ecri EUROPEAN CREDIT RESEARCH INSTITUTE

CEPS

AI and credit: Addressing the still open questions to prevent innovation paralysis

Explainer

Judith Arnal

Introduction: the benefits and risks of AI in the financial sector and in credit

Technological innovations in general, and AI in particular, hold great transformative potential for virtually all businesses. The financial sector is undoubtedly one of them, able to leverage AI to enhance analysis and prediction capabilities, automate processes, improve risk management and customer service, detect fraudulent operations, and even facilitate regulatory compliance. Although AI brings advantages, it can also amplify risks or pose new ones that should be addressed. A summary of the most relevant benefits and risks can be found below in Table 1.

Table 1: Benefits and risks of AI use in the financial sector.

Benefits and risks	Fraud detection	Quantitative analysis	Operational processes and compliance support	Risk management	Customer interaction	Cybersecurity
Benefits	Analysis of large amounts of data to detect patterns and anomalies that may indicate fraudulent activities.	Better extraction of information from (more) data.	Efficiency gains due to the potential for automating routine tasks and streamlining various financial processes, such as loan underwriting, account opening and claims processing. Compliance facilitation by analysing complex regulatory requirements.	Greater efficiency in risk assessment and capital and liquidity planning.	Better adaptation of product types to customer needs. Personalised financial advice. Improved customer service, such as chatbots providing 24/7 assistance.	Improvement in threat detection.
Risks	Bias and discrimination risks.	Technological challenges may reduce the robustness of predictions.	Overreliance on AI could make the operational system more fragile. Bias and discrimination risks.	Limited robustness may reduce the quality of risk assessment.	Data privacy issues if not managed correctly.	Low entry barriers for hackers and new forms of attack (e.g. deepfakes).

Source: Own elaboration based on ECB and OECD data.

According to a survey-based analysis by the OECD, banks are the financial firms currently experimenting with or deploying AI the most, followed by insurance firms and asset managers. According to the ESMA, AI is currently not widely used by financial market infrastructures. However, the use of AI in post-trading appears to be emerging. In terms of products and activities involving the use or experimentation of AI, banking products and payments – such as customer services, chatbots, client onboarding and fraud prevention – are the most relevant, followed by credit underwriting (e.g. credit scoring) and financial advice (e.g. robo-advisors and risk management).

Though financial stability risks do not currently seem to be a core issue, given the still relatively low use of AI for core activities, the future may be different. To keep track of possible risks to financial stability, it is necessary to closely monitor both the technological penetration and the concentration of AI system providers. There is a particular perception that increased levels of AI penetration in the financial sector, combined with the concentration of foundational model providers, will increase the likelihood that the AI decisions made by financial entities will be tainted by the same biases and technological challenges.

Still, given the nascent use of AI in the financial sector, this needs to be further investigated. Some respondents to the OECD's survey indicated that since AI models are not trained for black swans and tend to rely on similar databases, sudden market movements could exacerbate fire sales, bank runs or similar destabilising events. These elements will require heightened vigilance from macroprudential, microprudential and conduct supervisors.

Focusing specifically on creditworthiness assessments and credit scoring, AI also presents benefits and risks. Among the benefits, AI will enable more precise credit scoring systems, allowing (1) consumers to benefit from fairer credit assessments, thus fostering financial inclusion, and to have access to faster loan decisions; (2) lenders to improve the quality of credit thanks to more accurate credit risk assessments; (3) regulators to gain confidence in the accuracy of the model and its compliance with regulatory requirements; and (4) credit markets to become more efficient.

But risks are non-negligible: (1) the principle of interpretability is key in any AI system and, in some cases, AI models can be particularly opaque and function as a 'black box'; and (2) as with any other system, AI models, if not properly trained with the adequate data, can perpetuate or amplify historical discrimination patterns. AI systems rely on an enormous quantity of data and if said data is incomplete or inaccurate, the AI systems' outputs can be severely biased.

In any case, financial institutions and users of AI technologies in general are making substantial investments to ensure model fairness and robustness, as it is also in their interests to develop highly predictive and correct models that will bring long term benefits.

The EU's regulatory response: the AI Act

On 1 August 2024, the AI Act entered into force in the EU. The AI Act has broadly followed the OECD's definition of AI, referring to an AI system as a *'machine-based system designed to operate with varying levels of autonomy, 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'*.

A risk-based approach

The AI Regulation follows a risk-based approach, classifying AI systems into four different categories: unacceptable risk (e.g. social scoring systems), high risk (e.g. systems used in critical infrastructure), limited risk (e.g. chatbots), and minimal or no risk (e.g. spam filters).

The AI Act establishes two high risk use cases for the financial sector:

1. AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, except for those AI systems used for detecting financial fraud.
2. AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

Providers of high-risk systems will need to meet strict requirements regarding risk management, data quality, technical documentation, human oversight, transparency, robustness, accuracy and cybersecurity. Entities using these AI systems must operate them according to the detailed instructions provided by the supplier, ensuring that their use remains within the system's capabilities and limitations. Additionally, entities involved in credit rating or life and health insurance are obliged to conduct a fundamental rights impact assessment before deploying a high-risk AI system and to monitor for any risk to the fundamental rights of individuals all along the high-risk AI system's lifecycle.

Despite these two specific provisions in the AI Act affecting the financial sector, it is not deemed *lex specialis*, as it applies to many sectors. This means that the use cases of AI in the financial sector beyond the two classified as high risk will be dealt with in accordance with existing legislation.

The AI Act is largely a future-proofed piece of legislation, to the extent that it can be amended by delegated and implementing acts, for example to review the list of high-risk use cases in Annex III, which is where the cases for the financial sector fall.

Before the AI Act was adopted, national and EU financial authorities had already started issuing guiding documents. A few examples are a discussion paper by the Banque de France ACPR with their points of attention regarding the development and use of AI; a policy discussion paper by the Bundesbank on the use of AI and machine learning in the financial sector; the discussion paper on machine learning for IRB models by the EBA in November 2021 and the follow-up report of August 2023; EIOPA's AI governance principles of 2021; and the public statement by the ESMA in May 2024, on the use of AI when providing retail investment services and issuing initial guidance to investment firms utilising AI in light of their obligations under MiFID.

A staggered application timeline

The application of the different obligations included in the AI Act follows a staggered approach, in line with Table 2, with the first implementation deadline set for February 2025 and the last in August 2027. The European Commission has also launched the AI Pact, which encourages industry to voluntarily start implementing the requirements of the AI Act before they are legally applicable.

Table 2: Timeline for AI Regulation actions in the EU.

Relevant date	Action
2 February 2025	Prohibitions will begin to apply.
2 May 2025	Codes of practice should be ready.
2 August 2025	Obligations for general-purpose AI – including governance – will apply and sanctions will come into force.
2 August 2026	Obligations for high-risk systems in Annex III (including creditworthiness assessment systems) will apply.
2 August 2027	Obligations for high-risk systems in Annex II will apply.

Source: Own elaboration based on the AI Act.

A complex governance system

The AI Act establishes a two-tiered governance system, with national competent authorities overseeing and enforcing rules for AI systems, and the EU in charge of governing general-purpose AI models. Consistency will in principle be guaranteed by the European Artificial Intelligence Board, made up of high-level representatives from Member States and the European Data Protection Board (EDPB). The AI Office will be the Commission's implementing body for the AI Act, providing strategic guidance to the AI Board. Two advisory bodies will provide expert input, namely the Scientific Panel and the Advisory Forum.

The AI Act provides for the designation of one or more competent authorities to assume the role of market surveillance authority but it leaves the choice of the specific authority to Member States, which will need to appoint one or more authorities by 2 August 2025. On 17 July 2024, the EDPB adopted a statement, indicating that (1) national Data Protection Authorities (DPAs) should be designated as market surveillance authorities for high-risk AI systems used for law enforcement, border management, administration of justice and democratic processes; (2) Member States should also consider appointing DPAs as market surveillance authorities for other high-risk AI systems, taking into account the views of the national DPA, particularly where those high-risk AI systems are in sectors likely to impact natural persons rights and freedoms in terms of the processing of personal data; and (3) DPAs, where appointed as market surveillance authorities, should be designated as the single points of contact for the public and counterparts at both the Member State and EU levels.

For high-risk AI systems placed on the market, put into service or used by financial institutions regulated by EU financial services law, the market surveillance authority for the purposes of the AI Act will be the relevant national authority responsible for the financial supervision of said institutions. The AI Act also includes provisions on institutional coordination for credit institutions. It states that national market surveillance authorities overseeing regulated credit institutions and participating in the Single Supervisory Mechanism must promptly report to the European Central Bank (ECB) any information from their market surveillance activities that could be relevant to the ECB's prudential supervisory responsibilities.

A wide territorial scope

The AI Act has a wide territorial scope, as it applied to: (1) providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are located or established within the EU; (2) uses of AI systems either located in or with establishments in the EU; (3) providers of AI systems that are located in or with establishments in a non-EU country, where the output produced by the system is used in the EU; (4) importers and distributors of AI systems; (5) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; (6) authorised representatives of providers, which are not established in the EU; and (7) affected persons that are located in the EU.

Open questions and assessment

The Commission has conducted a targeted consultation on the use of AI in the financial services sector. This is a positive move which will hopefully clarify several open questions that may be stalling new business opportunities and governance decisions by financial institutions.

Open questions that lead to regulatory uncertainty – what is classified as AI?

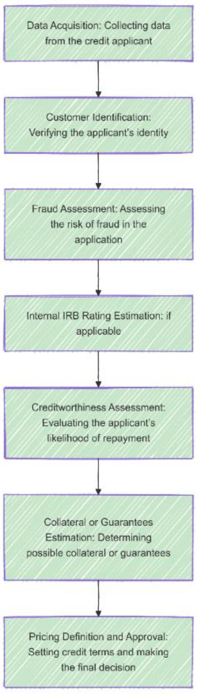
The implications of the AI Act for the financial sector are a clear example of regulatory uncertainty. In the particular case of AI and credit, open questions remain as to what will be classified as AI. Specifically, some argue that traditional statistical techniques, such as logistic regression models, should be classified as AI and fall under the high risk category of the AI Act, to the extent there is a risk of discrimination. Nevertheless, such an approach would be inconsistent with an adequate interpretation of the AI Act, which follows a clear staggered approach, first defining whether a system is AI and in case of a positive answer, then including it in one of its risks classifications. Against this background, logistic regression models, which have been used for a number of decades, should not be classified as AI. Moreover, discrimination risks have already been duly catered for in sectorial legislation and financial regulators like the EBA and the ECB.

Open questions that lead to regulatory uncertainty: what part of the loan origination process falls under the category of creditworthiness assessment or credit scoring?

There is still regulatory uncertainty regarding the loan origination process that will fall under the category of creditworthiness assessment or credit scoring. Typically, an end-to-end origination process is based on seven steps, as shown in Figure 1. Of these seven steps, only the fifth step (the creditworthiness assessment) corresponds to the credit capacity assessment and should thus be considered as creditworthiness and credit scoring. If AI were to be used as part of this step, the AI Act provisions for high-risk use cases should be applicable.

These provisions should, however, not be applicable to the rest of the loan origination process – even if AI is used. More specifically, Step 4 should also be excluded considering Recital 58 *('AI systems provided by Union law (…) for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation'*). It is urgent that clarity is provided on this as soon as possible.

Figure 1: End-to-end loan origination process.


Data Acquisition: Collecting data from the credit applicant
Customer Identification: Verifying the applicant's identity
Fraud Assessment: Assessing the risk of fraud in the application
Internal IRB Rating Estimation: if applicable
Creditworthiness Assessment: Evaluating the applicant's likelihood of repayment
Collateral or Guarantees Estimation: Determining possible collateral or guarantees
Pricing Definition and Approval: Setting credit terms and making the final decision

Source: Own elaboration.

A burdensome regulatory framework that puts technological neutrality at risk

The AI Act's implications for the financial sector are a clear example of the regulatory burden the sector needs to cope with, having to simultaneously implement vertical (financial sector specific) and horizontal legislation (e.g. the AI Act or the GDPR). Indeed, the financial sector will need to follow AI Act provisions for the two cases identified as high risk, implementing pre-existing legislation for all other use cases. This implies that for robo-advice, the Consumer Credit Directive, the Mortgage Credit Directive, the Markets in Financial Instruments Directive (MiFID) and the Insurance Intermediation Directive (IDD) will all need to be applied, depending on the specific financial sub-sector; the Capital Requirements Regulation will be relevant for provisions on risk management in relation to credit risk assessment; the Payment Services Directive for fraud prevention; the Anti-Money Laundering Directive for AML risk use cases; the Market Abuse Regulation for market abuse detection use cases; Solvency II and institutions for occupational retirement provisions (IORPs) for risk management in relation to insurance risk assessment; MiFID for algo-trading and High Frequency Trading; and the Digital Operational Resilience Act (DORA) for operational resilience.

The vertical regulatory approach is understandable, to the extent it is aligned with the principle of technological neutrality and is shared by most other advanced jurisdictions. Indeed, non-EU OECD jurisdictions broadly tend to consider existing financial regulation, laws and guidance as adequately covering financial activities regardless of the technology used and whether the decision came from AI, traditional models or humans. This is consistent with the view that up to now, AI has not created new risks but rather intensified some existing ones. Nevertheless, to the extent the AI Act flags two specific financial sector AI use-cases as high risk, the principle of technological neutrality could be at risk.

And most importantly, the financial sector could struggle to deploy both basic statistical models and AI systems due to how EU judicial authorities are interpreting the GDPR. A landmark ruling issued by the General Court on 7 December 2023, also known as the SCHUFA case, clearly highlights this. The General Court concluded that if a credit information agency automatically establishes a probability value based on personal data relating to a person and concerning their likely ability to meet payment commitments in the future, then it would constitute 'automated individual decision-making' within the meaning of Article 22(1) GDPR.

As argued previously in this other CEPS-ECRI piece, the institution that made the decision not to grant credit was the bank and not SCHUFA itself. Whether the bank only used the information transmitted by SCHUFA to make its decision should not have a direct impact on SCHUFA's business and methodologies. Unless a legal basis to allow for the application of Article 22(2)(b) was deemed applicable, this ruling could severely hinder technological progress for assessing natural persons' creditworthiness, which will ultimately lead to worse lending practices. Moreover, this Court decision will most likely lead to (negative) spillover effects for automated processes in the EU. This decision not only risks shaking up SCHUFA and other credit reference agencies' business model, potentially forcing them to reassess and adjust their practices to ensure their alignment with the GDPR, but its implications could well span across a range of businesses that use algorithms to make decisions, e.g. healthcare, insurance or employment, among others.

All this calls for the need to clarify regulatory practices, catering for real risks but avoiding an overly restrictive interpretation that will only deter innovation in the EU.

A fragmented governance system that risks damaging the level playing field

Regarding the AI Act, there will be a variety of institutions involved implementing it, with national competent authorities overseeing and enforcing rules for AI systems. The fact that such an important task will be implemented at national level creates unlevel playing field risks. And these are relevant risks, that have indeed already materialised in the AI field, in relation to data protection. Indeed, the EU's data protection governance architecture is very complex, leading to contradictory interpretations depending on the Member State. In many cases, the GDPR's provisions are vague and to some extent ambiguous, leading to a need for interpretation. This is where the EU's complex data protection governance comes into play.

Each EU Member State has its own data protection authority, which already means 27 potentially different interpretations, with 16 individual data protection authorities per German state on top. And finally, data protection law applies beyond the EU, also including Liechtenstein, Norway and Iceland, i.e. the European Economic Area. This leads to 46 potentially different views. Although coordination mechanisms exist under the European Data Protection Board (EDPB), they often do not work. Indeed, according to the European Commission's second report on the implementation of the GDPR, market participants indicate that (1) data protection authorities in three Member States have a different view on the appropriate legal basis for processing personal data when conducting a clinical trial; (2) there are often divergent views on whether an entity is a controller or processor; (3) in some cases, data protection authorities do not follow the EDPB guidelines at national level; and (4) these problems are exacerbated when multiple data protection authorities within the same Member State adopt conflicting interpretations.

This situation is leading companies of all kinds to halt transformative projects in the EU. The case of Meta is paradigmatic – both the UK and the EU have the same regulation (GDPR) but the UK has been relatively quick to consider that Meta can train its generative AI model using first-party public data shared by Instagram and Facebook users under the legal basis of legitimate interest, while the EU has yet to reach a clear position. This has led Meta to halt its project in the EU. These barriers to regulatory implementation may be even more damaging for startups, which have fewer resources that they can dedicate to navigating through an uncertain regulatory framework.

In this context, the EDPB's request to designated DPAs as market surveillance authorities for high-risk AI systems should be disregarded by Member States. Indeed, for financial high-risk use cases, Member States should not deviate from the general provision of appointing financial National Competent Authorities. Regarding all other use cases, it is probably more sensible to create a new dedicated AI authority. A possible benchmark is the Spanish *Agencia Española de Supervisión de Inteligencia Artificial* (AESIA). The AESIA stands out as a valuable benchmark due to its targeted approach and specialised focus on AI governance. Unlike other institutions, AESIA is designed specifically to address the unique challenges posed by AI systems. Its establishment reflects a proactive effort to centralise expertise, ensure consistency in enforcement and reduce the fragmentation risks that arise when multiple authorities handle overlapping responsibilities.

Conclusions

While AI offers significant opportunities for the financial sector to improve efficiency, risk management and customer service, the regulatory uncertainties introduced by the EU's AI Act could inhibit its full potential. The Act's risk-based approach, coupled with overlapping horizontal and vertical legislation, poses complex compliance challenges, particularly for credit assessments and scoring.

To prevent innovation paralysis, it is essential to clarify these regulatory ambiguities and ensure harmonised implementation across Member States. Achieving a balanced regulatory framework will enable the financial sector to leverage AI responsibly, fostering innovation while safeguarding stability and consumer rights.

European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

ecri
EUROPEAN CREDIT RESEARCH INSTITUTE

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.

CE
PS