Finance Watch

Making finance serve society

Protecting EU consumers in the age of AI-driven retail finance

Policy proposals to close regulatory gaps and address emerging risks

A Finance Watch Report

July 2025

Author: Peter Norwood
Editor: Robert Nosker
Graphics and typeset: Camila Dubois
Cover photo: Adobe Stock

Acknowledgement: The author would like to express his thanks to the members of Finance Watch for their valuable input and comments and to his colleagues at Finance Watch, who contributed to this report by sharing their thoughts and experiences.

Finance Watch has received funding from the European Union to implement its work programme. There is no implied endorsement by the EU or the European Commission of Finance Watch's work, which remains the sole responsibility of Finance Watch.

Co-funded by the European Union

Contents

Executive Summary

The world is witnessing an increasing mainstream commercial adoption of artificial intelligence (AI). The retail financial services sector also forms part of this trend, with financial institutions in the European Union (EU) and beyond increasingly deploying AI for processes involved in the provision of financial services, such as risk assessment and pricing of insurance, and creditworthiness assessments for the sale of personal loans.

The use of AI in the retail financial services sector undeniably yields efficiency gains and cost reductions for financial institutions. In addition, it can bring with it benefits and opportunities for consumers, such as speedier sales processes and, if properly regulated, improved customer services. For example, AI can enable financial institutions to provide customer assistance around the clock with the help of well-functioning chatbots. However, AI also entails major consumer risks that need to be properly mitigated by appropriate and robust regulations.

This report serves as a follow-up to the March 2025 Finance Watch publication on AI in the financial services sector. It focuses on the consumer dimension of AI deployment in financial services. It identifies the risks AI poses for consumers and examines whether the existing regulations applying to retail financial services in the EU are sufficient for addressing the risks that stem from the use of AI in the sector, or whether there are important regulatory gaps that need to be filled. By doing so, the report explores what regulatory provisions are needed to ensure that AI is safely deployed in the retail financial services sector, allowing consumers to reap AI's many benefits without being exposed to harm.

The use of AI in financial services brings risks for consumers, ranging from exclusion from essential financial services, such as bank accounts or insurance, to exposure to unfair price discrimination and the mis-selling of risky financial products, which can lead to financial detriment. These risks hit vulnerable consumers the most and can lead to a lack of societal trust in both AI and the financial sector.

Existing horizontal consumer law in the EU, such as the Unfair Commercial Practices Directive (UCPD) and the General Data Protection Regulation (GDPR), includes rules that help mitigate some of the abovementioned consumer risks. For example, the UCPD bans aggressive marketing techniques facilitated by AI. Similarly, sectoral financial services legislation (e.g. the Consumer Credit Directive [CCD] and Distance Marketing of Financial Services Directive [DMFSD]) includes some important provisions. For instance, the DMFSD rules provide consumers with a right to human intervention when firms use online tools, such as chatbots, to provide explanations about financial products.

However, most of the existing EU legislations that apply to the use of AI systems in the retail financial sector were approved at a time before AI systems even existed or were widely used. As a result, they do not sufficiently protect consumers from the challenges and risks that AI brings.

The EU AI Act, which was adopted in June 2024 and will become applicable in August 2026, introduces rules that would fill many of the key regulatory gaps in the existing EU regulatory framework for retail financial services with regards to the fair and safe use of AI. It introduces regulatory requirements tailored to the specific risks of AI, including requirements on data governance, risk management, record-keeping and human oversight. However, only two financial sector applications (i.e. the assessment of creditworthiness of natural persons and the risk assessment and pricing of life and health insurance) are deemed "high-risk" under the EU AI Act and are, as a consequence, subject to specific requirements and enhanced supervision. Therefore, there is an urgent need to broaden the list of high-risk applications to all retail financial services under Annex III of the EU AI Act.

In addition, there is a need to update sectoral consumer financial services legislation to introduce a number of rules addressing risks that are unique to financial services and/or require tailored solutions that cannot be adequately addressed in the EU AI Act, given its cross-sectoral/horizontal scope of application. For example, because AI enables highly granular risk assessments in the area of insurance, there is a need for rules in the Insurance Distribution Directive (IDD) that clearly stipulate how data accessed for risk assessments and pricing of insurance may be used in order to avoid excessive granularity that undermines the risk-sharing principle of insurance.

Finally, given AI systems' lack of explainability, it is difficult, and in some cases impossible, for consumers to easily seek redress when damages are caused by the use of AI by financial institutions, as existing civil liability regimes are not tailored to the unique challenges stemming from AI. Thus, an EU-harmonised AI liability regime must be urgently introduced that addresses the transparency and explainability challenges of AI outputs, including by reversing the burden of proof in favour of the individual claimant when seeking redress.

Implementing the above-mentioned policy recommendations would ensure that AI can be employed in the financial sector in a safe way, while still yielding efficiency and productivity benefits for financial institutions, as well as unlocking opportunities for consumers. The current policy debate, however, is increasingly wrongly considering the introduction of new regulations in the area of AI deployment as an administrative burden that would stifle innovation and undermine competitiveness. For example, at the AI Action Summit in February 2025, European leaders shifted focus away from ensuring AI safety towards competitiveness and deregulation, prompting the European Commission to withdraw its AI Liability Directive (AILD) proposal shortly thereafter.

In consideration of the implications of the consumer risks highlighted in this report, having the proper safeguards in place to ensure that AI used in retail financial services does not harm consumers is necessary not only to ensure consumer protection but also to meet the EU's competitiveness goals. For AI to be adopted and financial institutions to be competitive, societal trust in AI and in the wider financial system is needed. Therefore, implementing the right regulation of AI and promoting its development and uptake in the EU go hand-in-hand and must be pursued in parallel; they must not be seen as being in opposition to each other.

Key Recommendations

1 Designate AI systems used in the provision of all retail financial services as high-risk under the EU AI Act.

2 Update sectoral consumer financial services legislation to introduce rules that address risks unique to financial services and/or require tailored solutions that cannot be adequately addressed in the AI Act given its cross-sectoral/horizontal scope of application.

3 Introduce an EU-harmonised AI liability regime that allows consumers to easily seek redress in cases where damages are caused by the use of AI by financial institutions.

I. Key risks to consumers associated with the use of AI in retail financial services

Firms operating in the retail financial services market have been increasingly adopting AI. A report by the European Insurance and Occupational Pensions Authority (EIOPA) shows, for example, that AI is used by 50% of non-life insurers and 24% of life insurers in the EU, with many more expected to use AI in the near future.[1] The main use cases of AI systems in the retail financial services sector are as follows:

- Customer due diligence (know your customer [KYC]) process when a consumer wants to open a new bank account
- Creditworthiness assessments of clients when granting consumer credit and mortgages
- Risk assessments and pricing for insurance
- Claims management in insurance
- Automated investment advice and portfolio management for retail investors (also called *robo-advice)*
- Assessment of suitability and appropriateness in the area of retail investments
- Using chatbots to reply to customer queries or provide assistance

The use of AI in the retail financial services market brings with it efficiency gains and cost reductions for financial institutions. For consumers, AI use may translate into speedier processes when concluding contracts. However, if not properly regulated and supervised, the use of AI tools in the consumer financial services market brings considerable risks.

A. Financial exclusion risks

Financial exclusion is a key risk associated with the use of AI systems in the retail financial services market. As mentioned above, AI systems are increasingly used for the customer due diligence process (know your customer) and to create customer risk profiles when a potential customer wants to open a bank account. However, if the AI algorithm used for this process is biased, this can lead to a potential consumer unfairly being denied the right to open a bank account. **AI models can be biased** if they are trained on data that reflect historical patterns of discrimination or disparities.

A commonly cited shortcoming of AI systems used for anti-money laundering purposes is that they are prone to produce *false positives*[2] that affect vulnerable consumers, such as migrants and people with low incomes, the most. However, access to a bank account is crucial to carrying out essential transactions needed to participate in social

1 EIOPA, *Report on the digitalisation of the European insurance sector*, April 2024.

2 Stiefmueller C. , The Soul of a New Machine: Promises and Pitfalls of Artificial Intelligence in Finance, January 2022.

and economic life, such as receiving a salary or social benefit, paying rent or paying taxes. Thus, unfairly excluding someone from accessing a bank account, which is an essential basic financial service, means excluding them from being able to access any other financial products and to be socially excluded.

Another prominent way that AI systems can lead to financial exclusion is linked to the deployment of AI systems in assessing a potential client's creditworthiness (CWA), which is done when a consumer wants to take out a personal loan or mortgage. There is a risk of **errors or biases** in the AI models used for the assessment, which can lead to **incorrect or discriminatory outcomes** and someone being wrongly denied a loan and/or mortgage.

Finally, in the insurance sector, the use of AI systems for risk assessments and pricing of insurance risks leaving swathes of vulnerable consumers being **denied insurance coverage** or being faced with prohibitively **high insurance premiums**. Since its establishment, the insurance business model has been built on solidarity or risk pooling, which has allowed potentially vulnerable consumers with higher risk profiles to still be able to afford insurance (i.e. be insurable), as the risk is spread out collectively across policyholders. The increasingly powerful algorithms of AI systems, however, enable highly granular risk assessments (i.e. highly personalised pricing), which endangers this business model. AI deployed by insurers sometimes also uses proxy data for sensitive data for insurance pricing, which can result in discriminatory outcomes. Research by the UK consumer association Citizens Advice shows, for instance, that postcode data which correlates with ethnic origin is used by AI systems, resulting in discriminatory insurance pricing.[3] In addition, as in the case of CWAs, there is a risk of errors or biases in the AI model or in the data it relies on, which can produce incorrect or discriminatory outcomes.

B. Mis-selling risks

The use of AI in the financial sector also carries with it risks of mis-selling, which can result in financial detriment for consumers. The key areas in which these risks are relevant for citizens are retail investments and consumer credit.

When providing personal recommendations in the field of retail investments, firms are required to carry out suitability and appropriateness assessments to identify products suitable for prospective clients. Errors in the models or data that AI models rely on can result in **bad suitability and appropriateness assessments** if firms use AI systems when selling investment products. This, in turn, can lead to financial institutions recommending clients retail investment products that are not suited to the client's risk tolerance and ability to bear losses.

Given that retail investment products are risky, the mis-selling of these products can potentially entail **significant losses** for consumers – in some cases, consumers could

3 Citizens Advice, *Discriminatory pricing: Exploring the 'ethnicity penalty' in the insurance market*, March 2022.

lose all of the money they have invested. Research conducted by Better Finance, for example, shows that the investment advice provided by AI systems (robo-advisors) is often inconsistent with investors' risk profiles. In addition, the study indicates that there are strong divergences in asset allocation and expected returns for the portfolios suggested by different robo-advisers for exactly the same investor profile.[4]

Furthermore, creditors' use of AI systems for the purpose of conducting creditworthiness assessments (CWAs) when determining whether to sell a loan and/or mortgage to a consumer can result in **unaffordable loans/mortgages** being offered to consumers who are unable to repay. A proper CWA is based on data relevant to analysing the borrower's financial capacity to repay the loan offered. This includes data on the consumer's income, essential expenditures and ability to manage their budget, including their credit and debt instalments. If the wrong data is used for a CWA, however, it can lead to consumers being sold a loan they cannot afford. This, in turn, can lead to and exacerbate over-indebtedness, which brings with it not only economic hardship for the affected consumer but also physical and mental health issues. It is also a strain on a country's economy as a whole due to loss in production and rising costs for social welfare systems.[5]

C. Exposure to price optimisation practices

The use of AI systems in the consumer financial services sector also facilitates price optimisation practices, i.e. practices where, with the help of algorithmic tools, firms set prices that are **not based on justified criteria**, such as the individual's level of risk with regards to insurance, but on their price sensitivity (willingness to pay more). In the insurance sector, for example, this could manifest in assessing whether consumers tend to switch general insurance products, such as home or motor insurance, at renewal or tend to hold them for long periods of time and are thus unlikely to react to price rises and shop around. It can also mean determining someone's likelihood to pay more based on **non-risk-based factors**, such as income, level of education and the type of device used to purchase the insurance (e.g. the brand of their smartphone, tablet or desktop computer), location, downloaded apps, etc.[6] Data from the EIOPA show that firms are increasingly using price optimisation practices for popular insurance products, including accident, health, household and motor insurance.[7] A survey by the UK consumer organisation Which? shows that 6 in 10 (60%) car insurance policyholders found their premiums rose when they last renewed or switched their insurance policy, with 1 in 7 (15%) noting that it rose "significantly".[8]

---

4 Better Finance, *Robo-advice 2022 Report - Breaking Barriers of Traditional Advice*, April 2023.

5 R. Ahlström et al., The Swedish Consumer Agency, Report, Is debt relief rehabilitative?, 2014.

6 EIOPA, *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*, 2021.

7 EIOPA, Consumer Trends Report 2023, 2023.

8 Which?, *Despite insurance 'loyalty penalty ban', existing customers are still being disadvantaged versus new customers, Which? finds*, 2024.

D. Unfair denial of insurance claims

In addition, errors or biases in AI systems or the data on which they rely can lead to the unfair denial of insurance claims or to lower-than-expected compensations for claims. Numerous examples of this in recent industry practice exist. For example, the fatal shooting of UnitedHealthcare CEO Brian Thompson led to public scrutiny of insurers, which reveals that major insurers in the United States have used biased AI models that unfairly deny insurance claims.[9]

A lawsuit filed against UnitedHealth in 2023 revealed that 90% of the recommendations of the algorithm used by the insurer for insurance claims, known as nH Predict, were reversed on judicial appeal.[10] Moreover, US insurer Cigna faced legal action over its use of a separate **biased algorithm** to unfairly reject insurance claims. A complaint against Cigna alleged that the insurer relied heavily on the automated system and allowed claims to be denied without conducting any reviews of individual patient files.[11]

E. Transparency/explainability of outputs of AI systems and the ability to seek redress

Another significant challenge concerning the use of AI in retail financial services is with regard to *the black-box nature* of many AI models. AI systems are increasingly complex, especially those based on neural networks and deep learning, and have become increasingly complex.[12] Their decision-making processes are often **opaque**, making it difficult to understand how they arrive at the outcomes and decisions they generate. This, in turn, makes it difficult for consumers to establish a legal ground on which to base a potential complaint, let alone obtain documentary or other factual evidence to support it.

9 U.S. Senate Permanent Subcommittee on Investigations, *Refusal of Recovery: How Medicare Advantage Insurers Have Denied Patients Access to Post-Acute Care*, October 2024.

10 Gil, B. *How United Healthcare and other insurers use AI to deny claims*, Quartz, December 2024.

11 Ibid.

12 EU Supervisory Digital Finance Academy (EU-SDFA), *Digital Finance in the EU: Navigating new technological trends and the AI revolution*, April 2025.

II. Existing EU regulations applying to AI deployed in the retail financial services sector

There are a number of horizontal (cross-sectoral) and sectoral legislations in the existing EU acquis, which include rules that apply to AI deployed in retail financial services.

A. EU AI Act

In June 2024, the EU adopted legislation governing the use of AI in the EU. Known as the EU AI Act,[13] which will become applicable in August 2026, this piece of legislation aims to address the challenges of AI.

The EU AI Act introduces a **risk-based framework** with four levels of risk identified for AI activities, ranging from **"minimal" to "unacceptable risk"** and different rules applying to each level. AI activities that are classified as **"high-risk"** are subject to robust regulations and enhanced supervision to ensure that AI-assisted systems are free from fault or unlawful biases. As to activities in the financial sector, however, only AI systems carrying out risk assessment and pricing for life and health insurance and the assessment of creditworthiness when selling loans and mortgages to consumers are classified as "high-risk". Thus, critical activities such as customer risk assessments for anti-money laundering (AML) purposes to open a bank account, the risk assessment and pricing for most general insurance products (e.g. motor and home insurance) and the use of AI systems in suitability and appropriateness assessments for retail investors are not classified as high-risk. The provisions applying to high-risk AI systems in the EU AI Act that are particularly important for the deployment of AI systems in the retail financial services sector are as follows:

- Data governance rules (Article 10) to ensure that data used by the AI system is of high quality and unbiased
- Human oversight requirements (Article 14) to ensure that high-risk AI systems operate as expected and that adjustments are made when performance deviates from intended outcomes
- Rules requiring organisations to have a risk management system in place (Article 9) to monitor, assess and mitigate any risks associated with high-risk AI systems
- Record-keeping requirements (Article 12) to allow, among others, a proper and robust supervision of AI systems and their outputs by supervisory authorities

AI applications that are not classified as high-risk are merely subject to a requirement to inform the client that they are interacting with an AI system (e.g. if a financial institution uses a chatbot) and AI users (e.g. financial institutions) must ensure AI literacy among their staff. Applications in the retail financial sector that are not deemed "high-

13 See the *EU AI Act*.

risk", however, continue to operate subject to sectoral financial services legislation, as further expounded on in Section III. c. below.

B. Cross-sectoral consumer legislation

In addition to the EU AI Act, certain cross-sectoral consumer protection laws apply when AI is used in the retail financial services sector. Major pieces of consumer legislation falling into this category include the Unfair Commercial Practices Directive (UCPD) and the General Data Protection Regulation (GDPR).

The **UCPD bans misleading practices** that rely on information that is false, deceptive and "causes or is likely to cause [the consumer] to enter into a transaction that he would not have taken otherwise".[14] This rule also applies to AI; thus, in practice, if AI is used to generate false or deceptive information (e.g. in advertisements for retail financial services), it could be considered a misleading commercial practice. Thus, AI used, for example, to generate targeted personalised advertising that misrepresents a product is banned.

In addition, the UCPD bans **aggressive practices**, regardless of whether AI is used for these purposes, that "significantly impair the average consumer's freedom of choice or conduct".[15] Thus, AI-driven techniques used to pressure consumers into making decisions (e.g. pressuring them into buying a certain financial service/product) by, for example, push notifications would constitute an aggressive commercial practice and are banned.

The GDPR applies to the use of AI in the retail financial services sector to the extent that AI **processes personal data**. The same GDPR principles that apply to financial institutions when processing data without the use of AI also apply when AI is used. This means in practice that the following key principles of the GDPR also apply when financial institutions use AI:

- Purpose limitation: Any data collected by the AI system for a specific purpose (e.g. a CWA) cannot be further processed in a manner that is incompatible with those purposes unless the individual consents.
- Data minimisation: Data processed must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[16] This means in practice that AI systems in the financial sector should only collect and process personal data that are relevant and necessary for the use case. However, the **GDPR does not specify** which specific types of data are, in fact, relevant for the different use cases under which AI processes personal data within the consumer financial services sector.

14 Article 6 of the UCPD

15 Article 8 of the UCPD.

16 Article 5 of the GDPR.

- Data accuracy: Any data processed by an AI system used by a financial institution should be accurate and up-to-date.

Interestingly, the GDPR also has explicit rules on automated decision-making (Articles 21 and 22). Article 21 provides citizens with a right to object to profiling based on personal data, and Article 22 stipulates that citizens have the right "not to be subject to a decision based solely on automated processing, including profiling". However, in both cases, **exemptions apply** where the practice "is necessary for entering into, or performance of, a contract".[17] This means that in effect, the GDPR does not apply to the use cases for which profiling is used in financial services (e.g. CWAs, risk assessment and pricing for insurance, and KYC processes).

C. Sectoral financial services legislation

AI systems used in the retail financial services sector are also subject to relevant sectoral legislation. Key legislation in this area includes the Insurance Distribution Directive (IDD), the Markets in Financial Instruments Directive (MiFID II), the Distance Marketing of Financial Services Directive (DMFSD)[18], the Consumer Credit Directive (CCD), the Mortgage Credit Directive (MCD) and the AML Directive (AMLD 5). The principle of technology neutrality applies to sectoral EU financial services regulations. This means that the use of AI by financial institutions to deliver or support financial services is subject to established sectoral rulebooks. Most of these rules, however, were promulgated **before the introduction of AI** and therefore do not expressly mention the term and are not tailored to its specific characteristics and associated consumer challenges. Only the revised versions of the CCD and DMFSD, which came into force in 2023 and will become applicable starting in 2026, refer to AI systems specifically and include rules addressing the use of AI in retail financial services delivery.

The rules in the revised CCD specifically addressing the use of AI in the provision of consumer credit concern the processing of personal data for the purposes of **personalised pricing** as well as to carry out **creditworthiness assessments** for prospective clients. When personalising the loan interest rates of consumer credit offers on the basis of automated decision-making, creditors must clearly inform consumers that the price presented to them is personalised through the automated processing of their personal data. In addition, creditors and credit intermediaries are required to inform consumers who receive a personalised offer of the sources of data used to personalise the offer.

Moreover, the revised CCD includes several rules addressing the risks associated with the use of AI systems to perform CWAs. According to Article 18, the consumer has the right to obtain human intervention on the part of the creditor if AI is used to conduct a CWA. The consumer is provided the right to obtain from an employee

17 Article 22(2) of the GDPR.

18 The DMFSD will be repealed, and a revised version of its rules merged with the Consumer Rights Directive from June 2026.

a meaningful and comprehensible explanation of the assessment made and of the functioning of the AI system used, including the main variables, the logic and risks involved. The consumer also has the right to express their point of view and to **request a review** of the assessment and the decision on whether to grant credit.

The revised DMFSD rules directly address the use of AI systems in the provision of pre-contractual information. Article 16d provides consumers with the **right to request human intervention** when AI systems, such as chatbots or robo-advisors, are used to provide explanations about a financial service/product before purchase. Moreover, the revised DMFSD includes rules that apply when financial institutions use AI systems to personalise the prices of offers, including when differentiating prices between different consumer groups and adapting the price to consumers' individual price sensitivity. Before they are bound by a distance contract, consumers must be informed that the price of the financial service is personalised on the basis of automated decision-making.

In conclusion, while there are rules in the existing regulatory framework of consumer financial services that apply to the use of AI in this sector, most of this legislation was not drafted with the deployment of AI and its unique risks to consumers in mind and therefore contains only a few, if any, rules specifically tailored to the use of AI in the retail financial sector. Given these circumstances and the fact that the EU AI Act subjects activities linked to only a limited number of retail financial services to robust regulatory rules, there is an **urgent need** to assess whether the existing EU horizontal and sectoral regulatory framework applied to consumer financial services is sufficient to adequately protect consumers from the risks linked to AI. The next section of this report will explore this issue and identify any existing regulatory gaps that may need to be addressed.

III. Gaps in existing EU legislation

This section of the report explores which specific regulatory gaps remain that need to be filled to ensure that consumers are adequately protected from the risks emanating from the use of AI in the financial sector.

A. Rules equivalent to the provisions applied to high-risk AI applications in the EU AI Act

The important provisions regulating high-risk AI systems contained in the EU AI Act, in particular with regards to **data governance, human oversight, risk management and record-keeping**, are not included in any of the other horizontal or sectoral pieces of legislation covering consumer financial services. While there are provisions in sectoral legislation covering aspects such as risk management or record-keeping, these provisions apply to the business in general and are not tailored to the **unique characteristics of AI**, as these rules were designed **before AI systems emerged** and were deployed in the financial sector.

EU policymakers, at the time of writing this report, were considering drafting guidelines/guidance that set out how sectoral legislation should be interpreted in the context of AI systems to ensure a responsible use of AI systems.[19] The thinking is that by implementing these guidelines/guidance setting out how existing sectoral rules (e.g. with regards to risk management) should be interpreted and applied to AI systems, sectoral rules can replicate many of the key provisions applying to high-risk AI applications in the EU AI Act. However, this approach is **not sufficient** to adequately protect consumers.

For one, **guidelines and guidance are not legally binding** and therefore are at risk of not being properly and widely adhered to. Given the significant risks for consumers stemming from the use of AI systems in the provision of retail financial services (as explored in Section 2), it is crucial that regulatory rules for AI deployed in the retail financial sector are in place that are properly followed and enforced.

In addition, not classifying the application of AI in the provision of all retail insurance products and bank accounts as high-risk renders the EU AI Act **inconsistent** with its goal of preventing AI systems from posing a risk to consumer access to essential private services and benefits. The unfair denial of essential financial services, which includes all insurance products and bank accounts, has significant negative impacts on a person's economic and life prospects. As mentioned in Section II, the denial of a bank account results in a citizen's **financial and social exclusion.** Similarly, a lack of access to essential insurance products can lead to financial ruin of a citizen if they are not insured against unexpected events such as accidents, the loss of employment or damages to their home – in fact, in some Member States, having home insurance is a requirement

19 EIOPA, *Consultation paper and impact assessment on EIOPA's Opinion on AI governance and risk management*, 2025.

for renting an apartment. Annex III (5) of the EU AI Act states that AI systems associated with the access to and enjoyment of essential private services and benefits should be classified as high-risk. It correctly includes (1) AI systems intended to be used to evaluate the creditworthiness of natural persons and (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 under this category. However, the regulation is inconsistent in that it does not include the risk assessment and pricing of other insurance products and customer risk assessments when opening a bank account under this category.

Moreover, Article 7 of the EU AI Act stipulates that use cases to be considered high-risk are AI systems that pose a risk of harm to the **health and safety** of persons. The mis-selling of retail investment products poses a risk of harm to health and the **financial safety** of an individual, as it can lead to huge financial detriment for a consumer, which, in turn, can also have an impact on the consumer's physical and mental health. Research has shown that financial problems such as over-indebtedness bring with them not only economic hardship for the affected consumer but also physical and mental health issues.[20] Furthermore, the mis-selling of investment products (e.g. unsuitable products that do not offer value for money) to retail investors undermines trust in the financial system, which is needed to boost retail participation in the capital markets to create a strong Savings and Investment Union (SIU).

Finally, as pointed out in the Finance Watch report *Artificial intelligence in finance: how to trust a black box?* on the regulation of AI deployed in the financial sector,[21] limiting the scope of the EU AI Act to only life and health insurance and credit products creates a **loophole in the regulation** and a possibility for regulatory arbitrage. For example, it makes human oversight compulsory for those products but not for financial products in general, making the regulation and supervision of financial products dependent on their legal wrapping. The following example provided in the referenced publication illustrates this problem well: *"…with the current wording of the EU AI Act, the same financial product with the same risk profile sold to the same customers (natural persons) will, for instance, require human oversight if packaged as a life insurance contract but not if packaged as a UCITS or a structured deposit."*[22]

Therefore, it only makes sense and is consistent to **broaden the EU AI Act** to also cover suitability and appropriateness assessments for retail investment products.

20 R. Ahlström et al., The Swedish Consumer Agency, Report, Is debt relief rehabilitative?, 2014.

21 Finance Watch, *Artificial intelligence in finance: how to trust a black box?*, March 2025.

22 Ibid.

Finance Watch recommendation:

- Extend the scope of high-risk AI systems in the EU AI Act by broadening the scope of Annex III of the EU AI Act to cover all financial services via adoption of delegated acts as per Article 7 of the AI Act.

B. Rules on data use

To adequately protect consumers from the risks outlined in Section II of this report, it is essential that there are rules in place that ensure that the right type of data is collected and used in automated decision-making and for the training of the AI model. In the current EU regulatory framework applying to retail financial services, including the EU AI Act, there are some rules on data governance for AI systems, but none of them, except for the revised CCD, contain specific **rules on which type of data** should be used by the financial institution for the different use cases under which an AI system processes personal data.

The EU AI Act, for example, stipulates under Article 10(3) that the training, validation and testing datasets used by high-risk AI systems must be **relevant, sufficiently representative and free of errors**. However, it does not specify which types of data meet these standards for the different use cases of AI systems within consumer financial services. Similarly, as indicated in Section III of this report, while the GDPR includes the principle of data minimisation, it does not specify the types of data that should and should not be collected and processed for the different use cases under which AI processes personal data in consumer financial services.

Thus, there is a need to introduce in the existing regulatory framework new rules specifying the **kind of data** that can be used and collected by AI-assisted decision-making tools and for the purposes of training AI models (e.g. to avoid biased models) for the following use cases:

- Risk assessment and pricing of insurance
- Suitability and appropriateness assessments for retail investment products
- The provision of retail investment advice and portfolio management
- CWAs for mortgages
- The KYC process when opening a bank account

The best legal vehicle to use for this would be to include these new rules in the respective sectoral legislation applicable to the different retail financial products. These rules should stipulate that any **social media data**, for example, should not be collected and used at all, as these data are not financially relevant and cannot be checked for accuracy.

Existing sources can be drawn upon to further identify the data relevant to the different

financial services use cases listed above. For example, the EBA Guidelines on loan origination and monitoring[23] stipulate which data are relevant for CWAs for consumer credit and mortgages. Moreover, the EBA Guidelines on money laundering/terrorist financing risk management and access to financial services[24] provide information about what types of data are relevant for the KYC process when opening a bank account and how unfair exclusion of vulnerable groups can be avoided. To ensure that the data use perimeter rules in these guidelines are properly adhered to, however, it is important that they are **legally binding l**evel 1 or level 2 measures in sectoral legislation and not merely non-legally binding guidelines.

In addition, to address the risk of large segments of vulnerable consumers becoming uninsurable due to the highly granular risk assessments enabled by AI, there is a need for rules that clearly stipulate how data used for **risk assessments and pricing of insurance** may be used to avoid **excessive granularity** that undermines the risk-sharing principle of insurance. Rules addressing this need to be included in the IDD. For example, the use of certain **proxy data**, such as shopping behaviour (e.g. using data on whether someone buys healthy foods and at which kinds of shops), to make inferences about an individual's level of risk (e.g. health risk) should be prohibited.

Finally, there is a need for rules protecting consumers from **discriminatory price personalisation** practices enabled by AI. While, as mentioned in the previous section of this publication, some existing legislation, such as the revised DMFSD, do include rules mandating the disclosure to consumers that the price of the financial service offered to them was personalised on the basis of automated decision-making, this is not sufficient to protect consumers.

Vulnerable consumers (e.g. elderly people or people with limited access to digital channels or other sources of information) are more likely to be affected by price personalisation, as they are more likely to lack knowledge about these practices or lack access to IT tools and the time to compare or switch products due to a particular life circumstance.[25] Therefore, merely making a consumer aware of the fact that the price has been personalised using an AI-assisted tool is not sufficient to protect them from an **unfair and unjustified** price. Instead, as part of the fitness check of EU consumer law on digital fairness, which is on the European Commission's agenda for the mandate 2024-2029, price optimisation practices should be banned in Annex 1 of the UCPD as an unfair commercial practice. Any price personalisation should not be based on the optimum amount of margin firms can earn from an individual consumer but only on fair and objective criteria, such as an individual consumer's risk and/or cost when taking out an insurance product.

---

23 See EBA *Guidelines on loan origination and monitoring*.

24 See EBA *Guidelines on management of money laundering/terrorist financing risks* when providing access to financial services.

25 EIOPA, Supervisory statement on differential pricing practices in non-life insurance lines of business, 2023.

Finance Watch recommendations:

- Introduce new rules in the existing sectoral legislation applying to retail financial services (the IDD, MiFID II, the CCD, MCD and AMLD 5), specifying the kind of data that can be collected and used by AI-assisted decision-making tools. These rules should also cover training, testing and validating AI models for the relevant use cases in the provision of retail financial services.
- Include, in the IDD, rules that clearly stipulate how data used for risk assessments and pricing of insurance may be used to avoid excessive granularity that undermines the risk-sharing principle of insurance.
- Ban price optimisation practices in Annex 1 of the UCPD as an unfair commercial practice.

C. Right to human intervention to review decisions made by AI systems

Human reviews of automated decisions generated by AI systems such as CWAs can be an important mitigant against inaccurate and biased decisions made by AI systems that can lead to mis-selling and/or financial exclusion. A consumer survey conducted by the European Consumer Organisation (BEUC) revealed that European consumers agree or strongly agree that AI users should have the right to say no to automated decision-making.[26]

As discussed in the last chapter of this report, the revised CCD, however, is currently the only legislation in the existing EU acquis that provides consumers with the right to human intervention to review a decision made by an automated decision-making tool. Thus, the sectoral legislation respectively covering the different retail financial services should be amended to include a **right for consumers to request human intervention** to review decisions made by AI systems for the following use cases:

- Customer due diligence (KYC) process when a consumer wants to open a new bank account
- Risk assessments and pricing for insurance
- Claims management for insurance
- Investment advice and portfolio management for retail investors
- Assessments of suitability and appropriateness in the area of retail investments

In addition, to help consumers decide whether a human review should be requested, whenever AI-generated automated decisions are involved in service provision, financial institutions should be **required**, via changes to sectoral legislation, to provide

26 BEUC, *Artificial Intelligence: what consumers say*, 2020.

consumers with information about the following:

- The sources and types of input data used
- A justification of why the data were used

Finance Watch recommendations:

- Introduce a right for consumers to request human intervention to review decisions made by AI systems in the sectoral legislation applying to retail financial services (the IDD, MiFID II, DMFSD rules, the MCD and AMLD 5) in alignment with the new CCD rules in this area.
- Introduce a provision in the sectoral legislation applying to retail financial services obliging financial institutions to provide consumers with information about the sources and types of input data used by an automated decision-making tool and a justification for why the particular types of data were used.

D. Redress and liability rules tailored to AI systems

Given the **complexity, autonomy and opacity** of AI systems, there is a need for redress and liability rules tailored to the unique characteristics and challenges of AI to ensure that consumers are able to seek redress in cases where damages are caused by the use of AI by financial institutions (e.g. to perform a CWA). The existing EU regulatory regime (including the AI Act), however, does not contain any liability rules tailored to the deployment of AI in the financial sector – or in any other retail sector.

Recognising this important **regulatory gap**, in 2022, the European Commission proposed the introduction of a directive on adapting non-contractual civil liability rules to artificial intelligence (AILD).[27] This proposal aimed to cover non-contractual civil liability for **damages caused by an output of an AI system** or by the failure to produce an output. Most importantly, the rules aimed at overcoming the challenges of the black-box nature of AI systems, which makes it difficult for consumers to successfully file liability claims when opaque AI systems are involved by introducing a rebuttable "presumption of causality". This concept would ease the burden of proof for claimants, meaning that if a victim can show that someone was at fault for not complying with a certain obligation relevant to their harm and that a causal link with the AI performance is reasonably likely, the court can presume that this non-compliance caused the damage.

While this proposal went in the right direction to address an important consumer protection gap, in early 2025, the European Commission unfortunately announced its **withdrawal of the AILD.**[28] To ensure the adequate protection of consumers sub-

27 See European Commission, *Liability Rules for Artificial Intelligence*.

28 Haeck, P., Bristow, T. and Herrero, O. *How the world stopped worrying and learned to love AI*, Politico, February 2025.

jected to automated decisions made by AI systems deployed in the retail financial sector, a new EU proposal to establish **non-contractual civil liability rules for AI should be introduced**. This new proposal, however, should not be a mere copy of the previous proposal but instead introduce the following improvements to address important flaws that would have resulted in it still being too difficult for consumers to successfully seek redress:

- The new rules should introduce not merely, as in the last AILD proposal, an easing of the burden of proof but instead **a reversal of the burden of proof i**n favour of the individual claimant. Under the previous proposal, consumers would still have to obtain relevant documentation that can eventually help them to prove fault of the AI operator. Consumers, however, may not have the expertise and sufficient skills to interpret this information, making it necessary for them to refer to external technical expertise, which, in turn, could significantly increase the costs involved in the process and the length of any court proceedings when a claim is brought.
- A **non-fault-based liability regime** should be introduced. The withdrawn AILD proposal took a fault-based liability approach, which means that the consumer would need to prove that the AI-based decision was erroneous. This approach would make it very difficult, if not impossible, for consumers to successfully obtain compensation for damages caused by an AI system. Due to the opacity and complexity of AI systems, very few consumers would have the knowledge, skills or resources necessary to prove fault. For example, in a situation where a consumer is unfairly denied an insurance product (e.g. home insurance) or only offered it at a prohibitively high price due to a biased AI system used to perform the risk assessment and pricing, it would be difficult, if not impossible, for a consumer to prove the discriminatory nature of the AI system without paying for expensive experts, if any can be found in the first place.

Harmonised rules in this area are also needed to avoid legal uncertainty and the risk of increased costs for businesses. Several EU Member States are considering or even concretely planning to introduce legislative measures on civil liability for AI.[29] Therefore, a lack of EU-level rules will result in fragmentation and increased costs for businesses conducting cross-border operations.

29 See European Commission, Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, SWD(2022) 319, 2022.

Finance Watch recommendations:

- The EU should introduce harmonised non-contractual civil liability rules for AI by reintroducing a directive similar to the AI Liability Directive proposal made by the European Commission in 2022 and withdrawn in February 2025 with the following key provisions:
  - → **Cover non-contractual civil liability** for damages caused by the output of an AI system or by the failure of an AI system to produce an output
  - → **A reversal of the burden of proof in favour of the individual claimant** to make it feasible for claimants to seek legal redress when necessary
  - → **A non-fault-based liability regime**

Conclusion

The use of AI systems is on the rise in all European industries, including the retail financial services market. While the deployment of AI in the provision of retail financial services brings efficiency and productivity gains, it entails considerable consumer risks that need to be mitigated. These consumer risks include the unfair denial of essential financial services such as a bank account or insurance, the mis-selling of risky products, unfair price discrimination practices and difficulty/inability to successfully seek redress in case of damages to consumers caused by the use of AI in the financial sector.

Existing cross-sectoral (horizontal) consumer legislation applying to retail financial services (e.g. the UCPD and GDPR) and sectoral financial services legislation (e.g. the CCD and the DMFSD) include some important provisions that address some of the consumer risks stemming from the operation of AI in retail financial services. However, most of these pieces of legislation were approved at a time before AI systems even existed or were widely used. As a result, there are major gaps in existing cross-sectoral consumer regulation and sectoral legislation with regard to addressing these risks. Some of these gaps are filled by the EU AI Act, which will become applicable in August 2026 and was, among other pieces of legislation, specifically designed to ensure that the key consumer risks stemming from the use of AI systems are adequately addressed. However, not all retail financial services are covered by the data governance, risk management, record-keeping and human oversight requirements introduced by the EU AI Act. Therefore, there is an urgent need to broaden the application of the requirements applicable to high-risk AI systems in the EU AI Act to all retail financial services.

In addition to extending the EU AI Act, there is a need to make some important and manageable changes to sectoral retail financial services legislation to address risks that are unique to financial services and/or require tailored solutions that cannot be adequately covered by the EU AI Act, given its cross-sectoral/horizontal scope of application. Key new rules required in this area include rules on which types of data can be used to train AI models and to produce outputs for the different use cases in the provision of retail financial services. In addition, given the unique challenges the opacity that AI brings with regards to successfully and feasibly seeking redress in cases where consumers face damages caused by the use of AI systems by firms, there is a need to urgently introduce an EU harmonised AI liability regime that reverses the burden of proof in favour of the individual claimant.

Deploying AI in retail financial services has tangible real benefits that can bring efficiencies and cost reductions, improving the competitiveness of EU financial service providers. As such, EU policymakers are correct in promoting AI development and uptake in the Union. However, without the right guardrails in place to adequately protect consumers from the considerable risks outlined in this report, these objectives will not be reached, as societal trust in AI and in the wider financial system will be hurt.

As evidenced by a survey of the European Consumer Organisation (BEUC), trust in AI among European consumers is currently already low.[30] Therefore, it is crucial that the current shift in focus by EU leaders away from ensuring AI safety and governance towards a wholesale embrace of AI with lighter regulation is reversed. AI safety and the promotion of AI development and uptake are not conflicting objectives; they are complementary goals that must be pursued in parallel.

30 BEUC, *Artificial Intelligence: what consumers say*, 2020.

www.finance-watch.org

About Finance Watch

Finance Watch is an independently funded public interest association dedicated to making finance work for the good of society. Its mission is to strengthen the voice of society in the reform of financial regulation by conducting advocacy and presenting public interest arguments to lawmakers and the public. Finance Watch's members include consumer groups, housing associations, trade unions, NGOs, financial experts, academics and other civil society groups that collectively represent a large number of European citizens. Finance Watch's founding principles state that finance is essential for society in bringing capital to productive use in a transparent and sustainable manner, but that the legitimate pursuit of private interests by the financial industry should not be conducted to the detriment of society. For further information, see www.finance-watch.org.

Finance Watch
Rue des Colonies 56 box 3
1000 Brussels
T: + 32 (0)2 880 0430

www.finance-watch.org

Finance Watch