Paris, 6 December 2024

AI in the financial sector
Key messages from the Paris Europlace AI Working Group

1. Main messages

Paris Europlace encourages European authorities to find the best regulatory balance between supporting technological innovations and ensuring investor protection and financial stability. The competitiveness of European companies, whether financial or not, must be preserved through a thorough assessment also including the regulations in place in other jurisdictions, especially when a new EU regulation has been implemented. The EU regulation must indeed focus on risks and remain technologically neutral.

Actually, in itself, AI is not new, having indeed quite a long history in the financial services industry (for credit risk scoring, high-frequency trading, and robo-advice) and being already subject to existing risk frameworks. Specifically, AI applications in finance are already subject to regulation through sectoral or cross-sectoral specific rules, such as consumer data privacy regulation, consumer protection regulation in lending operations, or prudential requirements concerning data governance, cyber risk, third-party risk, information systems outsourcing, or operational risk. We thus consider that the financial industry is already more heavily regulated than other sectors. We stand for that reason against an additional, sectoral regulation.

Consequently, any additional regulation resulting from the implementation of the AI Act should be proportionate and adequately defined, not hampering competitiveness or innovation. Further technology-specific regulation with respect to AI seems neither warranted nor desirable, if not tested ex ante correctly from a competitiveness standpoint. Actually, reaching a global level playing field is essential as the competition for EU firms is global and we see many providers developing technology faster in less regulated environments.

In addition, the risk of regulatory uncertainty is elevated for businesses pursuing innovation, just because AI applications are constantly evolving, so regulators are aiming at a moving target. Also importantly, AI and data are inexorably interlinked, as AI requires access to sufficient volumes of quality data: therefore, improper data localisation requirements could limit its potential and even risk creating bias and possible distortions to train AI systems. Consequently, open finance (FiDA) must remain carefully adjusted so as to maintain EU firms' competitiveness, avoid unintended consequences (cyber security risks, etc.) and never lead to asymmetric data sharing with non-EU competitors.

2. General questions on AI applications in financial services

Regarding the use of AI systems, the working group notes that all financial services players have already caught on to the emergence of AI and generative AI. The financial services industry is already using them with applications that improve productivity, operational efficiency, and risk management. The working group highlights the various benefits of AI. Through machine learning, natural language processing (NLP), and generative AI, financial services stakeholders can automate routine tasks and reduce operational expenses, improve decision-making, and analyze large data sets. For many stakeholders, AI represents an opportunity to both save time and to strengthen operational efficiency, and a valuable decision-making aid thanks to its ability to analyze data quickly. For financial services, AI also represents a significant opportunity for fraud pattern detection by quickly identifying and preventing fraudulent activity. When it comes to customer service, chatbots are already in use to provide instant answers, reducing waiting times and improving customer satisfaction. In addition, AI can improve the efficiency and accuracy of legal service delivery by automating routine tasks such as drafting, document review, contract management, and automation of regulatory oversight, thereby mitigating risk and reducing penalties.

Nevertheless, the use of AI and generative AI also involves certain risks. We highlight in particular the risk of dependency on non-European AI providers, which raises issues of data transfer, regulation and sovereignty risks. Added to this is the difficult transparency due to the complexity of AI, especially for large language models (LLMs) that suffer from biases and occasional hallucinations, potentially producing incorrect answers due to poor data quality or gaps. The lack of explainability criteria for AI, especially when provided by third parties, compounds this problem.

We thus underline the need to train and acculturate staff members in the use of AI and specifically generative AI.

When it comes to AI applications, there are two types of applications: in-house AI development (vendors) and external sourcing (deployers). Most financial services players balance in-house AI development and external sourcing based on use cases. In-house development provides greater control and mitigates “black box” issues, while external solutions are generally chosen when faster deployment is required. This hybrid strategy allows companies to:

- Maintain data privacy and security.
- Reduce economic dependence on third-party providers.
- Tailored solutions to specific business needs.

To govern these AI applications, firms are also establishing dedicated AI governance committees, high-risk system registers, and clear use-case documentation to ensure responsible and trustworthy use. Regulatory measures, including EU’s AI Act, will also play a role in standardizing practices across the financial services industry.

In terms of data needs, access to high-quality datasets is critical, although reliance on non-EU providers poses privacy and sovereignty risks. Data needs include:

- **Market Data**: Essential for predictive analytics and investment decisions.
- **Customer Data**: Used for personalization, fraud detection, and risk analysis.

- **Economic Indicators**: Support forecasting and trend analysis.

External data access is limited due to privacy regulations and integration challenges. Institutions advocate for policies that encourage safe data-sharing frameworks, which would enhance AI model performance and innovation.

3. Questions related to specific use cases in financial services

In the banking sector, AI is applied in diverse use cases, including risk assessment, credit scoring, robo-advice, sustainable finance, regulatory compliance, fraud detection, and customer service. AI offers significant opportunities, such as improved efficiency, personalized services, and enhanced risk management. However, it also brings challenges, including potential biases, opacity in decision-making, and supervision complexities. Major barriers to AI adoption include skills shortages, high regulatory compliance costs, and technology readiness. There is an ongoing debate on whether AI reduces or increases bias, depending on its application and monitoring. General-purpose AI introduces both new opportunities and risks, especially in customer interactions and decision automation. Banks rely on various AI development models, from in-house applications to collaborations with external providers.

In the market infrastructure sector, AI is used in areas like risk management, sustainable finance, and regulatory compliance, mainly to enhance data processing, automate tasks, and maintain competitiveness through innovation. Key challenges include setting clear goals, retaining expertise, and ensuring models stay updated. Barriers to AI development may be due to a shortage of combined technical and business skills, funding, and regulatory predictability. While AI aims to improve processes rather than affect individuals, bias risks remain a concern. General-purpose AI introduces risks, like dependency and energy consumption. Development models vary, including in-house, external providers, or hybrid collaborations.

In the insurance sector, the specific AI strategies, use cases, and levels of implementation may differ from one insurer to another. Various use cases are being considered, including but not limited to customer service, operational excellence, business development, compliance, fraud detection and support functions. The flexibility of AI enables tailored solutions that align with both customer needs and operational goals, improving data control and security. Opportunities may refer to enhanced risk assessment, customized model ownership, and optimized process efficiency, allowing firms to derive substantial financial and strategic value. However, integrating AI presents challenges such as educational needs, regulatory understanding, and integration with existing systems. The accelerated pace of AI development necessitates continuous training and cross-functional collaboration. AI offers potential bias reduction by standardizing decision-making but requires vigilant monitoring to prevent unintended biases. Insurers often adopt a hybrid approach for AI development, balancing external expertise with in-house solutions, particularly for risk qualification.

Last, asset managers are exploring AI applications to enhance productivity, operational efficiency, and regulatory and client reporting. AI is primarily used for risk management, portfolio optimization, compliance, reporting, ESG scoring, customer engagement, and process enhancement. AI offers efficiency gains by automating tasks, improving data accuracy, and supporting strategic decision-making in investment and client relations. Key challenges include managing reputational risks, data

sensitivity, regulatory compliance, and mitigating potential bias in AI outputs. Barriers to AI adoption involve high costs, resource needs, and regulatory complexities. While general-purpose AI brings substantial benefits in client interaction and operational efficiency, it also presents risks related to dependency and data management. AI solutions may be developed in-house, via external providers, or through collaboration (hybrid models), and asset managers are increasingly embedding AI compliance clauses in contracts with third-party providers.

4. AI Act

Paris Europlace notes that the constant evolution of artificial intelligence systems, correlated with the significant increase of use cases make the operational implementation of the AI law particularly complex, especially as the European Commission and European authorities have not yet published the expected implementing acts or guidelines.

This situation is creating uncertainty and apprehension for businesses, including financial institutions, as the first milestones in the implementation of AI occur on February 2, 2025, regarding AI mastery/literature (art. 4) and prohibited AI practices (Chap. II art. 5). This timetable does not allow establishments to wait for further clarification before starting their compliance. The entry into force of the AI Act in the already highly regulated financial sector raises questions and concerns for our members, who express a need for support from the national authorities to understand their expectations and have a homogeneous understanding of the text.

The main topics for which an expectation of accuracy is needed, to facilitate the preparation work for implementing AI Act in the financial sector are as follows:

1. Several definitions are subject to interpretation

- The **definition of AI** in the AI Act (consultation work in progress)
- The **content of Annex III** of the AI Act, on high-risk AI systems
- The context of **use of HR tools**
- The **terms "providers" and "deployers"** of AI solutions => focus on the context of the implementation of RAG (Retrieval-Augmented Generation)
- The ambiguity on **the scope covered by fraud** concerning high-risk uses

We note that a consultation is underway regarding the definition of AI and wish to express the strong expectation of financial market participants for the operational practicality of this definition which significantly complicate the efforts undertaken.

2. The ambition of the regulation highlights a pressing need for tools to support stakeholders on business issues

- Need for availability of tools, methodologies and benchmarks for the evaluation of General Purpose AI systems
- Need for codes of practice to be adapted to operational reality

3. Adherence to other texts: GDPR, FIDA; DORA, AML, ESG…

Furthermore, we would like to highlight the compliance challenges related to the integration of AI in financial activities such as credit scoring, risk assessment, fraud detection and automated customer services. In particular, the AI Act defines high-risk applications, especially for AI systems used in:

- **Creditworthiness assessments**: AI assesses consumer financial data to determine credit scores, potentially automating lending decisions)
- **Life and health insurance pricing**: AI evaluates risk factors such as medical history to customize premiums and detect anomalies in health data).

These applications require stringent oversight due to their significant impact on individuals' financial and health-related decisions.

We think that additional related functions, such as fraud detection, customer service automation, and claims processing, should not necessarily fall under high-risk AI but rather be classified as low-risk due to their supportive rather than decision-making nature. Similarly, claims processing focuses on operational tasks rather than risk assessment, and health engagement systems promote well-being without pricing insurance risks. Finally, policy recommendation systems assist in matching products to customer needs, serving as preparatory tasks that do not independently evaluate risks.

From a practical point of view, any AI applications, like chatbots, automated data entry, or fraud detection systems, are procedural or assistive, supporting human decision-making without autonomous impact. These applications are seen as low-risk ones and only indirectly influence credit or risk assessments.

As for supporting human decisions, AI tools that aid in tasks like underwriting assistance or compliance monitoring provide analytical insights without taking autonomous actions. The human review process remains central, and AI simply augments the quality and speed of these activities.

For example, fraud detection in financial services aligns more with operational oversight than with direct financial decisions, as these systems are primarily designed to detect and report irregular patterns rather than autonomously approve or deny transactions.

All in all, the broad definition of AI under the Act, which includes any machine-based system with autonomous capabilities, creates ambiguity. Traditional systems like regression models or rule-based algorithms might unintentionally fall under high-risk AI. Clearer distinctions, especially around autonomy, adaptiveness, and multi-purpose AI, are required to avoid overregulation.

Financial AI varies from fully autonomous trading models to systems requiring significant human oversight. Establishing clear criteria for what constitutes "significant autonomy" would help financial institutions determine compliance requirements accurately.

For example:

- **Documentation**: Standards for recording model assumptions, data sources, and decision rationales for example Human Involvement Standards which define the degree of human oversight necessary to mitigate potential AI errors or biases, especially in customer-facing applications with examples of human review process for high-risk applications.

- **Risk Classification Frameworks**: Establish criteria to differentiate AI by risk level based on function and impact.
- **Guidelines and best practices**: Develop guidelines and best practices for maintaining AI model robustness and to secure data handling, bias mitigation and the transparent use AI, particularly for sensitive data applications like health risk analysis.

Furthermore, we acknowledge the Draft General-Purpose AI Code of Conduct as a foundational document to guide providers and deployers of GPAI in aligning with the AI Act. Its framework addresses key compliance challenges, particularly in risk assessment, systemic risk mitigation, and governance. However, we express our concern regarding the publication of a final document early enough to allow companies sufficient time to comply before the regulatory deadlines next August.

Moreover, financial AI systems are already subject to regulations under GDPR, PSD2, and Basel III, creating a need for consistency to avoid redundant requirements. Guidelines should align AI Act compliance with the existing financial legislation. For example, the General Data Protection Regulation (GDPR) requires transparency in decision-making, a complex challenge for AI, especially with opaque models like deep learning. Similar transparency concerns arise with the Consumer Credit Directive (CCD), which mandates explainability in credit scoring.

Key articulation and clarifications via guidelines between the AI Act and the regulatory package of the financial institutions issued by the European Supervisory Authorities would thus be very welcome to ensure a smooth development of the AI in the financial sector.

Indeed, this lack of clarity induces challenges for financial AI Providers. AI development in finance requires flexibility and operational agility, but compliance with the AI Act's high-risk classification risks adding rigid layers of oversight, potentially stifling innovation and increasing operational costs. A risk-based approach should inform AI Act guidelines, ensuring financial institutions can integrate AI effectively while meeting regulatory requirements.

*

To conclude, the financial sector supports the AI Act's goals of responsible AI but calls for clearer, targeted and proportionate regulations that reflect the specific risks and roles of AI in finance, while not hurting competitiveness, nor impeding innovation. Tailored guidance will be critical to fostering AI innovation within the sector while ensuring transparency, fairness, and data protection.