A&O SHEARMAN

OPINION

Zooming in on AI – #7: AI under financial regulations in the U.S., EU and U.K. – a comparative assessment of the current state of play: part 3

READ TIME
10 mins

PUBLISHED DATE
Oct 18 2024

This is the final note in a three-part series on the regulation of artificial intelligence in the financial services sector in the United States, the European Union and the United Kingdom. Our first note, available here, provided a comparative assessment of the approach that the three jurisdictions are taking to regulating the use of AI in the financial services sector and presented an action plan for firms to consider. The second note, available here, examined the scope and extraterritorial application of AI laws and regulation, data governance issues and related third-party service provider regimes. This final note assesses the current approach to enforcement, remedies and liability in each jurisdiction.

Enforcement

U.S.

The U.S. has not established a specific AI regulatory enforcement regime, but that does not mean that enforcement will not be very active in the meantime.

U.S. agencies are not waiting and have already begun to apply existing laws and regulations to investigate and bring actions where financial services participants misuse or make false claims regarding AI. For example:

- The Securities and Exchange Commission (SEC) has launched a number of initiatives and specific enforcement actions focused on disclosures concerning AI technology that do not fairly or accurately describe the design or use of the technology, or so-called "AI-washing," for corporate issuers as well as broker-dealers and investment advisers. In March 2024, the SEC announced settlements against two investment advisers for allegedly making false and misleading statements about their purported use of AI, including claims that AI was used to inform investment decisions. In June 2024, the SEC filed a complaint against a founder and former CEO of a defunct AI recruitment startup alleging material misrepresentations about the business, including its use of AI technology, citing claims that the company's product used "seven different AI algorithms" and "machine learning to improve the matching process as candidates select the roles they're interested in." In addition, in October 2024, the SEC announced a settlement with yet another investment adviser and two of its principals for allegedly making false claims about having an AI-driven platform for trading securities. These cases have all focused on disclosures, but the SEC is equally focused on controls regarding AI; the SEC's Division of Examinations' Examination Priorities for 2024 include an express focus on "automated investment tools, artificial intelligence, and trading algorithms or platforms, and the risks associated with the use of emerging technologies and alternative sources of data."
- The Commodity Futures Trading Commission (CFTC) has brought fewer cases, but it is no less focused on AI. In June 2023, it formed a new Cybersecurity and Emerging Technologies Task Force within the CFTC Division of Enforcement, which will address "cybersecurity issues and other concerns related to emerging technologies (including artificial intelligence)."
- The Federal Trade Commission has also entered the fray, primarily from a consumer protection perspective to date. It has required certain companies to destroy illegally obtained personal data and the AI system which was trained using this data but could easily expand its focus.
- The Department of Justice has also said that it may seek tougher sentences where any criminal offense is undertaken using AI as it could be deemed to be a "sophisticated means," which is an aggravating factor under the U.S. sentencing guidelines.

Each state can likewise bring AI cases, and many of state Attorneys General are almost certain to try to investigate any potential misuse of AI under existing consumer protection laws.

Due to the lack of comprehensive federal AI legislation, remedies arising from any harms derived from AI would need to be sought under existing federal and state legislation, but the U.S. class action system gives private plaintiffs (and their lawyers) means to seek access to certain information or damages under existing state consumer protection laws.

EU

The AI Act stipulates a decentralized enforcement framework. EU Member States must designate at a national level an authority to monitor compliance with the AI Act and to take enforcement and sanctioning action for breaches. For licenced financial institutions, the market surveillance authority under the AI Act is the designated national competent authority under EU financial services laws. The AI Act will apply to a developer of an AI systems that places the system on the market and to deployers of AI systems. It will also apply to importers and distributors. More detail on the scope of the Act is in Zooming in on AI - #6. In addition to the powers under the AI Act, all market surveillance authorities will also have the powers under the EU Market Surveillance Regulation. Examples of these powers include powers to require information or documents to be provided, the power to carry out on-site inspections, to carry out investigations and the power to require in-scope entities to take certain action and the power to impose financial penalties.

The AI Act establishes maximum levels of fines, which are:

- Breach of the ban on prohibited practices: EUR35 million or if a company, the higher of that and 7% of its total worldwide annual turnover in the preceding financial year.
- Breach of obligations by providers, deployers, authorised representatives, importers and distributors, including transparency obligations for limited risk AI: EUR15m or if a company, the higher of that and 3% of its total worldwide annual turnover in the preceding financial year.
- Providing incomplete, misleading or incorrect information: EUR7.5m or if a company, the higher of that and 1% of its total worldwide annual turnover in the preceding financial year.
- Negligent or intentional breaches by general-purpose AI providers: the higher of EUR15m and 3% of the provider's total worldwide annual turnover in the preceding financial year.

The European Commission is able to levy such penalties starting one year after the relevant provisions apply.

Individuals and legal entities have a right under the EU AI Act to make a complaint to the relevant market surveillance authority regarding any alleged infringement of the AI Act. This does not affect their rights under other administrative or judicial remedies. This differs from the position under EU financial services laws—consumer remedies against financial services companies are generally a matter of member state law and are not subject to material harmonisation at an EU level.

Data processors and data controllers may also be subject to fines under the General Data Protection Regulation (GDPR), and EU data protection authorities have already taken enforcement action against companies infringing the data protection laws while using AI. Individuals alleging infringement of their rights under GDPR may lodge a complaint with the relevant supervisory authority or to a judicial remedy through the courts.

The financial services national competent authorities of EU member states are equipped with powers to tackle breaches of their rules and other regulatory requirements arising under EU legislation such as the Capital Requirements Regulation and the Markets in Financial Instruments package, known as MiFID II. These include, for example, product intervention rules under MiFID II, amending capital buffers under the Capital Requirements Directive, as well as written notices, financial penalties and withdrawal licences. Regulated financial services firms may see regulatory enforcement action under EU financial services laws if a firm's use of an AI system does not comply with those requirements.

U.K.

The U.K. has not established a standalone AI regulatory enforcement regime.

For failings relating to data processing and protection, the Information Commissioner's Office (ICO) may take various steps, including but not limited to:

- Require information to be provided to it.
- Require a controller or processor to submit to an assessment as to data protection compliance.
- Require certain steps to be taken, or are refrained from being taken.
- Impose fines, for which there are two levels of maximum fine, depending on the statutory provision infringed, referred to as the standard maximum amount and the higher maximum amount. These are:
    - The standard maximum amount is up to 2% of the undertaking's total worldwide annual turnover in the preceding financial year.
    - The higher maximum amount is up to 4% of the undertaking's total worldwide annual turnover in the preceding financial year.

The ICO has taken action against financial institutions, and other entities (including with regards to an AI chatbot) for breaches of the requirements, including issuing fines and requiring firms to submit to a data controller compliance assessment. Individuals may lodge a complaint with the U.K. ICO, alleging infringement of the U.K. General Data Protection Regulation (U.K. GDPR). Individuals may also seek redress in the courts where they believe that their rights have been infringed due to non-compliant data processing.

The financial service regulators have not issued any specific guidance on their approach to enforcement around the use of AI. Financial companies should be mindful that their use of any technology, including AI, may amplify risks in their activities. The financial services regulators have several tools to address non-compliance with their rules and expectations, including publishing a statement, imposing financial penalties and suspending or cancelling a firm's licence or imposing a condition on the licence.

Regarding the government's "accountability and governance" principle, under the Senior Managers regime, technology systems, including AI systems, are within the responsibility of the Chief Operations function, and the Chief Risk function is responsible for overall management of the risk controls of a financial company. Financial companies must also have a senior manager responsible for each business, activity or management function, and where AI is used, the senior manager may also be subject to regulatory action if there is a regulatory breach in his/her area of responsibility and, the senior manager did not take reasonable steps to prevent the breach. These measures also support the "safety, security, robustness" principle.

The existing regulatory rules require regulated financial firms to have and maintain complaints handling procedures to ensure that complaints are dealt with fairly and promptly. According to the Financial Conduct Authority, this would include complaints about AI decisions in the context of the provision of financial services, or the failure to provide those services. Customers unsatisfied with the outcome of a firm's internal complaints investigation may refer a matter to the Financial Ombudsman Service (FOS) for independent review. The FOS is empowered to order redress in appropriate circumstances. Remedies may also be available through voluntary or mandatory financial company redress schemes and for investment losses on the insolvency of a regulated firm, through the Financial Services Compensation Scheme.

Liability

U.S.

There is no AI-specific liability legislation at the federal level. However, as noted above, existing federal and state laws can often be used to assign liability to the misuse of or false claims regarding AI. Moreover, in an effort to broaden the protections provided, various states have begun to pass statutes to establish liability for specific actions regarding AI. For instance, the Colorado AI Act, which will take effect in February 2026, imposes various obligations for developers and deployers of high-risk AI systems and authorises Colorado's attorney general to bring enforcement actions for violations of the Act, including through fines or injunctive relief.

Allen & Overy, now A&O Shearman, discuss issues relating to liability, including whether existing laws and standards are appropriate, and how to attribute fault, in note, "Legal liability of AI: Dealing with minds immeasurably superior to ours."

EU

The EU's proposed AI Liability Directive, which seeks to adapt non-contractual civil liability rules to AI, is yet to be finalised. The aim is to introduce measures that reduce the usual burden of proof standard through the use of disclosure (in the AI Act) and rebuttable presumptions to make it easier to succeed in damages claims.

The EU is also proposing to replace its existing Product Liability Directive with a new EU Directive on Liability for Defective Products, which will apply to AI (as well as other standalone software). The new Directive is not yet law. The new Directive will give individuals a right to claim compensation for damages from manufacturers or products, or parts thereof, that are placed on the EU market or put into service in the EU. It would be on a strict liability basis.

Individuals have a right, for material or non-material damages arising from an infringement of EU GDPR, to compensation from the controller and data processor. Damages cover pecuniary and non-pecuniary losses.

U.K.

A data controller and data processor may be liable to compensate an individual for losses suffered as a result of material damage or non-material damage (e.g., distress) arising from an infringement of the requirements in U.K. GDPR.

AI companies (including where a U.K. regulated financial services firm uses its own data to fine-tune or otherwise customise an AI model) may also be subject to liability arising from breach of contractual terms or pre-contractual misrepresentation and may also be liable for damages under product liability laws, such as the Consumer Protection Act 1987 or common law negligence claims. There is also the potential for defamation claims to the extent that output from an AI model is published to third parties.

Contravention by a regulated financial institution of a regulatory requirement may be actionable by an individual who suffers loss as a result of the contravention, although that right of action is disapplied by the regulators for many rules (including many systems and controls requirements, upon which most AI-related regulatory pronouncements are based). Contravening a rule is not a criminal offence (unless it constitutes committing a crime as established in legislation), and subject to certain exceptions, contravention does not render a contract void or unenforceable.

In "Regulating AI: Businesses need to prepare for increasing risk of future disputes," Allen & Overy, now A&O Shearman, discuss the degree of exposure to disputes risks over time

when something disruptive like AI butts against the law.

Related capabilities

Financial services advisory and regulatory
Artificial intelligence
Intellectual property
Markets Innovation Group
Data privacy and data protection
Litigation
White collar defense and global investigations
Technology

Related people

Thomas Donegan

PARTNER **LONDON**

Thomas has broad financial regulatory experience, which includes advising on strategic and structuring matters, regulatory authorisatio...

David Wakeling

PARTNER **LONDON**

David is Global Head of the firm's AI Advisory Practice and Markets Innovation Group (MIG), the latter of which is a group ...

Andrew Denny

PARTNER **LONDON**

Andrew heads the UK Public Law Group and was instrumental in founding the firms global Business and Human Rights Practice.

Mark Lanpher

PARTNER **WASHINGTON DC**

Mark is Co-Managing Partner of Washington DC and focuses on white collar, securities, anti-corruption, and other regulatory enforcement...

Sandy Collins

SENIOR PROFESSIONAL SUPPORT LAWYER **LONDON**

Sandy specialises in financial services law and regulation, advising on a broad range of UK and international financial regulatory m...

Laurie-Anne Ancenys

PARTNER **PARIS**

Laurie-Anne is head of the Tech & Data practice in Paris. She is specialized in the fields of information technology and da...