Position Paper

Use of Third-Party AI Systems

February 2024

Executive Summary

While there are generic AI risks which may arise regardless of whether an AI system is developed in-house or with a third-party provider, this paper considers the particular challenges that are presented by the use by financial institutions (FIs) of third-party Artificial Intelligence (AI) systems. Such challenges can fall into two categories, which are broadly: third-party risks and AI-specific challenges. Since the former are partially addressed by existing regulation, this paper is focused on specific challenges introduced or exacerbated by AI as a technology. This may be particularly true of Generative AI.

These challenges, which must be assessed each time from a use-case and risk-based perspective, are:

Theme	Challenges	Suggested Mitigants
Transparency	Insufficient transparency over where AI is being used .	Third-party providers need to disclose to FIs all AI components within relevant services.
	Insufficient transparency over key aspects of third-party AI models, including model development, output and testing and the third-party provider's resilience and cybersecurity.	Greater transparency from third-party providers is crucial on all these points. While we generally do not support AI-specific regulation, the EU AI Act approach of placing specific transparency requirements on the "developer" of an AI system may be a helpful model to follow.
Data Governance	Insufficient information on key aspects of how data have been collected, assessed and used, as well as on intellectual property and data protection considerations.	It is crucial that third-party providers are transparent with how they have used data to train, validate and test their models, including what consent has been obtained. They should be encouraged to prioritise data relevance. Third-party providers must also be transparent regarding data flows, to ensure that FI data is not being comingled and used to train a third-party model without consent.
Systemic Concentration Risk from Foundation Models	Risks arising from the barriers to entry for foundation model developers, which could exhibit themselves in herding risks, competition risks or resilience risks.	As with AFME's existing positions on cloud concentration risk, this needs to be addressed at a jurisdictional policy level, rather than by individual firms. We would welcome discussion with regulators on how to achieve this – there is a risk that the introduction of policies which seek to restrict third-party provider usage by FIs or mandate multi-vendor strategies would actually limit the overall ability of the sector to progress their adoption of AI and could also impose a competitive disadvantage on FIs in the region.

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

- Transparency: it is critical for FIs to have proportionate information on a wide range of elements relating to the third-party AI systems they are deploying, including where within the system AI is used and details on model development, outputs and testing, as well as the operational resilience and cybersecurity of the third party itself;
- Data Governance: similarly, proportionate information is required by FIs on how data has been acquired, collected and prepared by the third party, the controls to which it has been subject, how data flows are managed and any additional requirements to which it is subject (such as data protection or intellectual property laws).
- Concentration risk in relation to foundation models: consideration needs to be given to how systemic concentration risk may arise from use of third-party AI systems, particularly given the increasing sophistication of foundation models, and how this can be addressed at an industry level without curtailing individual FI choice.

Definition of AI

For the purposes of this paper we broadly support the OECD's definition "*An AI system is a machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*"[1].

Arrangement Structures of Third-Party AI Services

Increased attention on the potential benefits of implementing AI within financial services over recent years has significantly expanded the market for third-party AI services. While some FIs are investing in in-house AI development, many more are also, or exclusively, exploring third-party solutions or creating hybrid versions, building internal solutions on third-party models. Here, they are able to benefit from AI solutions that have already been developed, tested and refined and that can be implemented on a shorter timescale.

However, not all third-party AI solutions are alike. There are a number of ways in which the interaction between FIs and third parties can differ, such as:

- Whether the third-party AI system is bought fully 'off the shelf' or modified by the third party to meet the individual needs of the FI;
- Whether the third-party system has been trained by the third party using data from the third party, public sources (e.g. public data), the FI or a combination of these;
- Whether the third-party hosts the system on its platform or whether it is hosted by the FI; and
- Whether the third-party service is a model (including multi-purpose foundation models) which the FI then uses to create its own AI system.

While the challenges we outline below may well be common to third-party solutions, some will be novel to the use of AI or nuanced depending on the above factors.

Regulation of Third-Party Operational Risks

There are two main challenges associated with adoption of third-party AI systems: first, challenges which are not specific to any particular technology and, second, AI-specific challenges, i.e. challenges which are introduced or exacerbated by the use of AI.

[1] Organisation for Economic Co-operation and Development (OECD) – see https://oecd.ai/en/ai-principles

Risks related to third-party relationships are not new to financial services firms or to regulators. Regulatory requirements are in place and under further development to assist firms in addressing these risks, including:

- The EU Digital Operational Resilience Act (DORA), which applies from January 2025;
- EBA Guidelines on Outsourcing Arrangements (2019) and ESMA Guidelines on Outsourcing to Cloud Services Providers (2020);
- Ongoing work in the UK on the Critical Third Parties (CTP) regime; and
- PRA Supervisory Statement SS2/21 Outsourcing and Third-Party Risk Management.

In light of this, our paper is focused on the AI-specific challenges which may arise beyond standard operational challenges.

Key AI-Specific Challenges

While using third-party systems can significantly broaden the ability of firms to implement AI at scale, there are a number of ways in which this can be more challenging than developing AI systems in-house. We outline some of these below and suggest mitigants.

Challenge 1: Transparency

It is crucial for any institution deploying a third-party AI system to have appropriate transparency from the third-party over key areas of the AI system's development and functioning. This should extend to areas such as how the model has been trained, how data have been obtained and used (see also below on data governance) and what controls are built into the model – particularly crucial since many of the risks that can arise from AI models need to be identified and managed at source, rather than later in the models' lifecycle.

This is particularly important within financial services, where institutions are subject to a complex regulatory landscape, which is generally technology-neutral and in which accountability/liability for compliance remains with FIs even where services may be provided by third parties. For example, obligations relating to investor protection, the use of data, IT risk and individual accountability/oversight regimes apply regardless of the underlying technology being used and financial institutions need to be able to evidence oversight and compliance.

From a risk management perspective, FIs must also be able to assess any third-party AI systems against their own risk tolerances and put in place additional mitigations where necessary. This involves the disclosure by the third-party provider of relevant components in products that utilise AI technology (including of new AI components into non-AI software) in order to ensure that FIs have a clear view of where AI is used within its organisation and assess the risks involved.

However, use of third-party AI services naturally results in a reduction of transparency for FIs compared to AI development that is performed fully in house, unless specific measures are put in place to address this. This may be particularly challenging in relation to:

- Model development: the way in which a model has been trained by the third party, including the way in which the purpose, capabilities and limitations of the system have been defined;
- Model outputs: the model's performance and (to the extent appropriate) the technical explainability of how the model is producing its outputs, which is particularly important where the model's deployment will have a direct client impact or impact on individuals;
- Model testing: the programme of testing to which the model has been subject prior to being approved by the third party and the ability of the FI to evaluate the model's performance on an ongoing basis;

- Operational resilience and cybersecurity: where the AI system continues to be hosted by third party, the ability of the FI to review and test the robustness of the third party's systems; and
- Data governance (see separate section below).

Suggested Mitigants

First, we note that the level of transparency which a FI will need over any individual third-party service will be risk-based and dependent on the specific use case and type of AI (for example, foundation model). We encourage regulators to consider how any obligations upon third-party providers can allow for this flexibility rather than mandating a one-size-fits-all set of requirements.

While AFME is not generally supportive of the regulation of specific technologies and does not call for a prescriptive approach to AI regulation, we note that there are elements of the EU AI Act which could be helpful in addressing some of these transparency challenges. In the Act, the EU sets out requirements on the "developer" of any "high-risk" AI system, which may be a third party, including provision of detailed technical documentation, containing the kind of details of which only the developer will have knowledge, and a post-market monitoring system[2]. This enhances transparency between the developer and deployer, which has the potential of achieving greater transparency across the entire AI value chain.

Although voluntary frameworks detailing requirements for transparency by the third-party provider can aid in adherence to FIs obligations, this may be only a temporary solution. It important to take note that in times of stress, the fate of these voluntary frameworks and shared responsibility frameworks may be uncertain due to a lack of enforcement mechanisms. We therefore encourage other regulators to consider how similar obligations can be placed on third-party developers of AI systems to provide appropriate levels of transparency over key technical information, whether through strengthened voluntary frameworks, or through appropriate and proportionate enforcement mechanisms.

We also note above that it is critical for third-party providers to disclose any components in their products that utilise AI technology, in order to ensure that FIs have a clear view of where AI is used within its organisation and assess the potential risks involved.

Challenge 2: Data Governance

There is a particular third-party challenge relating to data governance. AI models rely on three main types of data: training data, validation data and testing data. It is worth noting, with in the EU, that all three types of data are covered by the EU AI Act Article 10 on data and data governance.

An AI model may use data provided by the third party, the FI, or a combination of both. Where third-party data forms all or part of the data set, the FI will need a level of transparency from the third party over areas such as:

- How the data has been acquired, collected and prepared, including the type of data, the original purpose of the data collection, any relevant consent for use and whether 'alternative data' (data collected from non-traditional sources) or personal information has been used;
- How its accuracy and completeness have been assessed and, where necessary, mitigated;
- How its representativeness and susceptibility to unjust bias have been assessed and, where necessary, mitigated;

[2] See Articles 11 and 61

- Any assumptions to which the use of the data set has been subject;
- How data from the FI are being used, as, for example, there may be the possibility that the third party retains the data to train its model further; in such cases, additional data protection guarantees will be required from the third party;
- Consideration of intellectual property rights - AI models, while adept at generating contextually relevant and coherent text, operate by learning from large datasets that can include copyrighted material. The challenge lies in the inherent complexity of identifying and tracking the origins of information. Consequently, there's a heightened risk of unintentional copyright violations, especially when responding to queries that touch upon proprietary financial models and analyses; and
- Interaction with EU and UK General Data Protection Regulations (GDPR).

There also will be a particular challenge relating to the type of AI system used. For example, where an AI system relies upon a foundation model that may not have been created for that specific system, this means that the data in question is one step further removed from the FI. While seeking further transparency from third-party providers as we outline below, the industry must work on how to incorporate, within their own risk tolerances, third-party AI systems' output (especially foundation models' output), although these may be generated based on more data that is not known or controllable than would have been used in an AI system developed by the FI itself for a specific use case, purpose and objective.

In addition, the scale of the data on which Generative AI systems are generally trained means that ensuring appropriate data governance can be particularly challenging.

Suggested Mitigants

In relation to data governance, it is crucial that third-party providers are transparent with how they have used data to train, validate and test their models, including what consent has been obtained. In particular, they should be encouraged to prioritise the relevance of the data, i.e. by using high quality training data relevant to the use case the system is being deployed and/or to disclose the use cases they intended for the model. This will ensure that the deployment domain of the model matches its training domain. This will allow FIs to be able to use the system confidently knowing that training data is relevant to the particular use case it wants to deploy the AI system for, without responsibility for this being placed unnecessarily onto the FI itself.

Furthermore, third-party providers must be transparent regarding data flows, to ensure that FI data is not being commingled and used to train a third-party model without permission.

Challenge 3: Systemic Concentration Risk from Foundation Models

Concentration risk within individual firms is generic to use of third parties and therefore tends to be addressed via relevant regulation. However, with the expansion in development and use of foundation models in FIs' deployment of AI, the potential for market-wide concentration increases.

There are considerable barriers to entry impacting the range of foundation models available to industries such as financial services. The cost of providing foundation models is driven by competition for talent, access to computational power and sufficient data sets, combined with ongoing investments in product development, marketing and distribution. This is reflected in the largest technology companies owning the initial foundation models that have emerged within financial services. It has the potential to lead to a situation where there are only a few companies providing foundation models to the financial services industry.

Where multiple FIs are using the same foundation models for their AI deployment, there is a risk that their AI systems may tend towards similar outputs. In lower risk use cases, for example within banking operations,

this may not produce negative consequences. However, in market-facing use cases, there may be risks related to herding, in which there emerges a convergence of trading and investment strategies, or market manipulation, which could have systemic implications.

A separate concern is that market concentration has the potential to lead to less pricing competition and/or an imbalance between third-party providers and FIs, expressed through greater difficulty in agreeing contracts with sufficient transparency to meet FI's ongoing regulatory obligations. This may be exacerbated by the bundling of services, for example combining AI with cloud services.

Finally, we note the resilience risk (at an institutional and systemic level) arising from intersection of data/intellectual property related risks and the market dominance by a few suppliers. Concerns around improperly acquired data or intellectual property breaches could result in regulatory blocks on such models, that could jeopardise the operations of FIs (and the overall system), which would be particularly acute where multiple AI systems are built across the industry in top of particular foundation models.[3]

Suggested Mitigants

As previously noted in AFME discussions on concentration risk, particularly in relation to cloud services[4], it is a change that is difficult for individual FIs to measure or address. It should instead be managed at a jurisdictional policy level; we welcome dialogue with regulators on this subject and acknowledge the efforts that have already been made to address operational risks through initiatives such as DORA or the UK CTP regime. However, we also strongly caution against the introduction of policies which seek to restrict third-party usage by FIs or mandate multi-vendor strategies. Decisions on when and how to use third-party services should be made according to an FI's own strategy, needs and risk appetite. Placing restrictions on this would limit the overall ability of the sector to progress their adoption of AI and could also impose a competitive disadvantage on FIs in the region.

Regarding herding risk it is also worth noting that 'off the shelf' use of the same foundation models by FIs would prove a competitive disadvantage to the FIs involved. This is a strong incentive for FIs to ensure that any AI systems using foundation models, particularly for market-facing activities, are sufficiently tailored to their own strategies and needs.

Finally, we also refer back to our comments under 'Challenge 1: Transparency' above, in which we discuss the importance of clear information flow from third-parties to Financial Institutions, including as part of contractual arrangements.

Conclusions

Working with third parties in AI deployment presents FIs with specific challenges that are beyond both those generic to AI deployment and those generic to third-party relationships (that latter of which are generally addressed through existing regulation). While AFME is not calling for AI specific regulation, we would appreciate further dialogue with regulators and supervisors on how these can be addressed. Detailed information flow, proportionate to the risks and use case, between third parties and FIs on a range of information relating to the AI model, including on data governance, is critical to ensure safe and effective deployment. In addition, we encourage consideration of how concentration risk may arise at a systemic level and how this can be managed without placing undue restrictions upon the industry.

[3] We note, for example, the decision of the Italian Data Protection Regulator in March 2023 to temporarily ban the use of ChatGPT https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870847

[4] https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_CloudComputing2022_06.pdf

AFME Contacts
Coen ter Wal
coen.terwal@afme.eu
+44 (0)20 3828 2727

Fiona Willis
fiona.willis@afme.eu
+44 (0)20 3828 2739

Stefano Mazzocchi
stefano.mazzocchi@afme.eu
+32 2 883 55 46