afme/ UK Finance LMA Loan Market Association

AI in Wholesale Financial Services

Recommendations for Third Parties to Support Financial Institutions' Risk Management and Regulatory Compliance

November 2026



Disclaimer

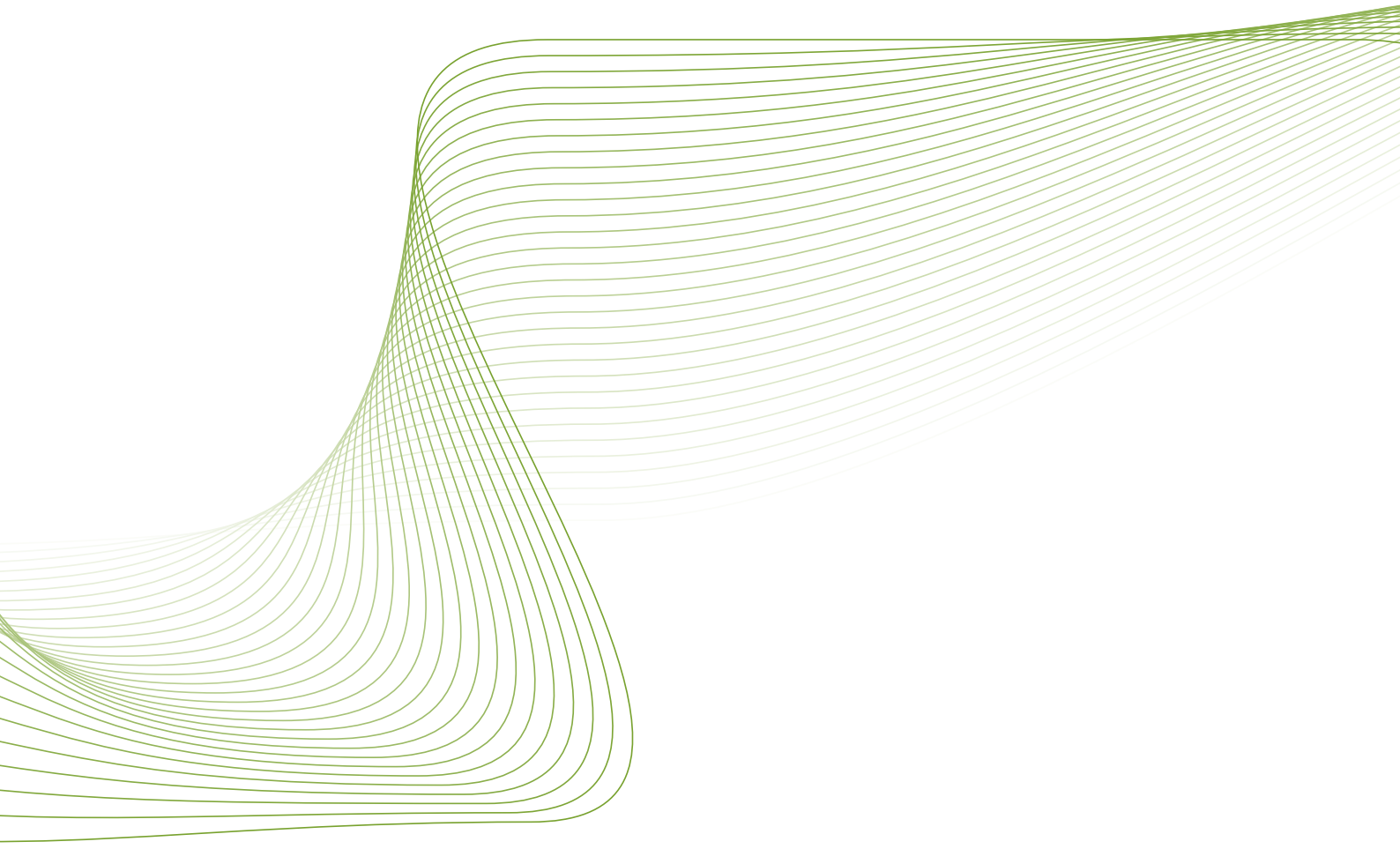
This document is intended for general information only and should not be treated as a substitute for independent legal advice on the matters addressed herein. It is not intended to constitute, and should not be relied upon as, legal, financial, investment, tax, regulatory, business or other professional advice.

The Loan Market Association (LMA), the Association for Financial Markets in Europe (AFME) and UK Finance (together, the "Authors") make no representation or warranty as to the accuracy, suitability or completeness of this document. The Authors accept no liability arising from, or relating to, the use of this document or its contents.

The recommendations contained in this document are voluntary and non-binding, both in relation to third parties and members of the Authors.

Nothing in this document is intended to affect the independent negotiation between members of the Authors and their third parties regarding the commercial terms and conditions governing the supply of any products and/or services. Each member and third party remains solely and individually responsible for its own independent commercial decisions and for ensuring compliance with all applicable laws and regulations, including competition law.

November 2026



Executive Summary

Financial services institutions are increasingly adopting AI-enabled products and services across their businesses. Where firms rely on third parties for AI capabilities, or where AI forms part of a third-party service, firms remain accountable for understanding and managing the associated risks and complying with applicable legal and regulatory obligations. This creates a dependency on third parties to provide the information, transparency and cooperation needed to support risk assessment, governance and oversight and evidence compliance with regulatory and supervisory expectations. In the context of AI, this dependency can be more complex due to the pace of adoption and technology change, opacity of systems and the increasingly complex and layered nature of AI ecosystems.

The paper sets out eight key recommendations for third parties providing AI products, or that use AI in the delivery of services to financial institutions:

1. Disclose the Use of AI in Service Delivery and Third Party's Supply Chain
2. Provide Transparent and Accurate Disclosure of AI Functionality
3. Provide Transparency Regarding Model Architecture
4. Disclose Clearly the Use of Financial Institutions' Data and Metadata
5. Include the Ability to "Toggle" AI Functionality
6. Enable Bring Your Own AI (BYOAI) / Bring Your Own Key (BYOK) Models Where Appropriate
7. Decouple AI Features from Unrelated Releases
8. Provide Adequate Notice of Planned AI Releases

While these issues will need to be discussed and agreed between third parties and financial institutions on a case-by-case basis, we believe that third parties that adopt these recommendations will bring direct benefits to their financial institution clients with regards management of associated risks and compliance with regulatory obligations.

Introduction

The adoption of AI within financial services continues to increase at pace, bringing significant opportunities for the growth and development of client offerings, operational processes and risk management. This adoption relies upon the services of third parties, who bring new products, services and expertise to add to the AI capabilities being developed by financial institutions in-house.

However, financial services is unlike many other industries with respect to the scale and complexity of the risks and obligations that firms must manage. As highly regulated institutions, financial institutions remain accountable for managing risks and regulatory compliance and rely on third parties to provide the information and transparency required to meet these obligations and support a range of risk management activities throughout the third-party lifecycle, including due diligence, contractual arrangements, ongoing oversight and assurance. Where AI forms part of a third-party service, related risks and information needs are assessed within this broader risk-based framework.

The Authors and their respective members wish to ensure that the financial services industry can continue to benefit from the broad range of AI-related products and services by third parties and the use of AI by third parties to enhance the delivery of their services. In this context, a key challenge is how the risk management and regulatory needs of financial institutions are translated into expectations placed on third parties, particularly where providers operate outside the regulatory perimeter and may have limited visibility into financial sector-specific obligations.

The aim of this paper is to assist third parties in making their services more attractive to financial institutions with respect to the regulatory and risk management implications of AI. The paper focuses, in particular, on implications that are salient for AI deployment, i.e. in addition to the wider set of considerations that may apply from a general third-party risk management perspective.

For the avoidance of doubt, we also note that this paper is not suggesting that third parties must:

- disclose source code or sensitive proprietary IP as a default position;
- treat every use of AI as "high-risk" (many uses are low-risk or incidental);
- adopt a one-size-fits-all control set regardless of the service or use case; or
- avoid using AI altogether.

Instead, we are seeking to address areas in which third parties can provide clarity, early notice, appropriate controls, and evidence with respect to AI usage, so that financial institutions can meet regulatory obligations efficiently and deploy services safely.

Definition of AI

For this paper, we apply the EU AI Act's definition of "AI" as below:

"'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."[1]

Scope of Third Parties

As discussed later in this paper, financial institutions are increasingly expected to understand where AI is used across their operations and third-party ecosystem. Therefore, the scope of third parties discussed in this paper includes not only providers of AI products and services (i.e. direct AI dependencies) but all third parties whose products and services include or use AI, however incidental the use may be (i.e. indirect AI dependencies). We note that direct reliance on AI services, AI embedded within a third-party solution, and more incidental or peripheral uses of AI present different issues in terms of visibility, control and ongoing monitoring. As discussed below, while these scenarios may warrant different levels of due diligence, firms should maintain sufficient visibility into AI use to understand and manage the associated risks.

[1] EU AI Act, Regulation (EU) 2024/1689, Article 3(1)

AI and Third-Party Risk – Context on the Regulatory Environment for Financial Institutions

Financial institutions operate within a highly regulated environment. This ranges from fundamental obligations on their operational resilience, governance and consumer protection to specific requirements on the use of AI.

While regulation is an important driver of firms' expectations, financial institutions do not manage risks solely because of regulatory requirements. The use of AI and third-party services can create risks for customers, firms and financial markets, and firms have a responsibility to identify, assess and manage those risks appropriately irrespective of the regulatory framework. The core requirements include the following interconnected risk management areas:

- Third-party risk management: Risk management and oversight of third-party arrangements, including assessment of risks such as operational resilience, security and data protection and the effectiveness of supplier controls. This includes identifying both direct and indirect use of AI within third-party services and assessing the associated risks in line with the criticality and risk profile of the arrangement.
- AI governance: Risk-based governance, assessment and documentation of AI use within the organisation, including both internal deployments and use in the provision of financial institutions' services. This should include appropriate controls around the use, monitoring and oversight of AI systems, with additional requirements applying to higher-risk use cases in line with applicable regulatory frameworks (e.g. EU AI Act, including where the institution assumes specific roles such as 'provider' or 'deployer').
- Model risk management: Documentation of models used, proportionate to the model's risk and materiality, to support financial institutions' oversight across areas including model development standards, data quality, model validation, performance measurement, risk mitigation and the management of model changes. For third-party and foundational models, financial institutions remain responsible for ensuring models are validated and monitored to standards consistent with their own model risk management framework, which depends on third parties providing adequate transparency and timely notification of material model changes (see Section 3).

In relation to third-party arrangements, financial institutions remain accountable under regulatory frameworks for all outcomes, even where AI components sit with external third parties or foundation model providers. However, in practice, financial institutions' ability to effectively manage risk is operationally dependent on third parties providing transparency, access and information about technical safeguards, and meaningful assurance. This creates an information asymmetry challenge, whereby accountability and responsibility sit downstream (with the financial institution), while information and technical controls often sit upstream (with the third party).

Factors Influencing How Financial Institutions Determine Appropriate Third-Party Due Diligence

Financial institutions apply a risk-based and proportionate approach to third-party due diligence, with the depth of assessment driven by the criticality and risk profile of the arrangement. The assessment of risk and applicable due diligence will vary from institution to institution based on the usage and risk profile of the particular institution. The same principles apply where third-party services involve the use of AI. However – particularly as AI technologies continue to evolve – this may increase the complexity of due diligence and the level of transparency required from third parties.

To this end, firms will assess the role and materiality of AI within the service, and may require information from vendors to support this assessment, including for example:

- Whether and how the vendor is using AI in the delivery of the service (including if it is incidental or integral to the vendor's product/service).
- The nature and use of data within the service and whether the third party is using or intends to use financial institution data in connection with the use of AI systems.
- Whether the AI use case may be subject to additional regulatory requirements under applicable frameworks (e.g. will the system be classed as "high-risk" under the EU AI Act[2]).
- The extent to which the service underpins the firm's most critical services, such that disruption would have a material impact on their delivery.
- The extent to which the AI use case may impact the financial institutions' risk profile.
- Whether AI is used within the third party's own supply chain and the nature of the usage.

In practice, firms' ability to assess and manage AI-related risks is heavily dependent on the availability of clear, accurate and proportionate information from third parties. Improving transparency around the use of AI can help reduce information asymmetries between firms and their providers, enabling more effective risk management while supporting AI adoption.

[2] EU AI Act Article 6 and Annex III

AI Recommendations to Third Parties Supplying Financial Institutions

Financial institutions need to identify and assess risks arising from third-party services, including where AI forms part of the service delivery, and to evidence how those risks are managed in line with regulatory requirements. In practice, this translates into specific information and transparency expectations for third parties. We set out below a series of recommendations which third parties could adopt to assist their financial services clients in managing the related risks and meeting regulatory obligations.

1. Disclose the Use of AI in Service Delivery and Third Party's Supply Chain

Disclosure of AI use in service delivery and supporting supply chains enables firms to assess associated risks and satisfy governance, risk management and oversight requirements. However, identifying where AI is being used can be challenging where it is not explicitly part of the product or service being procured, or where AI is used within third party's own supply chain.

Financial institutions are required to risk assess their third-party use and supply chains and to satisfy themselves that their third parties are themselves ensuring supply chain compliance. Third parties should provide sufficient information regarding the use of AI in service delivery and supporting supply chains to enable firms to understand where AI is being used, assess associated risks and apply appropriate oversight and controls. This would apply to services as well as technology vendors e.g. a law firm using an AI system for document drafting, and a back-office vendor automating previously manual processes using AI.

2. Provide Transparent and Accurate Disclosure of AI Functionality

Financial institutions are required to perform assessments of AI usage across their business to manage associated risks and ensure compliance with regulatory obligations. Where third parties use AI in the delivery of services, this can create challenges for financial institutions in identifying where and how AI is being used within third-party services.

For instance: third parties may add "AI features" to their products without prior consultation. While they may be positive product enhancements, to financial institutions these are features that cannot be deployed until an AI risk review process is completed, even if the use of AI is determined as minor or incidental. Conversely, "AI washing" is a term describing occurrences when third parties' marketing may imply a greater use of AI than exists, often with the aim of driving sales / brand value etc. In such circumstances, stating that a product "uses AI" would render financial institutions duty-bound to conduct a resource intensive AI risk assessment to ensure regulatory compliance. This can result in unnecessary delays in deployment of software and hence is a practice that financial institutions would discourage firms from engaging in.

Therefore, clear and accurate documentation of the purpose and scope of any AI functionality within a third-party product at onboarding and, on an ongoing basis, of any new release is required, providing as much detail as possible.

A concise disclosure pack of this kind reduces repeated follow-up questions, prevents late-stage surprises, and helps financial institutions align approvals with planned release dates.

3. Provide Transparency Regarding Model and System Architecture

Financial institutions require sufficient transparency on the architecture and operations of AI models procured from or used within third-party services in order to assess model-related risks and meet model risk management requirements. This includes understanding how the model functions, its intended use, key limitations and how it has been developed and tested, which may be presented in the form of model or system cards.

Separately, where firms are subject to regulatory obligations in relation to their use of AI systems (for example, where they act as deployers of a "high-risk" AI system under the EU AI Act, additional information may be required to support appropriate use, oversight and monitoring of the model). This may include, for example, information required to support assessments such as fundamental rights impact assessments.

Third parties are therefore requested to provide transparency on the architecture of their models, as well as the underlying data and training processes, proportionate to the model's risk and materiality, to enable efficient model risk assessment. This includes providing information on how the model functions and its intended use; key limitations, assumptions and known failure modes; how the model has been developed, tested and validated, including validation evidence; benchmarks and performance measurement; the data used for training and its quality, lineage and representativeness; explainability of model outputs, where applicable; and advance notification of material model changes or new versions, with sufficient detail for banks to assess impact and re-validate.

4. Disclose Clearly the Use of Financial Institutions' Data and Metadata

Financial institutions require transparency regarding how data (including metadata or derived data) originating from the financial institution will be used throughout the lifecycle of the service, and clear agreement on the rights and permissions associated with that use. This includes understanding what data is collected, where it is stored, how it has been treated (e.g. for unjust bias mitigation), what it is used for (e.g. training models or product improvement), who has access to it and how it is retained or deleted. Firms may require contractual provisions regarding the ownership, retention, deletion, confidentiality and permitted use of data generated through the use of AI systems, including prompts, outputs, metadata and derived data. Data handling provisions should be clearly set out in contractual terms. This is driven not only by GDPR[3] but by wider regulatory obligations e.g. obligations to clients, product laws, data location and transfer provisions etc, which are often specific to the use case.

[3] General Data Protection Regulation - Regulation (EU) 2016/679, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj and UK equivalent available at https://www.legislation.gov.uk/eur/2016/679/contents

5. Include the Ability to “Toggle” AI Functionality

Wherever possible, third parties should include the ability for financial institutions to “toggle” AI functionality on and off. This can serve as an important operational risk control (not merely a product preference), because it enables controlled roll-out, jurisdictional compliance and swift containment if issues arise. This should be offered at multiple levels, both, group-wide and by jurisdiction, legal entity and individual user levels. This means that the financial institution can, as deemed necessary, conduct a controlled release across their estate and/or ensure that only authorised roles are permitted to use the AI functionality. Often, the ability to control a release would make a positive contribution to an AI risk assessment and decrease the likelihood of a release being declined.

6. Enable Bring Your Own AI (BYOAI) / Bring Your Own Key (BYOK) Models Where Appropriate

Financial institutions should be provided with the option, where technically and commercially feasible, to utilise approved institution-controlled AI models and cryptographic controls ("Bring Your Own AI" and "Bring Your Own Key"). Such arrangements may enhance control over data processing, model selection, model changes, geographic hosting, monitoring, and regulatory compliance.

However, BYOAI arrangements do not remove the vendor's responsibility for the governance of the application, orchestration layer, access controls, workflow design, logging, resilience, security, and output handling. Responsibilities between the institution, vendor, model provider and any other relevant parties should be clearly documented and contractually allocated.

7. Decouple AI Features from Unrelated Releases

In some cases, third parties may issue releases which involve both “AI” and other “non-AI” features. Changes involving AI functionality may be subject to distinct governance, risk assessment or approval processes, depending on the nature of the use case and associated risks. Therefore, bundled releases can create dependencies that could delay or block the deployment until the AI elements are risk assessed, irrespective of how minor the AI component is. Where practicable, third parties should consider decoupling AI components and deploy them as standalone releases to avoid unnecessary delays to unrelated components.

8. Provide Adequate Notice of Planned AI Releases

Financial institutions require information on how model or AI-feature changes are governed, communicated, tested and rolled out as well as sufficient notice and clarity of material changes in order to assess potential impacts, manage associated risks and meet applicable governance and regulatory obligations. Late notification of an AI element can result in a release being declined or temporarily blocked while an AI risk assessment is completed. As a result, it is recommended that as much notice as possible is provided to clients, alongside detailed documentation, to allow time for the assessment to be completed and not jeopardise any planned release date.

Conclusion

The integration of AI within the financial sector presents both significant opportunities and challenges. Financial institutions have invested heavily in AI to enhance their processes and offerings to clients. However, the regulatory landscape within the EU and UK necessitates rigorous due diligence and risk assessments for any AI-related functionality introduced by third parties.

By adopting the recommendations set out in this paper, third parties can help build more transparent and collaborative relationships with financial institutions, reducing friction in due diligence and oversight, and enabling both parties to realise the benefits of AI. The proactive management of AI risks will not only enhance the trust between financial institutions and third parties but also contribute to the overall advancement of AI in the financial sector.

About the Loan Market Association (LMA)

The LMA is where EMEA loan markets meet.
For more than 30 years, we have brought together market participants to drive greater efficiency, liquidity, transparency and expertise across the loan markets. By fostering collaboration and developing market standards, guidance and education, we help enable better outcomes for lenders, investors and borrowers.
Today, with over 880 members across 69 jurisdictions, the LMA represents a diverse and growing community of market participants, including banks, institutional investors, private and public sector issuers, alternative lenders, technology providers and market infrastructure firms across the UK, US, EMEA and Africa.
Through our work in documentation, market practice, education, sustainability, operations and advocacy, we support the continued development of resilient, innovative and efficient loan markets.

Loan Market Association
10 Upper Bank Street
London
E14 5JJ
T+ 44 (0)20 4583 0576
lma@lma.eu.com

LMA Contacts



Aman Luther
Head of Technology and Innovation
LMA
Amandeep.Luther@lma.eu.com

About UK Finance

The financial services industry plays a vital and often underappreciated role in enabling individuals, families and communities to achieve their ambitions in a safe and sustainable way through home ownership, starting a new business or saving for retirement. The sector is fundamental to people's lives, and we are proud to promote the work it is doing to support customers and businesses up and down the country.

Whether it's through innovating for the future, driving economic growth, helping struggling customers amid increases in the cost of living, fighting economic crime or working to finance the net zero transition the industry is having an overwhelmingly positive effect on the lives of people across the UK and improving the society in which we live.

Further information is available at: www.ukfinance.org.uk

UK Finance Contacts



Adam Avards
Principal, Head of Cyber Security & Third-Party Risk Policy,
UK Finance
adam.avards@ukfinance.org.uk

AFME Contacts



Fiona Willis
Director, Technology & Operations
AFME
Fiona.Willis@afme.eu



Marcus Corry
Director, Technology & Operations
AFME
Marcus.Corry@afme.eu

afme/

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

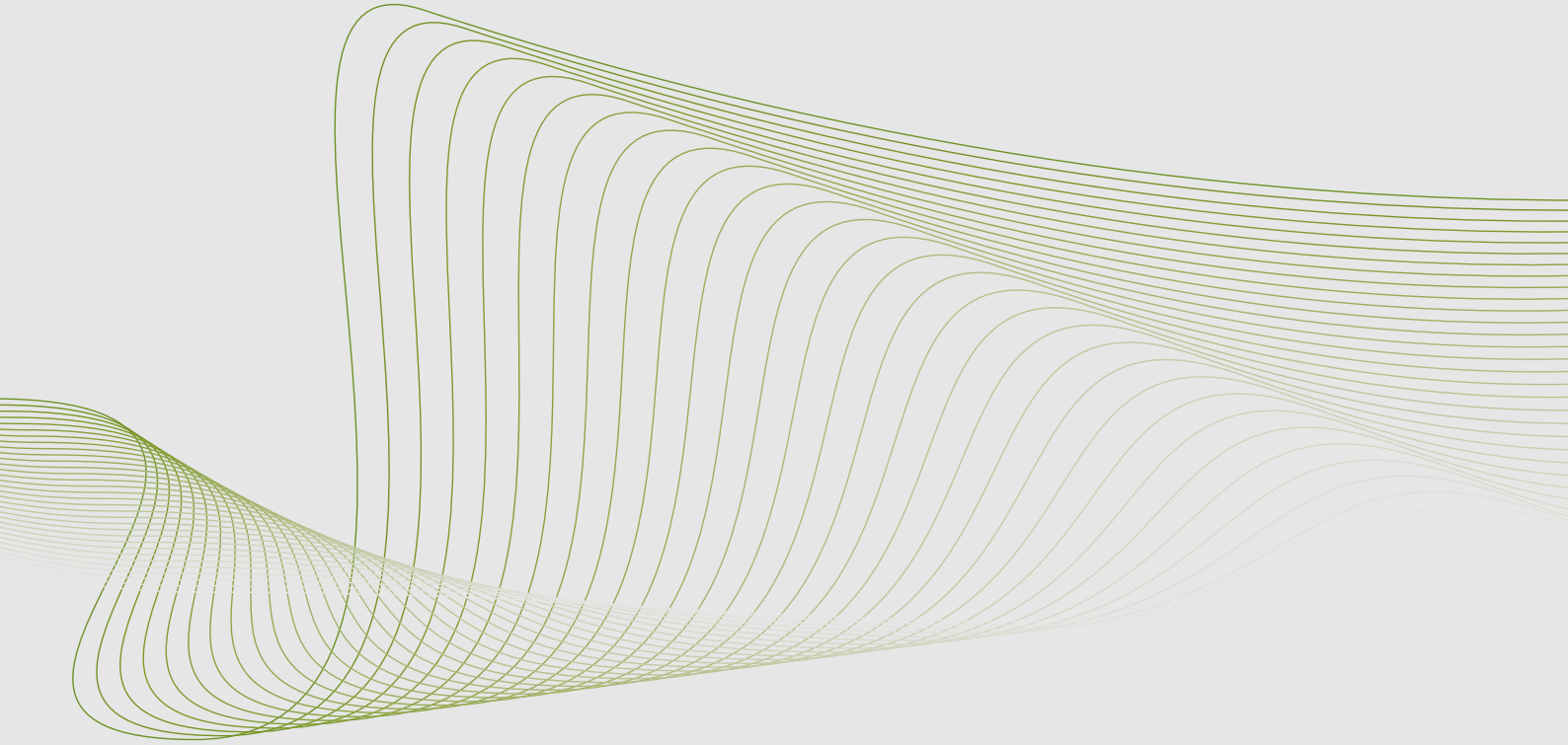
Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)



London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Press enquiries
Rebecca Hansford
Head of Communications
and Marketing
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Frankfurt Office
Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

AFME is registered on the
EU Transparency Register,
registration number
65110063986-76

www.afme.eu