AInsights

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Simon Toms
Partner / London
44.20.7519.7085
simon.toms@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Joseph A. Kamyar
European Counsel / London
44.20.7519.7325
joseph.kamyar@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services

Following the declaration of the international artificial intelligence (AI) "Safety Summit" at Bletchley Park (Bletchley Summit) on November 1, 2023, and the White House's October 30, 2023, Executive Order on AI (Executive Order), eyes are firmly fixed on the risks and threats posed by the increasing development and use of AI.

In this article, we look at measures being taken and considered by governments and regulators in the U.S., U.K. and EU to protect the financial services sector and its customers, and the chief concerns driving those:

- The reliability and potential biases in data sources.

- The risks of financial models.

- Governance as it pertains to the use of AI.

- Consumer protection.

The declaration issued by attendees of the Bletchley Summit (which included the U.S., the U.K., the European Union, Brazil, China, Japan and India) sets out an overarching commitment to the design, development, deployment and use of AI in a manner that is safe, human-centric, trustworthy and responsible.

That echoed the Executive Order, entitled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which specifically calls out financial services, and requires the U.S. Treasury to issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks within 150 days of the Executive Order.

Meanwhile, the E.U. is leading the way in regulating AI, reaching a political agreement on December 9, 2023, on the EU AI Act, which is now subject to formal approval by the European Parliament and the European Council. The EU AI Act will establish a consumer protection-driven approach through a risk-based classification of AI technologies as well as regulating AI more broadly.

What Use Cases Are There for AI in the Financial Services Sector?

AI is being used across a range of functions within financial services firms, including:

- Anti-money laundering activities.

- Credit and regulatory capital modelling.

- Insurance claims management.

How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services

- Product pricing.
- Order routing and execution of trades.
- Cybersecurity.

Responses to a Bank of England and U.K. Financial Conduct Authority survey in 2022 indicated that 79% of machine learning applications used by U.K. financial services firms had been deployed across respondents' businesses (having already passed through proof-of-concept/pilot phases), with 14% of those applications reported to be critical to the business area.

In short, we are seeing broad use cases for AI technologies, and the implementation of those technologies is now reaching an advanced stage for many financial service providers. Moreover, the complexity of these technologies is causing many financial services firms to rely on third-party providers to support the implementation of these applications.

How Have Governments and Regulators Reacted to the Use of AI in Financial Services?

In general, while we are yet to see a proactive statutory response to AI specifically targeted at the financial services sector, regulators have emphasized the relevance of existing regulations to AI and issued important guidance impacting financial services firms' use of AI.

United States

In the U.S., various past and forthcoming agency guidance and regulations are relevant to financial services firms, including:

- As noted above, the U.S. Treasury's best practice report for financial institutions is due by March 28, 2024.

- The Executive Order included instructions to the Consumer Financial Protection Bureau (CFPB) and Federal Housing Finance Agency (FHFA) to require the entities they regulate to use AI tools to ensure compliance with federal law, evaluate underwriting models for bias against protected groups, and evaluate automated collateral-valuation and appraisal processes to minimize bias.

- The Executive Order set out an expectation that regulatory agencies will use their authority to protect American consumers from fraud, discrimination and threats to privacy, and to address risks to financial stability. Agencies are asked to clarify where existing regulations or guidance apply to AI.

- The Executive Order specifically cites vendor due diligence (such as described in the June 2023 Interagency Guidance on Third-Party Relationships: Risk Management, issued by

the Federal Reserve Board (FRB), Federal Deposit Insurance Corporate (FDIC) and the Office of the Comptroller of the Currency (OCC)) and requirements and expectations relating to transparency and explainability of AI models (such as the OCC's Handbook, Model Risk Management, which calls on examiners to assess explainability if a bank uses AI models in its risk assessment rating methodology).

- The CFPB issued guidance regarding financial institutions' use of AI in denying credit, noting obligations under the Equal Credit Opportunity Act and Regulation B to provide specific and accurate statements of reasons to applicants against whom an adverse action is taken.

- Six federal agencies (FRB, OCC, FDIC, CFPB, FHFA and National Credit Union Association) teamed up in proposing a rule implementing quality control standards for automated real estate valuation models used by mortgage originators and secondary market issuers for valuing collateral.

- The CFPB, Department of Justice, Federal Trade Commission (FTC) and Equal Employment Opportunity Commission issued a joint statement on enforcement efforts against discrimination and bias in automated systems, noting that automated systems may contribute to unlawful discrimination or otherwise violate federal law.

- The SEC has proposed a rule requiring broker-dealers and investment advisers to take steps to avoid conflicts of interest arising from the use of predictive data analytics and similar technologies.

State and local laws in other domains, such as privacy and employment law, are also relevant to the use of AI in the financial services sector.

- The California Consumer Privacy Act gives residents the right to opt out of the use of their personal information by automated decision-making technology (even that which facilitates human decision-making) and requires pre-use disclosure of "meaningful information about the logic involved in such decision-making processes."

- Colorado and Virginia state privacy laws grant residents the right to opt out of "profiling in furtherance of decisions that produce legal or similarly significant effects."

- Connecticut's privacy law provides a right to opt out of the use of automated decision-making where decisions are "solely automated."

- New York City Local Law 144 of 2021 requires that the use of automated employment decision tools be subject to annual independent audits for bias on prohibited grounds.

How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services

- Illinois enacted the Artificial Intelligence Video Interview Act in 2022, which imposes certain requirements on employers that use AI to analyze video interviews.
- California, New Jersey, New York, Vermont and Washington, D.C., have also proposed legislation to regulate AI use in hiring and promotion.

United Kingdom

The U.K. government has set out its vision for a "pro-innovation approach to AI regulation" in a policy paper on AI regulation that was updated on August 3, 2023, stating that it does not intend to put its principles-based framework on a statutory footing initially, but is instead expecting a regulator-led, sector-specific approach.

While both the U.K. Prudential Regulation Authority and Financial Conduct Authority have been leading discussions on AI and machine learning, to date they have been focussed on information-gathering and reporting on industry feedback, as opposed to issuing any concrete regulatory guidance on the use of AI.

European Union

For financial services firms with operations in the EU, the EU AI Act will be effective from Spring 2024 and will govern the development, deployment and oversight of AI technologies.

The scope of AI technologies encompassed by the EU AI Act has not been finalized, but if adopted in its current form, the EU AI Act will classify products as either presenting unacceptable risk to individuals (such as social scoring), high-risk to individuals (such as through the use of AI systems in hiring processes or employee ratings) and low-risk to individuals (such as AI chat bots). The latest draft retains a filter-based approach that allows AI systems meeting certain exemption conditions to avoid "high-risk" classification.

While the EU AI Act is not limited to the financial services sector, it will clearly impact technologies being used and considered in the sector, and is distinct from the regulator-led approaches in the U.S. and U.K.

In addition, amendments to the EU Product Liability Directive and a new AI Liability Directive in the EU clarify consumers' ability to seek redress for product liability arising from defective or harmful AI products. The Network and Information Security Directive (NIS2) and the proposed EU Cyber Resilience Act are expected to complement the EU AI Act by setting cybersecurity standards for high-risk AI systems.

Alongside AI-specific regulation, the use of AI will also need to be considered in the context of the broader EU cybersecurity regulatory framework, such as the EU Digital Operational Resilience Act (Regulation (EU) 2022/2554) (DORA). DORA, which takes effect on January 17, 2025, focuses on the operational resilience of the financial sector and is designed to ensure that financial entities operating within the EU and their service providers can effectively mitigate information and communication technology (ICT) risks, including those presented by the use of AI. DORA also establishes significant reporting requirements in the event that a financial entity experiences an ICT-related incident, which can extend to those that implicate AI technologies.

Under DORA, financial entities must be prepared to monitor, manage, log, classify and report ICT-related incidents and, depending on the severity of the incident, make reports to both regulators and affected clients and partners.

Key Areas of Concern

While there are clear use cases and benefits flowing from the adoption of AI, regulators have shone a light on the key risks they see posed by such technology. See, for instance, the final report of Bank of England's Artificial Intelligence Public-Private Forum in 2022. Major concerns include:

Data Sources

AI processes significant volumes of data in the inputs for the AI technologies (user prompts and training data), the technology itself and its outputs. The input data may be sourced internally or from third-party providers and so the quality and provenance of any data used by AI technologies is key to managing its effectiveness and risks presented by the deployment of the technology.

Regulators are pointing to the complexity of data sources used in AI and the need to ensure financial services firms have robust governance and documentation in place to ensure data quality and provenance is appropriately monitored.

The protection of personal data is key at each stage of an AI technology's lifecycle and subject to applicable data protection regimes. For example, financial services firms operating in the U.K. and EU are required to implement the following:

1. **Clear documentation:** The use of individuals' personal data, including data sources, types of data (including special category data, such as race, ethnicity or health data), the purpose and lawful basis for processing, and how the data is stored must be clearly documented. Financial services firms should review the way in which they train

their AI technology in the input stage, often acquiring third-party data sets, extracting the data online through web scrapping, or by relying on user prompts.

2. **Transparent processing:** Financial services firms are required to give individuals prior notice in clear and easily accessible language of how their personal data will be processed and for what purpose. Additionally, financial services firms need to ensure that they can adequately address rights requests from data subjects in the context of AI (*e.g.*, access, correction, erasure, rectification, portability).

3. **Security safeguards:** From the earliest stages of AI technology development, financial services firms should implement technical and organizational measures to safeguard the security of the relevant personal data (*e.g.*, anonymization, pseudonymization, encryption, privacy-enhancing tools, contractual data processing agreements with third parties).

Model Risk

Financial institutions have used financial models to assist in economic and financial decision-making long before the introduction of AI, and the risks associated with their use are not unique to AI. But regulators have noted that AI models may amplify existing risks, driven in particular by the increased complexity of financial modelling and the challenges in explaining the inner workings of AI models. "Modellers must justify why the benefits gained are worth the trade-offs in the comprehensibility of the model. The extent to which a black box could be acceptable in supervisory terms is also dependent on how the model concerned is treated in the bank's risk management," the German regulator, BaFin, has stated.

Consequently there is the expectation that financial service providers can explain model outputs as well as identify and manage changes in AI models performance and behavior.

Governance

Robust governance is seen as a necessary pillar in the safe adoption of AI in the financial services sector. A real challenge is AI's capacity for autonomous decision-making, which limits its dependency on human oversight and judgment. While existing governance frameworks (*e.g.*, data governance, model risk management and operational risk management) will apply to the use of AI in financial institutions, firms will also need to consider existing governance frameworks to ensure that any novel challenges of AI are adequately addressed.

Financial services firms with operations in the EU will need to consider the requirements under both the EU AI Act and DORA. The regulations make it clear that governance is an ongoing

workstream. For example, DORA requires continuous monitoring and control of the security and functioning of ICT systems, with ultimate responsibility and accountability for compliance placed on the financial services firm's management body.

Examples of governance considerations include:

- Formalizing AI-specific procedures.
- Ethical considerations in the use of AI.
- Promoting a safe environment in which to test and promote innovation through AI.
- Continuous monitoring of AI implementation and outputs.
- Ensuring that legal compliance mechanisms are in place.
- Addressing skills gaps among an institution's workforce.
- Allocating responsibilities for the use and development of AI within an organization.

Consumer Protection

AI models track patterns and relationships, including consumer characteristics, and so the risk of bias is inherent in their use. Those biases may take various forms, such as reducing the availability of products to particular consumer groups, discriminatory product pricing and the exploitation of vulnerable groups.

The Executive Order and guidance from several U.S. agencies specifically cite the need for regulators to protect consumers from discrimination, and the state of Colorado has introduced legislation to require insurers to test algorithms, models and sources of information to eliminate unfair discrimination of protected classes.

The Next Step for Governments and Regulators

Regulators continue to report on and gather information and industry insights on AI in order to shape their supervisory approach. For example, the Bank of England and the U.K. Financial Conduct Authority recently published a summary of industry responses to their discussion paper (Feedback Statement) on AI and machine learning. What does this tell us so far?

More Guidance, Not More Rules

Regulators are seeing demand for more guidance, including in relation to:

i. Risk-based approaches to be adopted by firms.

ii. The application of bias/fairness requirements in practice.

iii. The use of third-party vendors.

iv. Data protection and cybersecurity.

How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services

While many governments may not currently be proposing statutory frameworks for the use of AI in financial services or otherwise, there are calls for a "stocktake" of existing legislation and regulation to better understand how existing regimes apply to AI (*e.g.*, existing equality and data protection laws).

This approach is being mirrored in government policy, for example in the U.K., where the government is focussed on a principles-based framework, which is considered to be more adaptable to the rapidly evolving nature of AI.

A Harmonized Approach

Governments are under pressure from the financial industry to adopt a harmonized approach internationally. The multinational spread of financial institutions and extra-territoriality of new regimes, such as the EU AI Act, are increasing calls for legislators to regulate AI consistently.

It is hoped that greater international cooperation and information-sharing will also help to reduce barriers and promote greater innovation in the field of AI. Whether a uniform global response to AI is achievable in the face of competing pressure to protect domestic industries from foreign competition is yet to be seen.

Time To Revisit Data Protection and Cybersecurity Laws?

The U.K. Feedback Paper asserts that some aspects of the U.K. GDPR are incompatible with the use of AI technologies (*e.g.*, the right to erasure), which raises a question of whether data protection laws more generally need to be updated to take account of AI.

In Europe, the European Commission has made clear that the incoming EU AI Act complements existing data protection laws and there are no plans to make any revisions to revise them.

Regulatory guidance is starting to emerge, with the French data protection authority (CNIL) recently publishing "AI How-to" sheets providing step-by-step instructions on how to develop and deploy AI technologies in a EU GDPR-compliant manner.

Financial services firms should consider how to incorporate AI into their existing data protection and cybersecurity frameworks in light of emerging AI-specific regulatory guidance and DORA's financial sector-specific operational resilience requirements.

We should note that there has been an increase in the use of synthetic data technologies, providing an alternative to using individuals' personal data. Synthetic data is information that is artificially generated using algorithms based on an individual's data sets. However, financial services firms still need to be aware of the quality of the initial data set that will filter into these technologies, as synthetic data may carry through or introduce inaccuracies or biases, and there is a risk the synthetic data could retain residual personal data. Still, the use of synthetic data may lessen the compliance risk of training AI technologies.

The Outlook for AI in Financial Services

The uptake of AI in financial services continues and there is no indication that will change, but the regulation and guidance surrounding its use certainly will. The EU AI Act, once in force, will set the tone for financial services firms with operations in the EU. U.K. regulators will no doubt have something to say following the industry feedback they have received, and keep your eyes peeled for developments in the U.S., where the Executive Order has mandated regulatory action. Stepping back, however, we are still some way off a detailed statutory framework for the use of AI in financial services, nor does there seem to be significant demand for one.