Position Paper on the Artificial Intelligence Act

Executive Summary

The European FinTech Association (EFA) welcomes the European Commission's (Commission) legislative proposal on Artificial Intelligence (AI) to promote the development of AI in Europe. We support the efforts towards making Europe a global leader in trustworthy AI. However, the EFA would like to provide its recommendations on the following points:

1. **A clear definition of what is considered an AI system:** EFA believes that under the current scope the companies won't be able to fight fraud and maintain continuity of their transactions.
2. **Provisions on general purpose AI need to be re-considered:** The inclusion of general-purpose AI systems into the scope of the AI Act needs to be reconsidered to avoid unintended consequences and disproportionate regulatory burden especially for smaller providers in the financial services sector.
3. **The exclusion of tools facilitating the assessment of creditworthiness from the high-risks AI systems list:** Credit Worthiness Assessments needs to be excluded as a high-risk application to ensure European consumers can benefit from better, faster and cheaper financial services.
4. **A refined definition of "remote biometric identification system":** The AI proposal needs to acknowledge the differences between identification, verification and authentication.
5. **Clarifications for the requirements for "high-risk" AI systems:** Further clarification is needed on the AI systems of human oversight, risk management, data governance, record-keeping, transparency and provision of information.

EFA recommendations for the AI Act

EFA is committed to contributing to the proposal to ensure that the new regulatory framework is fit for purpose, and strikes a balance between safety and innovation. If designed properly, the EU regulation of innovative AI will facilitate further digitalisation andallow for a wide-scale uptake of AI across the EU, while most importantly protecting its citizens. However, we consider that in order to realise this shared goal, further improvements to the text are needed:

A clear definition of what is considered an AI system

The AI Act needs to be clearer in order to achieve the desired objective. The AI definition set out in the proposal is too broad and would include a vast amount of systems that may not always be considered AI per se.

This would be disproportionate and have a direct detrimental impact on incentives to invest and innovate, particularly by smaller companies. Similarly, the process to assess whether some AI systems should be considered high risk is only vaguely defined in Annex III, leading to uncertainty in terms of

product planning decisions. The definition of a "safety component" (Art. 3(14)) is a good example of this lack of clarity, as the definition refers to ambiguous concepts which are not further defined (e.g. "safety function"). Similarly, the definition used for "manipulative, exploitative and subliminal techniques" in relation to prohibited AI systems and the exact definition of a "bias" should be made explicit to avoid legal uncertainty.

Annex III presents a list of AI systems classified as high-risk. We as EFA see the need to further clarify the scope. This will prevent misinterpretation, and help to avoid the unintended inclusion of non-critical systems or ancillary use of AI systems that pose no safety risk. For example, the inclusion of "AI systems intended to be used to control or as safety components of digital infrastructure" (subsection (2)(b)) is overly broad and could include various different use cases such as cloud services, software, etc. The challenge for companies is to be able to fight fraud and yet also maintain continuity of their transactions, so they can continue to grow their business. Relying on a robust digital payments infrastructure is necessary for safety and fraud prevention, and does not carry the same risks as "AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity." (subsection (2)(a)).

Provisions on general purpose AI need to be re-considered

EFA is also of the view that the inclusion of general-purpose AI systems into the scope of the AI Act needs to be reconsidered. This could lead to unintended consequences and disproportionate regulatory burden especially for smaller providers in the financial services sector.

The scope of the proposed new rules is excessively broad and could impact current contractual business relations since they would redefine the regulatory burden between initial providers of general purpose AI systems and those companies that use these systems under their own brand.

There are invariably existing contractual commitments from the companies developing or providing general-purpose AI systems, as well as and, where appropriate, civil liability which apply to them should they cause any damage to third parties. Furthermore, there are always usage restrictions set out in the contracts between developing entities and the companies using them to provide services to end-users.

Tools facilitating creditworthiness assessments (CWA) should be excluded from the list of high-risks AI systems

Today, many innovative and efficient solutions are emerging that can provide more convenient creditworthiness decisions. For instance, AI-based use of credit applicants' relevant data by lenders is key to providing better, faster and cheaper financial services. This contributes to achieving a higher degree of financial inclusion and benefits EU consumers seeking to access credit in different EU countries.

We as EFA consider that AI systems for creditworthiness assessments (CWA) should be excluded from the list of high risk AI for their potential to disincentivise Fintechs and other financial firms to use this technology which has valuable consumer benefits.

As AI models are more accurate than human review they make fewer mistakes (e.g., less false positives and false negatives), resulting in the AI model offering a higher level of fairness to consumers. AI, in particular, facilitates the inclusion of individuals, or of and businesses, who were previously invisible to or underserved by credit markets, as well as risk management techniques. Algorithmic credit scoring also reduces lending costs and allows for the inspection and re-optimization of lending decisions[1]. Thus, the use of AI can actually help mitigate and reduce gender bias in Europe[2].

Further, we think this could bring about overregulation for fintechs and financial service providers, since the use of AI systems for creditworthiness assessments is already regulated and part of the supervisory regime in the EU[3]. In addition, several key stakeholders, including the European Central Bank (ECB), have stated that software that qualifies as a high-risk AI system is too broadly defined under the current proposal, causing rather simple statistical models to fall within the scope of the high-risk category and that such simple AI systems should not be classified as 'high-risk' when they are used to establish credit scores or creditworthiness [4].

The definition of "remote biometric identification system" needs clarification

We further see the need to more precisely target biometric use cases in the AI Act. Biometric data is often used for common security or fraud techniques such as detecting account takeovers through the detection of anomalous behavioural patterns.

The definition of "remote biometric identification system" needs to exclude from its scope verification and authentication as used commonly in financial services and payments. Identification, verification and authentication are three totally distinct types of activities with different use cases and risk levels associated. Biometric identification typically occurs without prior knowledge of the subject and in a public space, and is often associated with law enforcement.

In contrast, verification is used by businesses to ensure that the consumer is a real person, and then the person they claim to be on the basis of identity documents such as ID card, passport or driver's licence. This process helps businesses avoid falling victim to fraudsters and prevents malicious users from gaining access.

---

[1] Feedback from the Association of Consumer Credit Information Suppliers (ACCIS) on the European Commission's proposal for a Regulation laying down harmonized rules on Artificial Intelligence, 4 August 2021, p.4
[2] "Could AI help reduce gender bias in Europe?", Eline Chivot, Center for Data Innovation.
[3] Guidelines of the European Banking Authority (EBA) on loan origination and monitoring of 29 May 2020, para 4.3.4, p.26
[4] Opinion of the European Central Bank (ECB) of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (CON/2021/40) 2022/C 115/05, para 3.2

Authentication focuses on determining that the true account holder is making the transaction (with the use of codes, such as passwords, or specific questions for example). This improves customer service, and reduces fraud or cases of stolen identities.

These fundamental distinctions between identification, verification and authentication were recognised by the EU Commission itself in its AI White Paper of February 2020[5], and recently in a study for the JURI and PETI Committees of the European Parliament[6]. In the current draft of the AI Act, these very important nuances are lost, leading to ambiguity and legal uncertainty. This could lead to products that are designed exclusively to combat fraud falling within the scope of "remote biometric identification systems" and being subject to high-risk requirements or even prohibited. We must avoid this scenario to boost trust in AI and sustain vital elements of the broader consumer protection framework.

Furthermore, we must ensure that financial services, crypto platforms, and trusted marketplaces are able effectively combat one of the most common and damaging forms of fraud: bad actors creating multiple identities using the same credentials or face. In effect, an attacker may attempt to perform the remote identity proofing process several times using the same face but different identities in order to benefit from welcome offers, gifts, and rewards for signing up.

We understand the objective of the text is not to categorise such fraud prevention activity as high risk, which it clearly is not – but rather to focus instead on identification as used by authorities for mass surveillance in public spaces for example. It is therefore necessary to refine the definition to explicitly exempt such activities from the scope of the text.

The GDPR provides a sufficient regulatory framework for this type of processing, ensuring, for example, that a DPIA is performed and the necessary remediations are administered. Consequently, the EFA would urge the co-legislators to ensure that the definitions are clarified and explicitly exempt identity verification and authentication from the scope of the AI Act. This would provide legal clarity and ensure that important AI tools used by businesses to combat fraud and provide a safe business environment for consumers are not subjected to disproportionate rules.

The requirements for "high-risk" AI systems need clarification

According to the AI Act proposal, providers and users of "high-risk" AI systems will have to comply with strict obligations if they want to introduce or use AI systems, and will be subject to conformity assessments, specific management systems, and registration requirements.

[5] European Commission (2020), White Paper on Artificial Intelligence - A European approach to excellence and trust
[6] European Parliament Policy Department for Citizens' Rights and Constitutional Affairs (2021) Biometric Recognition and Behavioural Detection

Here, it is crucial to find the right balance between innovation and security: EU legislators need to ensure that the specific requirements are appropriate for the AI systems they apply to, and especially the set of requirements and obligations for 'high-risk' AI systems.In particular, we as EFA would like to see clarifications on the following points:

- **On human oversight (Article 14)**: The proposal suggests that "high-risk" AI systems shall be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which the AI system is in use". We as EFA are concerned that such a requirement will be disproportionate and that it will not contribute to reaching the goal of improving the accuracy of decisions. It should therefore be limited to certain evidence-based cases which effectively pose a high-risk to legal and natural persons, such as law enforcement surveillance.

- **On risk management systems (Article 9)**: The substantive requirements appropriate. However, similar to GDPR (Article 35) – which allows businesses to analyse the risks of their data processing, through a Data Protection Impact Assessment (DPIA – it seems useful to allow AI systems providers or users to explore ways to make the AI system less risky rather than thinking in terms of strict liability. We believe this would align incentives to increase security rather than just bringing about new compliance obligations. It is also necessary to provide a clear proportionate framework for this testing.

- **On data and data governance (Article 10):** The initial proposal of the European Commission suggests that "Training, validation and testing data sets shall be relevant, representative, free of errors and complete" (Article 10(3)). The debates in the Council as well at the European Parliament have already questioned whether that is possible or appropriate.[7] It seems more applicable to suggest that the data sets should be designed with the best possible efforts to ensure that they are relevant, and that the error rate is measured and assessed to be low enough for the intended purpose. Building an AI system is a long iterative process and we do not consider the current approach reflects the way AI systems are developed and built.

- **On record-keeping (Article 12):** The proposal suggests specific requirements for AI systems "intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons", classified as high-risk in paragraph 1, point (a) of Annex III. This may conflict with a desire to delete input data after a certain time, or even immediately after use, in order to ensure privacy and minimise security risks, and allowing the AI providers to delete the date after a

[7] The ITRE Committee recognised this through amendment 6, recital 44 of their Opinion on the AI Act (14.6.2022) which called for training, validation and testing data to be designed with "*the best possible efforts to ensure they are relevant, representative, free of errors and appropriately vetted for errors.*"

certain time according to their internal privacy policies seems more appropriate and practicable.

- **On transparency and provision of information to users (Article 13):** The text suggests that a certain degree of transparency should be required for AI systems classified as high-risk. They "shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured" (Article 13(1)). It would be useful to clarify how the transparency will be measured, and if individual decisions have to be explained in detail, as well as the level of details required. While transparency is key to ensuring trustit may not be practical to provide transparency that is meaningful to users, especially as it relates to fraud prevention.