between data and the results obtained when they are used in investment analysis. For example, an analyst may believe that the value of a company – a dependent variable – is related to its commitment and ability to combat climate change and other factors, which are independent variables. The analyst would then have to design proxy indicators to measure both the company's commitment and its capabilities. A proxy for commitment might be the number of times a board chair has made a positive statement about combating climate change in speeches and publicly available documents. A proxy for capabilities might be a combination of weighted environmental scores from third-party rating agencies.

AI can then go through large volumes of relevant data sources, such as publications, annual reports, industry research, and YouTube and Vimeo videos, by using techniques such as natural language processing (NLP), natural language understanding (NLU) and sentiment analysis.[22] The modeler defines sentiment indicators with positive, negative, and neutral tones – that is, signal classification – though there are various clustering techniques, which may yield vastly different results.

The data universe worked on by analytics should be subject to scrutiny by users and buyers; it should not be a black box. Every dataset is a subset of all the data available in the world, so there is always a risk of excluding data that should have been included in an investment analysis. Users should also be aware of fake news that may have an impact on investments.

Data is only part of the overall picture. Firm value, a dependent variable, is a vague term, so it needs tighter definition. Here are some examples of proxy indicators of firm value:

- EV/EBITDA – enterprise value divided by earnings before interest, tax, depreciation, and amortisation. This measures the return on capital investment
- Total shareholder return (TSR), which measures the return to shareholders including dividend payments
- Earnings per share (EPS), which measures profitability, based on the assumption that investors are willing to pay more for profitable companies

Added business value: Research functions that are currently too costly or labour intensive can be automated. Currently these include going through multiple data sources – such as company blogs and industry reports – to identify relevant information that paints a full picture of a company's alpha generation and capability to create long-term value. Visualisation tools and user-friendly interfaces can help people grasp data better and gain insight from them.

Measurable results: Investment decisions can be made in a timely manner, improving the performance of investments and ESG factors.

SUITABILITY FOR ALPHA GENERATION AND STEWARDSHIP

The suitability of big data and AI for alpha generation will vary according to the investment style and process. High-frequency quant trading is entirely reliant upon powerful computers to analyse data feeds, identify patterns, and then act on the information at speeds that humans can't keep up with. On the other hand, Warren Buffet does not use a computer for his investments.[23] Most investors lie somewhere between those two extremes and should be able to benefit from AI to some degree.

Active portfolio managers can, roughly, be split into two camps: short-term and long-term. The value of short-term investments is influenced by catalysts. For example, a cold winter will increase demand for gas for heating, which will push up the price of gas. Therefore, reliable weather prediction will confer an investment advantage. Investors also need to consider whether regulations permit use of a particular data source. Seeing government data in advance of its release may be considered insider trading and illegal – as with the orange crop forecast report in the 1983 film Trading Places. However, analysing weather conditions and touring orchards to arrive at the same conclusion as the report would not be illegal. Therefore, the challenge for short-term investors is relatively straightforward: identify a cause-effect relationship and identify a way to predict the determining fact – or see it before others – in a legal manner.

Long-term investing brings different challenges. Over a longer time horizon, many more factors affect the value of the investment and it may be difficult to predict their impact. It may be tempting, therefore, for long-term investors to say that big data and AI have less relevance for them, as is the case with Mr Buffett. They may also argue that some AI applications, such as sentiment analysis, can intensify herd behaviour.[24] However, AI does

have value for long-term investors in its abilities to complete existing tasks in a more efficient manner and to offer additional insights when monitoring a portfolio. In particular, AI can help enhance investors' understanding of companies, which is an important element of their stewardship activities. An increasing number of third-party providers[25] are deploying AI to assess companies' exposure to ESG risks, such as water stress. Use cases include the application of AI both to collect data and to generate undisclosed or unmeasured data.

AI has the potential to significantly disrupt business models. If it is not handled appropriately, this could lead to significant damage to customers, employees, and society at large. That might make the assets unsustainable in the long term. As Saker Nusseibeh, the Chief Executive of Hermes, points out: "Active stewardship is the investment management industry's social license to operate."[26] As stewards of their clients' assets, asset managers must look after different stakeholders, including customers, employees, suppliers, investors, governments, and society. Therefore the industry has a key role in addressing global challenges such as climate change and inequality, in addition to and in order to deliver sustainable financial returns. In fact, both passive and active asset managers are now devoting more resources to stewardship. Collaborative efforts between the industry and companies' boards and management teams have substantial potential to harness the power of AI for the benefit of all stakeholders. That could, ultimately, help the assets create more sustainable wealth.

The Executive Summary outlined briefly why investors care about companies' responsible use of AI. The benefits and pitfalls mentioned apply to other sectors beyond finance. In the technology sector, there are concerns about data privacy and security in interconnected digital technologies following controversies over hidden microphones in home devices[27] and information sharing by voice-controlled virtual assistants.[28] Further examples are available in the Hermes' article *AI: brave new worlds*.[29]

Over the past few years, and especially in 2019, investors have been increasingly using their shareholder rights to engage with companies over the societal impacts of AI and technology in general. This is particularly the case for companies listed in the United States, where Amazon shareholders have put forward resolutions over various environmental and social issues. These include disclosure related to climate change, management of food waste, and the sale of facial recognition technology to government agencies, amid concerns that this can violate rights and target communities of colour.[30] Also in 2019, Alphabet's shareholders put forward a resolution urging the company to establish a societal risk oversight committee at the board level. The resolution also called for technology deployment to be subject to robust assessments of product design and impact, taking into account feedback from employees and developers. Facebook's shareholders called for better content governance. Though these resolutions were not approved, investors' concerns over this kind of topic are undoubtedly growing. The material ESG topics raised by shareholders are closely tied to companies' long-term value creation capacities, including their current business models. Investors' stewardship activities are therefore closely linked to the performances of their investments.

QUESTIONS BOARDS SHOULD ASK ABOUT AI DEPLOYMENT IN INVESTMENT ANALYSIS:

- Have you considered the network effects and scalability of AI applications in relation to third-party dependencies, such as for analytics?

- Could the use of a large amount of momentum-driven corporate ESG news push a value-driven investment manager to adopt more of an event-driven style, without them intending to?

- Are there published and peer-reviewed papers on the methodology of the AI systems you deploy?

- How do you map data from subsidiaries to parent or issuer companies? What is the procedure for when the relationship between subsidiaries and parents change over time?

- How often do you change your data universe? What would trigger a review?

- Do you test the consistency of outputs? If so, how often?

- Have you considered the potential disruption that AI might cause to business models of assets that have been invested in? What impacts might AI have on different stakeholders?

- What stewardship actions are you taking to support companies and other assets affected by disruption to business models? Do these meet the needs of all stakeholders?

Defining the investment proxy definitions and framework in which AI operates is crucial in its successful applications, and it lies in the responsibilities and choices of the modeller.

IS AI REALLY A BLACKBOX?

The term 'black box' is one of the industry's favourites. It implies that something happening is strictly proprietary and that it is so complicated that most people cannot understand how it generates the results it does. Essentially the term describes a system that receives a set of input signals and produces an output. This output can be of various types, such as a Boolean value – yes or no – a projected price trajectory, or a probability distribution. AI models are often considered black boxes, not necessarily because they are complicated. One possible reason is that they cannot be easily interpreted or visualised – either because they are highly recursive, as in the case of deep learning, or because they exist in a large number of dimensions, as with support-vector machines (SVMs). Another reason can be that their input signals are not known. A third possibility is that they are an ensemble of models rather than a single, independent model. To promote accountability and facilitate the audit of decisions, there has recently been a trend towards explainable AI – or XAI – that can be understood by non-experts.

Questions that boards should ask about the evaluation of an AI model:

- How dependent is the model on specific inputs?

- How are missing or non-synchronized data handled?

- What type of biases are inherent in the model?

- What type of metadata are generated to support the output?

- How is consistency of output guaranteed and monitored?

- What are the confidence intervals for the output?

- Does the current training set capture the complexity of the input data

APPLICATIONS IN BANKING

Artificial Intelligence (AI) is poised to be a game-changer for the banking industry. With numerous AI applications in the pipeline, huge gains could be realised over the coming decade. The industry is expected to save more than $1 trillion by 2030 thanks to AI, with traditional financial institutions shaving 22 percent from their costs.[31]

In this section, we dive into selected use cases and explore the impact that AI is making in the banking industry.

CHATBOTS AND VIRTUAL ASSISTANTS

Pressure is mounting on banks to adopt a digital mindset. They need to adapt to evolving customer expectations, reduce costs, prevent losses of business to nimbler start-up competitors, and find novel ways to grow revenues. Banks trying to expand face a barrier in the form of rising customer costs caused by rapid growth and widening product lines. They often struggle to deal with an inflating volume of call-centre queries and customer emails, as their traditional customer-service model has limited economies of scale and adapts poorly. Therefore, banks are embracing chatbots or "automated personality". These can help deliver on-demand, automated help, such as dealing with frequently-asked questions; perform account services; and assist with financial requests.

QUESTIONS BOARDS SHOULD ASK WHEN EVALUATING WHETHER TO DEPLOY CHATBOTS AND VIRTUAL ASSISTANTS:

- What is the level of functionality of your chatbot? Does it make financial promotions or provide investment advice?

- What is the threshold for the provision of investment advice in the various jurisdictions where it is available? Can its functions be restricted in jurisdictions with higher compliance requirements?

- How is new text generated? Can it be checked by the compliance function to the extent required by local regulations?

- What are the current use-case expectations around which the bank will develop and tailor the chatbots and virtual assistants?

- What are the strategic fundamentals, such as goals, users, and platforms?

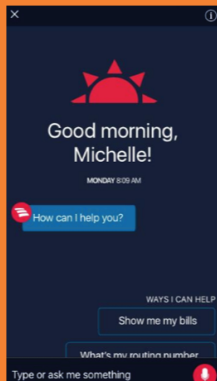- How can the chatbot or virtual assistant represent your brand and value?

AN AMERICAN MULTINATIONAL FINANCIAL INSTITUTION PROVIDING CUSTOMERS WITH AI-ENHANCED INSIGHTS THROUGH A CHATBOT

AI AS AN ENABLER

The intelligent assistant is built from scratch, based on a natural language processor and using chatlogs. It then "understands" financial services terms and the different ways that customers text about their money.

Over time, the team – of experts in algorithms, platforms, and customer-service – effectively built a rich and layered NLP architecture to power the chatbot.

HOW IT WORKS

"What's my balance?"

"What amount do I owe?"

"Yes", "yep", "Yah", "Ok"

INPUT

"Nah", "Nope", "No"

"I want to report loss for my credit card"

"um, wait, actually no"

Customer interactions as conversations (not commands)

"yds"

Natural Linguistic Programming

OUTPUT

Chatbot's learnt responses

ADDED BUSINESS VALUE

Chatbots are getting smarter and improving banking

⊕ Improved relationship-building with more convenience from enhanced conversational banking and mobile banking

⊕ Enhanced customer experience through increasingly human-like interactions and streamlined user interfaces. These reduce friction that arises from disjointed, multiple banking channels

⊕ Retained knowledge of customers, as conversational banking gets better with each customer contact. The bank builds up the ability to answer more sophisticated questions

⊕ Reduced costs combined with the maintenance and improvement of customer service levels, as business grows, and customer numbers increase

⊕ Increased job satisfaction as enhanced working practices allow former customer service personnel to focus on higher-value tasks

… A GAME-CHANGING "AUTOMATED PERSONALITY"

Bank of America's virtual assistant "Erica"

By the end of 2019, Erica is capable of understanding about 500,000 variations of questions consumers would ask. Out of the bank's 27 million active mobile users, 7 million of them have activated the chatbot. Here are some of Erica's online customer services:

Lock/Unlock debit cards

Schedule face-to-face meetings

Bill reminders; Alerts when payments are higher than expected

Credit score insights

Track spending and schedule payments

Dispute a charge

UNDERWRITING

Credit is the master of all payment methods. According to a recent survey, 77 percent of consumers preferred paying with debit or credit card, compared to only 12 percent who favoured cash.[32] Yet loans have always been a major source of credit risk. Banks have long relied on heavy historical credit data to delicately determine an applicant's credit worthiness, repayment ability, and lending risk. These factors ultimately determine their lending decisions. However, legacy credit-risk modelling using traditional data sources to facilitate lending decisions is increasingly associated with diminishing margins, an incomplete view of risks, data management issues, a loss of corporate knowledge, and slow credit decisions. Nonbank lenders, such as AI-powered fintech players, are making the financial industry ever more competitive. So, banks have an urgent need to resolve these inefficiencies and optimize their underwriting and loan-application processes.

QUESTIONS BOARDS SHOULD ASK WHEN EVALUATING WHETHER TO DEPLOY AI IN UNDERWRITING:

- What kind of alternative data does the bank use in underwriting?
- How does the bank source or collect data?
- What due diligence process has the bank put in place to evaluate third-party data providers?
- How does the bank train the data?
- Is the board fully aware of all the data points fed into the credit underwriting model?
- Are there potential biases that could need human intervention? What could be done to remove or reduce the biases?
- Who is legally responsible in the case of bias?

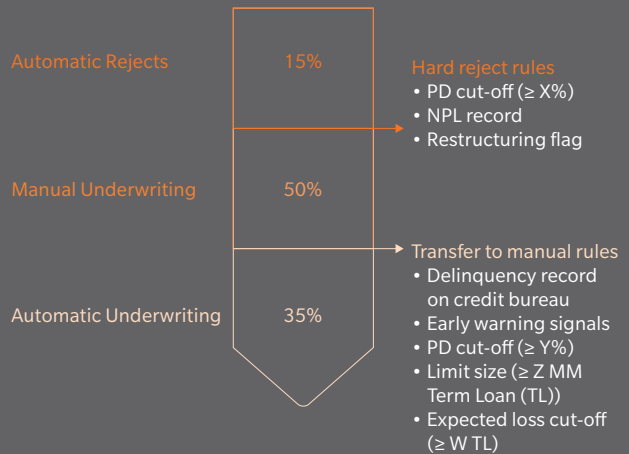# UNDERWRITING IMPROVEMENTS ARE BEING TAKEN UP BY MID-MARKET AND LARGE BANKS, AS WELL AS LARGE CORPORATIONS

AI AS AN ENABLER

AI-assisted underwriting provides a 360-degree view of an applicant. It draws together big and traditional data; social, business and internet data; and unstructured data.

- State Support
- Semantic news analysis
- Financials
- Warning signals
- Behavioral factors
- Qualitative Support
- Stock market analysis
- Group support
- Public tenders
- Railroads traffic
- Legal actions
- Owners

- Active portfolio management
- Client targeting
- Automated monitoring

- Instantaneous scoring
- Better credit decisions (Gini improvement from 6 to 21 percentage points)

HOW IT WORKS

Example: Automating 50% of Mid Market Credit Decisions

Automatic Rejects	15%
Manual Underwriting	50%
Automatic Underwriting	35%

Hard reject rules
- PD cut-off ($\geq$ X%)
- NPL record
- Restructuring flag

Transfer to manual rules
- Delinquency record on credit bureau
- Early warning signals
- PD cut-off ($\geq$ Y%)
- Limit size ($\geq$ Z MM Term Loan (TL))
- Expected loss cut-off ($\geq$ W TL)

ADDED BUSINESS VALUE

- Enhanced client experience due to a faster, more accurate approval process – at a fraction of current costs

- Improved productivity, as teams are given analytics-enhanced decision support and workers are redirected to higher-value tasks (which possibly bring greater job satisfaction)

- Improved risk control, leading to lower risk costs, through the AI- and analytics-aided techniques

- Added sources of growth thanks to new insights based on an analytical approach, some of which help to shape new business models

MEASURABLE IMPACT FOR A GLOBAL BANK IN HONG KONG...

...that reaped the benefits of AI-assisted underwriting[33]

>2 days

Reduction of the approval process time from an original 10-to-15 days

94%

Accuracy rate in credit analysis calculations

RELATIONSHIP MANAGER AUGMENTATION

Cross-selling or prospecting initiatives have been a major source of revenue growth for banks. More often than not they target existing customers, for whom the banks already have information on attributes such as financial standing, historical spending behaviour, and portfolios. However, the disconnect – and AI opportunity – lies in the ability of banks to accurately and promptly anticipate these customers' unaddressed needs. To interest customers through digital campaigns, digital marketing teams will first conduct product-level exclusions and then leverage customer relationship management (CRM) lists to find the next best product for those customers. This implies finding a logical way to group customers and audiences based on testing to find out their needs and/or wants.[34] Many customers qualify for multiple products, making it challenging for the relationship managers – while in their roles as financial advisors rather than sales personnel – to decide which products to recommend and how and when to recommend them.

**QUESTIONS BOARDS SHOULD ASK TO EVALUATE WHETHER
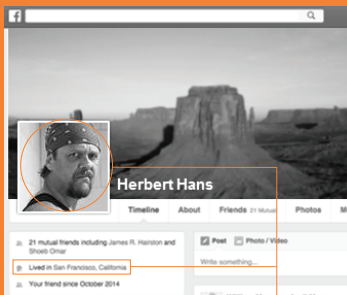TO DEPLOY RELATIONSHIP MANAGER AUGMENTATION:**

- Is there a clear understanding in each jurisdiction of when information counts as a promotion and when a promotion becomes investment advice?

- Will the technology deployed dovetail with the product governance and suitability systems the firm uses to conform to applicable regulations?

- How can the AI used by relationship managers to make cross-selling recommendations also help make client experience the central focus of the relationship?

A EUROPEAN BANK ENHANCED ITS CROSS-SELL TARGET EMAIL LIST THROUGH A SOCIAL MEDIA SEARCH

AI TECHNOLOGY AS AN ENABLER

Based on data from social media activities, AI helps to improve understanding and learning in real time. The bank can then identify patterns and make previously unnoticed connections to form new, actionable insights.

Bank records

Other **markers**, such as location and email, help further improve **match**

HOW IT WORKS

Social network data trigger		Bank offer
Client started to use smartphone		Suggest to install bank mobile app
Client changed marital status		Tell about the benefits of mortgage lending
Client bought a car		Offer car insurance
Client changed job		Send application blank for accounting department to transfer salary to your bank
Client got a big promotion		Offer settlement and cash services for clients business at your bank
Client travels/check-in abroad		Offer bonus miles credit card

ADDED BUSINESS VALUE

A deeper understanding of customers enabled more meaningful and effective engagement.

+ The bank's focus shifted from products to existing customers. It made more-personalized and better-targeted decisions on whom the relationship manager should contact and what messages to deliver

+ Improved customer experience with enhanced channel engagement. To remove friction from the customer journey, the engagements are real-time, consistent, and omnichannel

+ Enriched revenue sources with more-accurate identification of opportunities

+ Improved retention and acquisition rates thanks to prompt flagging and proactive resolution of issues

MEASURABLE RESULTS

5x
Email addresses available for cross sell activities

4x
Annual income from email cross sell

1 month
To implement the project

2 months
To recover project investments

FRAUD DETECTION

In financial year 2018-2019, a record number of complaints about banking fraud and scams were reported to the UK Financial Ombudsman Service. More than 12,000 complaints about financial fraud were logged, an increase of 40 percent on the previous year and more than double the volume received three years previously.[35] Fraud mitigation is increasingly a top priority for banks. However, traditional methods of fraud identification – such as the use of rules engines written by humans – capture only a small percentage of fraud cases and produce a significantly high percentage of false positives. The large pool of false positives required significant manpower and money to investigate what might still turn out to be dead ends. Therefore, banks are turning to AI to improve their predictions, identify a higher percentage of actual cases, and reduce false alarms. In fact, fraud detection has been identified as the most valuable application of AI in banking.[36]

According to a 2019 study[37] by the Association of Certified Fraud Examiners, the world's largest anti-fraud organisation, 13 percent of 1,000 companies have already used AI to tackle financial crime. A further 25 percent plan to do so in the coming year. Twenty-six percent currently use biometrics as part of their anti-fraud programmes, and another 16 percent expect to deploy biometrics by 2021.

Financial institutions have been early adopters of AI for fraud detection. The FinCEN Artificial Intelligence System (FAIS) was already used to predict potential money laundering in the 1990s.[38] In a survey conducted by the Bank of England and the Financial Conduct Authority in 2019, 57 percent of respondents reported that they were using AI applications for risk management and compliance, including anti-fraud and anti-money laundering applications.[39] Some regulators are attempting to use AI to detect misconduct. For example, the Australian Securities and Investments Commission is using AI to supervise equity and futures markets, and it is sponsoring research into the use of natural language processing technology to detect misconduct.[40]

Machine-learning algorithms have the potential to analyse millions of data points to detect fraudulent transactions that would likely go unnoticed by humans. They improve the precision of real-time approvals and reduce false positive results.

QUESTIONS BOARDS SHOULD ASK ABOUT THE DEPLOYMENT OF AI TO DETECT FRAUD:

- What are the estimated costs of running risk- and intelligence-based fraud detection and anti-money-laundering activities in parallel?
- Does the bank have statistics that compare the timeliness and effectiveness of both approaches?
- How does the bank tackle Type I errors (false positives) and Type II errors (false negatives) in fraud protection?
- Where does the bank source biometric data? Are its processes for handling biometric data adequate?

A LEADING SINGLE SUPERVISORY MECHANISM (SSM) BANK IS USING NEW ANALYTICS FOR NEXT-GENERATION FRAUD MODELLING

AI AS AN ENABLER

AI and machine-learning solutions can combine supervised and unsupervised machine learning to calculate a weighted score for any digital business activity in milliseconds. This can powerfully challenge any rapid instances of nuanced, sophisticated fraud attempts.

These AI-powered systems can also examine up to decades of transaction data in a 250-millisecond response rate to calculate risk scores. Their scores are up to 200 percent more predictive.

HOW IT WORKS*

1. Fraud detection and prevention based on anomalies is more common than solutions based on predictive and prescriptive analytics.

2. This type of application **trains on a continuous stream of incoming data**. The data provide a baseline picture of normal banking transactions, loan applications, and information for opening a new account.

3. The software can then **notify a human monitor of any deviations** from the normal pattern, so that they may review it.

4. The monitor can **accept or reject this alert**, which signals to the machine learning model whether or not it was correct to determine fraud from a particular transaction, application, or piece of customer information.

5. **This further trains the machine learning model to "understand"** that the deviation it found was either fraud or a new, acceptable type of deviation.

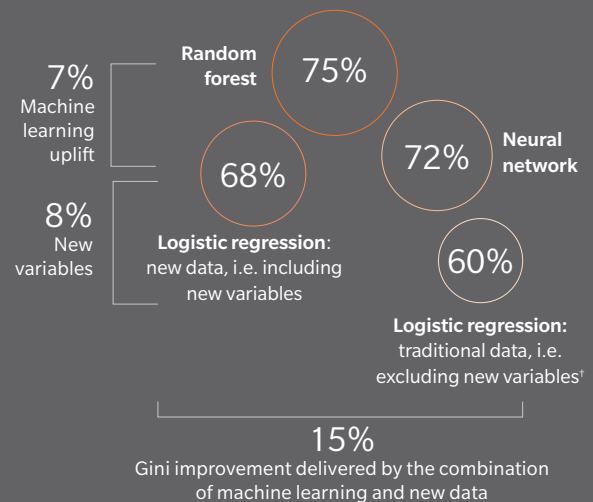*Source: Emerj, 2019. AI-Based Fraud Detection in Banking – Current Applications and Trends

ADDED BUSINESS VALUE

More accurate and timely fraud mitigation minimizing implications**

- Reduced impact from fraud compared with the previous six or eight weeks (due to enablement of real-time fraud detection)

- Improved sales and reduced fraud; risk scores accessible in real time and deeper insights available to help set threshold scores and chargeback rates

- Greater ability to filter out fraudulent activities and to thwart nuanced, sophisticated attempts at fraud, such as abuse of promotions and collusion with sales personnel

- Enhanced customer experience, as easier online approval reduces friction, and false positives for fraud are reduced

**Source: Forbes, 2019. Top 9 Ways Artificial Intelligence Prevents Fraud

MEASURABLE RESULTS FOR THE SSM BANK

7% Machine learning uplift

8% New variables

Random forest 75%

68% Logistic regression: new data, i.e. including new variables

72% Neural network

60% Logistic regression: traditional data, i.e. excluding new variables†

15% Gini improvement delivered by the combination of machine learning and new data

† Source: Oliver Wyman analysis, 2019. Logistic regression only with those variables currently used by the bank in other risk models. The Gini Coefficient is the capacity to discriminate between good and bad risks; the larger the Gini Coefficient, the better the discriminatory power of the models.

ALGORITHMIC TRADING

Financial institutions, especially hedge funds and proprietary trading houses, have been using algorithmic trading over the past decade. Benefits can include faster execution at the best prices, which will benefit the firm and clients; increased accuracy and fewer mistakes; the ability to automatically check multiple market conditions simultaneously; and fewer errors with psychological or emotional causes.[41]

LEGAL PERSPECTIVE

Algorithmic trading is a prime example of an area under increased regulatory scrutiny. One reason is a fear of the type of flash crashes seen during and after the global financial crisis; another is a desire on the part of regulators to shine light into the darker corners of the financial markets. MiFID II and related measures are examples of regulations that impose specific regulatory burdens upon firms that use algorithms, particularly for high-frequency trading. MiFID II requires investment firms authorised in the EU to notify their local regulators if they engage in algorithmic trading. Secondary legislation then imposes additional requirements on firms that engage in algorithmic trading to: (i) have clear lines of accountability within the firm for the development, deployment and update of trading algorithms; (ii) ensure that the compliance function has a general understanding of how such algorithms operate; (iii) have sufficient staff to manage and monitor their algorithmic trading systems and trading algorithms; (iv) monitor algorithmic trading activity in real time; and (v) have an emergency kill functionality that can cancel unexecuted orders immediately. Firms that pursue high-frequency trading are subject to additional requirements, including the maintenance of accurate, time-sequenced records.

RISK MANAGEMENT IN BANKS – FRAUD DETECTION AND ANTI-MONEY LAUNDERING (AML) MANAGEMENT

Banks have traditionally used a rules-based approach to manage the risks of fraud, money laundering, and sanctions. This rules-based approach is also referred to as a risk-based or risk-scoring approach: Companies undertake a formal money-laundering risk assessment and then document the risk scenarios they are exposed to based on their customers, products, and business lines. Companies submit pre-determined scenarios to the regulators for approval and the AML process must follow the approved processes. The traditional risk-based approach could be costly, as simple pre-determined scenarios could give rise to false positives or negatives. For example, if a scenario is to red flag politically exposed persons (PEPs) from a high-risk country, all PEPs from that country would be subject to further scrutiny and documentation even though there are no other transaction or activity based data that support such a risk assessment. With the help of AI, banks can run two approaches in parallel: one based on an intelligence-based approach using big data and another that uses AI's capabilities to recognise patterns. The data is usually based on transactions and also features detailed information on the customers and their business or personal activities – so each bank prefers to use its own dataset. Blockchain, a distributed ledger system that allows the anonymisation of transaction-level information, could enable banks to maintain their competitive positions and protect customer data privacy while also contributing to industry-wide efforts to combat fraud and money-laundering.

Whilst these requirements impose a significant burden, they do have the benefit of establishing a relatively clear framework in which firms can operate. In the absence of such a framework, it might be difficult for firms to interpret how other regulations should apply to them in a proportionate manner. A common concern for firms is how to interpret and adapt pre-existing regulation to new technologies. If they over-comply, they risk being at a competitive disadvantage. But if they under-comply, they risk significant sanctions from regulators or reputational damage if shortcomings are identified.

As a side point, the MiFID II provisions on algorithmic trading require significant human supervision and interaction, despite the common concern that increased use of AI and related technologies will reduce jobs.

APPLICATIONS IN INSURANCE

Insurance is a multi-faceted industry divided along traditional structural lines, which have been recently reinforced by legal and regulatory oversight. Traditionally the industry has been divided into life and non-life insurance products – a division that also applies to organisations, though some offer both kinds of product. Non-life insurance is further divided into marine and non-marine types.

The industry deals with both consumer – retail – clients and commercial clients, from the smallest self-employed individuals to the largest global conglomerates. Each area has its own practices, traditions and – often – laws, as well as differing regulatory and capital-holding requirements. This market structure, combined with a lack of investment and a complicated history of M&A activity, means that many insurers use multiple IT systems. Often, these do not cross-communicate, and older data may be on inaccessible legacy systems. A significant frictional cost comes from a number of traditional insurance market practices with heavy human resource needs.

The ability of the insurance industry to adopt and utilise new technologies such as AI has been challenged by commentators for some time. However, it has been suggested that the rise of AI could eliminate the need for most life insurance brokers and agents: According to Forbes, "the ability to source and construct life insurance portfolios, facilitate underwriting, and monitor policies can all be accomplished by the robo-life agent".[42]

CORE SUPPORT PRACTICES

Insurers have been working to automate core system interactions and augment their agents with robotic process automation – the penultimate step on the path to full AI. AI has entered the insurance industry in the form of first-tier technology, such as Allstate's chatbot, "the Allstate Business Insurance Expert", and in the form of third-tier augmented intelligence, such as Fukoku Mutual Life Insurance Co.'s 2017 replacement of 34 workers with IBM's Watson Explorer program.

Robotic Process Automation (RPA) systems, which use software to handle high-volume business processes and workflow, are being investigated by a number of insurers. They can be trained to learn specific processes, automatically handle transactions, manipulate data, trigger responses, and communicate with other systems. Davies Group implemented RPA in 2016 to enable a team of four people to process around 3,000 claims documents a day.[43] Without RPA, the team would have needed to be up to 300 percent larger, showing the extent to which these systems are moving to fill roles traditionally occupied by humans.

Likewise, Xchanging (a long-term service provider in the London-based insurance market) introduced RPA into its Insurance Market Data Repository in 2013. Within two years it had 13 automated processes in its insurance servicing business. The company said this reduced claims processing time by over 90 percent and eliminated human error, as well as facilitating 24-hour uninterrupted operation by using multi-skilled robots to work on various processes.[44]

AI has long been thought to have the potential to replace some insurance broking functions altogether. For example, it could operate via an electronic network and perform administrative functions normally carried out by insurance placement brokers. The brokers could then focus on tasks that need human judgement, continuing the evolution of insurance brokers towards the role of providing advice and analysing risk.

There is some scepticism about the ability of an AI system to fully replace an experienced broker. It is likely that for complex and nuanced insurable risks, insurance brokers will retain their traditional market making and finding role, which they will combine with a healthy overlay of analytical and risk advisory value. They are likely to continue in this role until AI systems can make nuanced decisions and replicate human interaction.

Insurers, as they implement AI, are expected to take more of a backseat role as product manufacturers. Brokers will become more important for their role in identifying customer requirements and ensuring that customers get risk transfer solutions – including insurance coverage – that fully cover their insurable exposures. Broker AI will of course help them do this. It will also be able to capture and disseminate trends and losses, thereby helping to educate customers and product manufacturers on how to avoid those risks.

CUSTOMER-FACING ACTIVITIES

Current uses of AI include chatbots to handle sales and queries in retail insurance and to identify fraudulent claims by seeking data patterns. AI can also simplify and speed up the insurance claims process, improve customer profiling, and process data in risk-rating models to provide information to insurance underwriters as they make decisions.

AI will continue to expand into new areas, where it will make human broking intermediaries and underwriters unnecessary. It will also be used to educate human decision makers on more-complex risks. But the current thinking is that AI systems such as RPA in insurance will not necessarily lead to a loss of jobs or a reduction in the size of the human workforce. The systems will instead lead to changes in responsibilities and focus for a number of roles. So RPA and other levels of AI will result primarily in an improvement in employees' ability to carry out work that only they are capable of, thanks to a reduction in the burden of administrative tasks. AI and RPA are thus expected to increase efficiency and, therefore, client satisfaction. The training and retraining of staff will be key to managing the transition.

The insurance market sees AI technology as mature, and is focusing on usage options that increase productivity, improve customer service, and detect fraud more effectively. AI will also help to monitor sanctions controls and anti-money laundering controls, as well as to simplify the processing of claims.

RISKS OF AI IN INSURANCE

There is a growing belief that the insurers with the best data will win in market competition, making the quality of data a more important factor even than bias in their input, in algorithms, or in the way insurers use data. That means, of course, that data should be the best available – fair, explainable, robust, and stored in a good system. However, if data are not accessible, they are useless.

Many insurers have enormous amounts of valuable data in numerous systems, some of which are legacy systems. But they were often not recorded in an easily-interrogable form with consideration for future use. So many data are not readily accessible. Other major concerns include data corruption, which can be accidental, malevolent (as when done by a disgruntled employee), or intentional (done by a third party). The impact of a product based on corrupted data will be multiplied by the number of customer sales.

The common view within commercial insurance around AI sees insurers talking about "intelligence without cognition" and observing that AI will augment humans, rather than replace them. This indicates a view that AI-based systems will better inform underwriters and claims decision makers over commercial insurance risks, but not replace them.

Other concerns include the lack of understanding by leadership of how to use AI properly. In addition, it is difficult to understand the investment returns. The regulatory regime is unclear, changing, and – especially across borders – conflicting. And expectations may be unduly high for the effectiveness of AI and the error rate. Under the Senior Managers & Certification Regime in the UK, the organisation's digital strategy and risk framework need to be within a Statement of Responsibility signed by one or more individuals. Those individuals need to understand the technology and its associated risks, and their board must give them the access and resources to properly identify, assess, mitigate, and monitor the risks, as they will be held accountable under the regime.

QUESTIONS FOR THE BOARD ABOUT THE DEPLOYMENT OF AI IN INSURANCE:

A number of the questions that boards should consider are similar to those listed in the section on banking, so these should be asked, as well as the following:

- Has the right opportunity been identified? Does the solution really improve things? Can it be monetised?
- Does big-data analysis for sales and pricing create the risk of an uninsured or uninsurable class of buyer? If so, what might be the reputational and regulatory response?
- Does the board have sufficient knowledge, experience, and understanding to risk manage the entire process?
- Is the data set accurate and held securely? Is it being managed properly? Has it been trained correctly? Has the potential for bias in the data or the algorithms been fully understood, managed, and protected against?
- When using third-party providers, is the liability clearly understood, defined, and managed?
- Are we employing, identifying, (re)training, and continually developing the right staff with the right skillsets?
- At the underwriting stage, how will the use of tools such as big data, web crawling, and customer profiling impact the insurer's knowledge (e.g. in the UK, under the Insurance Act 2015)?

INSURANCE – THE FUTURE

It is expected that insurers' AI will be able to remotely interrogate the AI systems of a proposed insured, and utilise the vast amount of data the Internet of Things will capture. These data, combined with connected systems, will enable better designed, better priced, and better performing insurance products. Insurance based on usage, such as mileage or occupancy, will become mainstream Insurers have been steadily increasing their data utilisation to help avoid the impact of events on their customers. In future, AI may be able to move the insurance industry from a detect-and-repair approach to a predict-and-prevent one.

HIRING

Banks and insurance companies globally increasingly use AI to screen job applicants and chatbots to conduct online interviews. These categorise potential employees into character buckets so as to optimise training effects for the AI systems through customised development programmes. Some companies, such as Ping An, develop their own AI tools. Others outsource it to third-party vendors such as HireVue. Its algorithm assesses candidates' performance based on 15,000 different traits, including eye movements, body language, speech patterns, and blinking.

Advocates of AI in recruitment claim that AI reduces the cost of human workers and minimises the potential effects of human bias and intuition. HireVue said that its solutions reduce time searching for the right candidates by 90 percent on average.[45] At Ping An's interim results announcement in 2019, co-CEO Jessica Tan talked about the benefits of its AI-powered technology in recruitment, including the number of hours saved by AI-based interviews.

However, one potential unintended consequence is discrimination against groups of people, if there is inherent bias in the input data. In a case cited by James Proudman, Executive Director of UK Deposit Takers Supervision, a major technology company discovered that its AI-empowered experimental hiring tool preferred male to female candidates. That might have been related to the training of its AI models, which was based on resumes submitted over a 10-year period, mostly from men.

QUESTIONS THE BOARD SHOULD ASK ABOUT AI DEPLOYMENT IN HIRING:

- At what stage should hiring algorithms be brought into the recruiting process – screening, interviews, or selection?
- How does the company define and measure the success of AI deployment in hiring?
- Has the company developed a proprietary AI model? Or does it source models from third parties?
- If third-party models are used, what due diligence process has been put in place or been planned?
- How does the company establish relevant data sources and candidate profiling characteristics?
- How does the company clean data if multiple input sources are used?
- If the company uses historical data that may exacerbate discrimination in the hiring process, how does it assess and attempt to correct for data bias, such as over gender and ethnicity?
- As part of algorithm-led hiring, what temptations should be avoided and noted in respect of candidates' privacy? (This could include things like lifestyle, private activities, disabilities, and personal attributes.)
- How often does the company renew or update its recruitment analytics?

REGULATORS AND AI IN FINANCIAL SERVICES

Perhaps surprisingly, there has to date been little in the way of dedicated regulation for the use of AI in financial services. That is not to say that no regulations apply. As discussed in other sections of this paper, data privacy legislation such as the EU GDPR has a considerable impact. And equalities laws mean it is necessary to iron out any learned biases in AI systems. But how do financial regulators view AI?

One challenge for the development and use of AI in financial services is to understand the extent to which regulation applies. Some regulators, such as the UK's FCA, describe themselves as technology agnostic: They regulate in order to improve the industry and protect consumers irrespective of technology or means of delivery. So pre-existing regulation applies to AI as it does to any other product, service, or technology used in a regulated business. In practice this means that firms must carefully consider what technology they are using and how, and then assess how regulations will apply to it.

The first step towards using AI in a financial services business is to consider whether the technology will carry out activities that are regulated in the jurisdiction in question. For example, a chatbot may simply guide users round a website or answer direct questions. But at what point is the chatbot considered to be promoting financial products? When will its responses be viewed as investment advice? Will these points be reached at different stages of activity in different jurisdictions? Similarly, though anti-money-laundering and know-your-customer checks may not necessarily be regulated services, regulators will nonetheless require a firm using AI in these activities to comply with its general obligations for the processes. A further layer of complexity may arise when technology is used or made available in different jurisdictions. This is of course an issue for financial services firms operating on a global basis irrespective of their use of technology. However, the potentially 'closed' nature of AI can cause additional risks, as can the possible inability of local compliance and legal teams to understand the AI being used.

The next step is to consider what regulation does apply. As indicated above, even where a regulatory body purports to be technologically neutral, it may have provided guidance referencing particular technologies. For example, the European Securities and Markets Authority (ESMA), the EU regulatory authority, has produced guidance for firms giving investment advice and providing portfolio management services. This guidance specifically includes additional steps that firms should take when using robo-advisers to advise retail investors in the EU.[46] ESMA reminds firms to have appropriate systems and controls in place to ensure that suitability assessment tools that perform tasks such as risk-profiling are fit for purpose and provide satisfactory results. Similarly, ESMA recommends that firms regularly test algorithms that underpin the suitability of the transactions they recommend and the

trading decisions they take for portfolios. It also recommends that firms have policies in place for managing changes to the algorithms.

This in many ways encapsulates the approach that regulators take to AI and other technological advances. Whilst there is little regulation directed specifically at these new types of technology, regulators expect firms to consider their use holistically within the compliance framework. They also expect the same level of testing and reporting as for any other product line or means of delivery. Similarly, regulators expect firms to continue to comply with their general duties of care and professionalism. They can be expected to look unfavourably on any attempts to use technology to pursue anti-competitive practices or to mislead consumers.

To enforce and uphold their rulebooks, regulators can use existing rules on outsourcing, customer care, and integrity to examine the manner in which technology is being deployed and its results monitored. The FCA's fine of an insurer for overreliance on voice analytics is one such example of the application of existing rules and behavioural expectations to new technologies that are not the subject of specific regulation. (See Executive Summary.) That investigation demonstrated the need for firms employing third-party technology providers to fully understand what they are signing up for, so that they can monitor their compliance.

ETHICS AND AI IN FINANCIAL SERVICES

Against the existing regulatory (compliance) landscape, including cybersecurity and data privacy considerations, financial services industry should also note that the responsible implementation of AI has been a growing topic of discussion in various key stakeholder groups. The OECD has adopted AI guidelines[48] the G20 has human-centred AI principles[49] the EU has Ethics Guidelines for Trustworthy AI[50] and Singapore has its Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT)[51] and Personal Data Protection Commission (PDPC) framework for AI.[52] In fact, global momentum has gathered over the last 12 months for the development of principles for responsible and ethical AI. The practical ramifications are illuminated by these guidelines with shared focus across four pillars: transparency, accountability, fairness and ethics.

In a leading move towards translating principles to practice, Singapore's central bank has worked with 16 other financial services players to create an AI ethics framework, Veritas.[53] This enables financial services to evaluate AI and data-analytics-driven solutions and can provide a baseline to strengthen internal governance of AI applications and the use and management of data. To secure trust in the digital age and maximise the opportunities presented by AI, financial services providers must integrate ethical considerations into their AI deployment and development.

Financial services have taken steps to ensure they are responsibly introducing AI applications. Bank of America, for example, has founded The Council on the Responsible Use of Artificial Intelligence with Harvard University to study the ethics and consequences of AI. Wells Fargo has entered a multi-year agreement with IBM to ensure its AI and quantum computing capabilities are not just fast and convenient, but also safe.[54] Great strides have been made, but challenges lie ahead.

The technology-agnostic approach may not last forever. In the UK, the FCA has started warning that it may take action if technological advances lead to poor behaviour by firms. "As the market in data grows and new challenges arise as a result of the wider application of machine learning, some market players will have greater access to data and technological ability," the FCA said in its Business Plan for 2019/2020. "This may lead to behaviours that are not always in the interest of competition."[47] Christopher Woolard, Executive Director of Strategy and Competition at the FCA, gave a starker warning in a speech: "As regulators, we [already] have a range of powers and tools to tackle these issues now, but as we see greater and greater use of technology, those tools may need to be updated for a fully digital age." Furthermore, we are already seeing some regulation directed specifically at the use of technology by investment firms. For instance, MiFID II includes specific provisions regulating the use of algorithmic trading. (This was discussed on pages 25 and 26, in the section Algorithmic Trading.)

The commentary from the FCA is in line with moves in other areas of the financial services industry. When the FCA perceives poor practice, it will initially seek to encourage better behaviour through generic, principles-based pre-existing regulations. If it considers that poor behaviour is continuing, it may start to pursue enforcement action against individual firms. But if such actions do not sufficiently change behaviour, the FCA will seek to impose additional requirements on firms, thus bringing a wider range of activities within the regulatory net. It is likely that other regulators will follow a similar trajectory.

CONCLUSION

Though not all firms are ready, artificial intelligence is a growing business priority in the financial services industry – in asset management, banking, insurance, and other fields. The sector broadly recognises the strategic nature of AI, and players are already making large investments and channelling substantial resources into the space in order to keep up with – or get ahead of – the competition.

This paper has presented a multi-stakeholder perspective to help business leaders navigate the complexities of AI adoption and prioritise oversight from when they start to use it. While there are many ways to use AI, the sector needs to uncover what the technology truly means in business terms. To distinguish the reality from the hype, business leaders need to question and evaluate their objectives and examine the value of their AI deployment beyond the technology. The use of AI is changing fast and still evolving, with clear merits but also unexpected challenges. That makes it imperative for leaders to develop a clear understanding of the technology and to establish a clear and responsible path for successfully integrating AI into their business models and broader strategic objectives.

BIBLIOGRAPHY

1. Hermes, BCLP (2019). Investors' Expectations on Responsible AI and Data Governance. Retrieved from https://www.hermes-investment.com/wp-content/uploads/2019/04/investors%E2%80%99-expectations-on-responsible-artificial-intelligence-and-data-governance.pdf

2. The Guardian (2016). Admiral to price car insurance based on Facebook posts. Retrieved from https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts

3. The Guardian (2016). Facebook forces Admiral to pull plan to price car insurance based on posts. Retrieved from https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data

4. Financial Conduct Authority (2018). The FCA has fined Liberty Mutual Insurance Europe SE £5.2 million for failures in its oversight of mobile phone insurance claims and complaints handling. Retrieved from https://www.fca.org.uk/news/press-releases/liberty-mutual-insurance-europe-se-fined

5. Hermes, BCLP (2019). Investors' Expectations on Responsible AI and Data Governance. Retrieved from https://www.hermes-investment.com/wp-content/uploads/2019/04/investors%E2%80%99-expectations-on-responsible-artificial-intelligence-and-data-governance.pdf

6. Financial Reporting Council (2011). Boards and Risk. Retrieved from https://www.frc.org.uk/getattachment/b88db2b6-af08-4a0e-9755-ab92de1268c2/Boards-and-Risk-final-Sept-2011.pdf

7. Financial Reporting Council (2018). The UK Corporate Governance Code 2018. Retrieved from https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UKCorporate-Governance-Code-FINAL.pdf

8. Parliament UK (2019). Government flagship digital identification system failing its users. Retrieved from https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/news-parliament-2017/accessing-public-services-through-verify-report-published-17-19/

9. TechCrunch (2019). Demanding privacy, and establishing trust, in digital health. Retrieved from https://techcrunch.com/2019/03/26/demanding-privacy-and-establishing-trust-in-digital-health/

10. The Medium (2018). Data Brokers Have Access to Your Health Information, Do You? Retrieved from https://medium.com/@patientory/data-brokers-have-access-to-your-health-information-do-you-562b0584e17e

11. H. Ernst & N. Omland (2011). The Patent Asset Index – A new approach to benchmark patent portfolios World Patent Information 33(1): 34-41

12. The Patent Asset Index represents the strength of corporate patent portfolios, accounting for ownership, legal status, and portfolio sizes. It is defined as the sum of the competitive impact of all patents in the corporate portfolios, where competitive impact is the combined effect of two additional indicators, technology relevance, and market coverage. Technology relevance measures the number of citations received, corrected for patent ages and citation propensities in different technology fields and patent offices. The market coverage of patents measures the global market size that is protected. Apple, Microsoft and Sony were the original players in this field. However, other players have been growing and even overtaking, notably Samsung since around 2012 and Magic Leap and OPPO since 2016

13. FIS (2018). Readiness Report 2018: The Pursuit of Growth across Asset Management. Retrieved from https://www.fisglobal.com/-/media/fisglobal/files/pdf/report/the-readiness-report-2018-the-pursuit-of-growth.pdf

14. The Medium (2019). Controversial weapons, Primark-owner offers a sweetener, and AI in investment management. Retrieved from https://medium.com/@genuineimpact/controversial-weapons-primark-owner-offers-a-sweetener-and-ai-in-investment-management-d1e80997ef4d

15. Financial Times (2019). AI and climate change transform investment sector. Retrieved from https://www.ft.com/content/fa8885f6-ad69-3dd0-a437-6aeb23c753ad

16. Hedgeweek (2018). Can machine learning tools improve portfolio risk management...? Retrieved from https://www.hedgeweek.com/2018/11/28/270954/can-machine-learning-tools-improve-portfolio-risk-management%E2%80%A6

17. Tail risk is the additional risk of an asset or portfolio of assets moving more than 3 standard deviations from its current price, above the risk of a normal distribution

18. RiskNet (2019). Can robots learn to manage risk? Retrieved from https://www.risk.net/our-take/6810536/can-robots-learn-to-manage-risk

19. Wikipedia (2019). Value at risk. Retrieved from https://en.wikipedia.org/wiki/Value_at_risk

20. Citi (2019). Citi Global Data Insights: The Rise of AI in ESG Evaluation

21. DigFin (2019). ESG now a third of MioTech's A.I. business. Retrieved from https://www.digfingroup.com/esg-ai/

22. Sentiment analysis is the process of computationally identifying and categorising opinions expressed in a piece of text, especially in order to determine whether the writer's attitude towards a particular topic, product, etc. is positive, negative, or neutral

23. Bloomberg (2016). Warren Buffett: Smartphone Is Too Smart for Me. Retrieved from https://www.bloomberg.com/news/videos/2016-11-02/warren-buffett-smartphone-is-too-smart-for-me

24. World Economic Forum (2019). Navigating Uncharted Waters: A roadmap to responsible innovation with AI in financial services. Retrieved from https://www.weforum.org/reports/navigating-uncharted-waters-a-roadmap-to-responsibleinnovation-with-ai-in-financial-services

25. Aquantix. Retrieved from https://www.aquantix.ai/

26. Hermes (2019). Stewardship. Retrieved from https://www.hermes-investment.com/ukw/insight/stewardship/stewardship-the-2020-vision/

27. BBC (2019). Google admits error over hidden microphone. Retrieved from https://www.bbc.com/news/technology-47303077

28. The Guardian (2019). 'Alexa, are you invading my privacy?' – the dark side of our voice assistants. Retrieved from https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

29. Hermes (2019). AI: brave new worlds. Retrieved from https://www.hermes-investment.com/ukw/insight/outcomes/aibrave-new-worlds/

30. Amazon (2019). Notice of 2019 Annual Meeting of Shareholders. Retrieved from https://ir.aboutamazon.com/static-files/35fa4e12-78bd-40bc-a700-59eea3dbd23b

31. The Financial Brand (2018). Artificial Intelligence and The Banking Industry's $1 Trillion Opportunity. Retrieved from https://thefinancialbrand.com/72653/artificial-intelligence-trends-banking-industry/

32. Jason Steele (2019). Payment method statistics. Retrieved from https://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php

33. South China Morning Post (2019). Citi turns to AI for the early work in approval of corporate loans – and choose Hong Kong for first testing. Retrieved from https://www.scmp.com/business/banking-finance/article/2186508/citi-turns-ai-early-work-approval-corporate-loans-and

34. The Financial Brand (2019). 5 Tips For Financial Marketers to Tap AI's Personalization Potential Retrieved from https://thefinancialbrand.com/80693/tips-financial-marketing-artificial-intelligence/ ; 4 Ways Bank Brands Can Supercharge Their CRM-Driven Digital Marketing. Retrieved from https://thefinancialbrand.com/84329/bank-brands-crm-digital-marketing-addressable/

35. The Financial Brand (2019). 5 Tips For Financial Marketers to Tap AI's Personalization Potential Retrieved from https://thefinancialbrand.com/80693/tips-financial-marketing-artificial-intelligence/ ; 4 Ways Bank Brands Can Supercharge Their CRM-Driven Digital Marketing. Retrieved from https://thefinancialbrand.com/84329/bank-brands-crm-digital-marketing-addressable/

36. Celent (2017). Understanding the investment into AI in Banking. Retrieved from https://www.celent.com/insights/776416737

37. Association of Certified Fraud Examiners (2019). Study: AI for fraud detection to triple by 2021. Retrieved from https://www.acfe.com/press-release.aspx?id=4295006598

38. T. Senator, H. Goldberg, J. Wooton, M. Cottini, A. F. Umar Khan, C. Klinger, W. Llamas, M. Marrone & R. Wong (1995). The FinCEN Artificial Intelligence System: Identifying Potential Money Laundering from Reports of Large Cash Transactions

39. Bank of England (2019). Managing machines: the governance of artificial intelligence - speech by James Proudman. Retrieved from https://www.bankofengland.co.uk/speech/2019/james-proudman-speech-at-fca-conference-on-governance-in-banking-london

40. Financial Times (2019). Australian regulators cautiously embrace AI to boost compliance. Retrieved from https://www.ft.com/content/33eb5934-4519-11e9-b168-96a37d002cd3

41. The Alan Turing Institute (2019). Artificial intelligence in finance. Retrieved from https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_1.pdf

42. Forbes (2015). How Artificial Intelligence Will Eliminate The Need For The Vast Majority Of Life Insurance Agents. Retrieved from https://www.forbes.com/sites/russalanprince/2015/04/12/how-artificial-intelligence-will-eliminate-the-need-for-the-vast-majority-of-life-insurance-agents/#173f73c149d7

43. Ninety Consulting (2016). The Rise of the Robo-insurer. Retrieved from https://www.the-digital-insurer.com/wp-content/uploads/2016/05/731-ninety-consultingwhite-paperthe-rise-of-the-robo-insurer-160329133010.pdf

44. Ninety Consulting (2016). The Rise of the Robo-insurer. Retrieved from https://www.the-digital-insurer.com/wp-content/uploads/2016/05/731-ninety-consultingwhite-paperthe-rise-of-the-robo-insurer-160329133010.pdf

45. PR Newswire (2019). HireVue to Receive Growth Investment from New Majority Investor The Carlyle Group. Retrieved from https://www.prnewswire.com/news-releases/hirevue-to-receive-growth-investment-from-new-majority-investor-the-carlyle-group-300910307.html

46. European Securities and Markets Authority (2018). Guidelines on certain aspects of the MiFID II suitability requirements. Retrieved from https://www.esma.europa.eu/system/files_force/library/esma35-43-1163_guidelines_on_certain_aspects_of_mifid_ii_suitability_requirements_0.pdf?download=1

47. Financial Conduct Authority (2019). Business Plan 2019/20. Retrieved from https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf

48. OECD (2019). The OECD AI Principles. Retrieved from https://www.oecd.org/going-digital/ai/principles/

49. G20 (2019). G20 Ministerial Statement on Trade and Digital Economy. Retrieved from https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf

50. European Commission (2019). Ethics guidelines for trustworthy AI. Retrieved from https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

51. Monetary Authority of Singapore (2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. Retrieved from https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

52. Personal Data Protection Commission Singapore (2019). A proposed model AI governance framework. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/A-Proposed-Model-AI-Governance-Framework-January-2019.pdf

53. Monetary Authority of Singapore (2019). MAS Partners Financial Industry to Create Framework for Responsible Use of AI. Retrieved from https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai

54. IBS Intelligence (2019). Wells Fargo: 200,000 jobs to go in US banking in the next decade. Retrieved from https://ibsintelligence.com/ibs-journal/ibs-news/wells-fargo-200000-jobs-to-go-in-us-banking-in-the-next-decade/

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

ASIA PACIFIC
+65 6510 9700

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

www.oliverwyman.com

OLIVER WYMAN