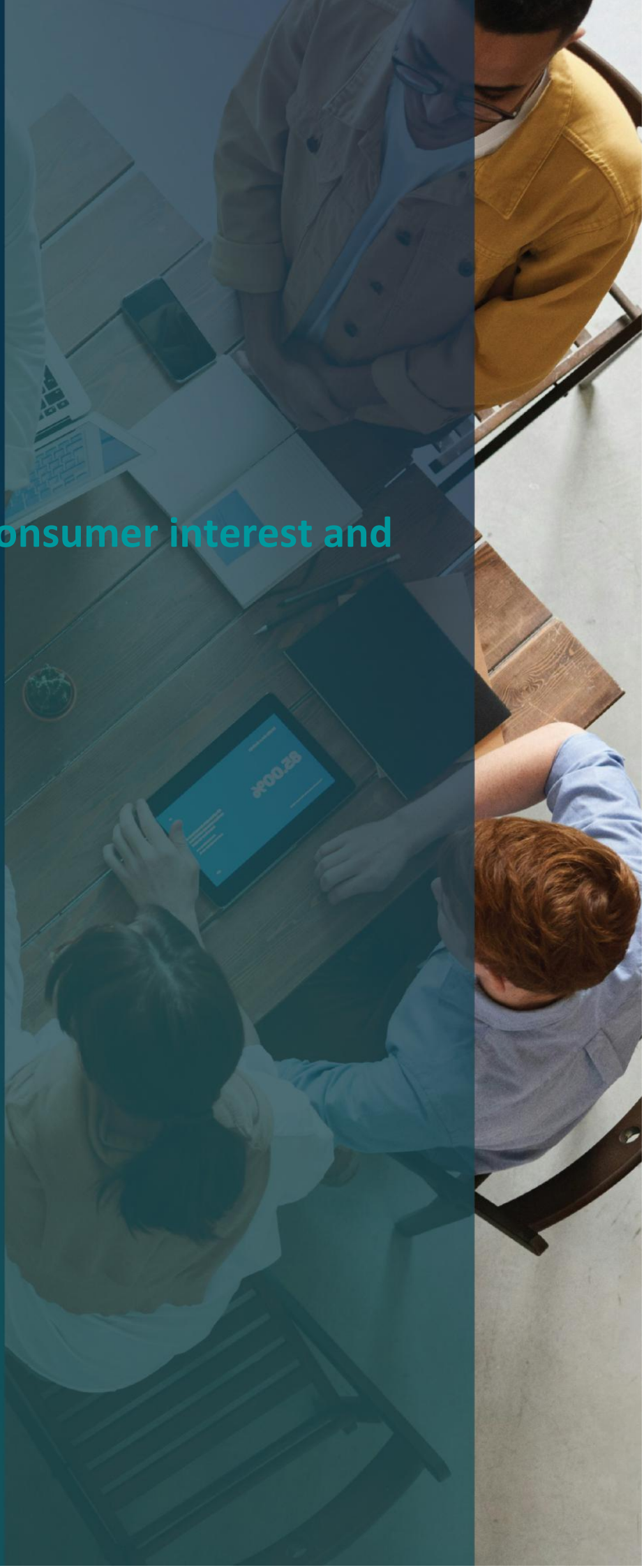
TISA

DRCF call for input -Consumer interest and AI

Phil Turnpenny
Policy Executive

August 2026



About TISA

Supporting the financial journey through life

The Investing and Saving Alliance (TISA) is committed to improving the financial wellbeing of all UK consumers by working collectively with the financial services industry to deliver solutions and champion innovation, for the benefit of people, our industry, and the nation.

We do this by working with our member firms to deliver practical solutions and devise innovative, evidence-based strategic proposals for government, policy makers and regulators that address major consumer issues.

We care about the entire financial life of consumers: from their first savings account opened to ensuring people can age and retire with dignity. TISA believes that savings and investments play a significant role in the lives of people and small businesses. Consumers benefit when they put aside money for their future. Saving and investing can provide a buffer for emergencies; help people achieve big and small goals throughout their lifetime; and give people quality of life in later years.

TISA is a not-for-profit membership organisation and a trusted partner of key industry stakeholders in helping shape the future of the UK financial services and the environment in which we operate. We have approximately 260 member firms involved in the supply and distribution of savings and investment products and associated services.

Our work, your influence

Our policy work reflects TISA's broad scope of interests and aims on meeting the needs of UK consumers, members and our industry. From improving financial education, inclusion and accessibility, right through to savings, investments and retirement planning, the work we do with our members to **influence policy** is crucial in enhancing the industry we operate in and driving positive change.

As part of our commitment to delivering focused and impactful consumer outcomes, TISA's policy working groups have been structured into **three distinct workstreams**:

1. **Consumer Protection -** *Protecting the best interests of UK consumers in their financial journeys.*
2. **Consumer Access -** *Considering issues that could directly impact access to financial products.*
3. **Effective Products -** *Examining key considerations and legislation relating to products across the investing and saving landscape.*

All groups focus on both strategic and technical elements of policy/regulation. We provide a channel for firms to have their say on the policy we develop and present, contribute to our technical and regulatory interpretation work and, importantly, gain insights from other TISA members, policy makers, government and regulators.

Find out more about TISA here: www.tisa.uk.com/about-tisa

Introduction

TISA welcomes the opportunity to respond to the DRCF's call for input on Consumer interest and AI.

AI is already beginning to reshape how consumers interact with financial services, how firms design and deliver products, and how regulated entities manage operational, conduct and consumer protection risks. As adoption increases, it is essential that consumers remain properly protected while firms are given the clarity and confidence needed to innovate responsibly.

TISA's central recommendation is that regulators should build on the UK's existing financial services framework when overseeing the use of AI, rather than creating a separate AI-specific regulatory regime. Existing requirements, including the Consumer Duty, governance and accountability obligations, data protection law, outsourcing and operational resilience rules, and wider conduct standards, already provide important safeguards that can be applied to AI-enabled services. A parallel framework could create unnecessary duplication, increase uncertainty for firms and slow the adoption of technologies that may improve consumer outcomes.

We also recommend that the official sector works with industry to develop model contractual clauses for AI use, procurement and third-party provider relationships. These could provide a practical and timely way to clarify accountability, liability, data use, governance responsibilities and oversight expectations across the AI value chain, particularly where firms rely on external technology providers.

Consumers should be supported through transparency, fair treatment and proportionate choice. TISA supports targeted opt-outs where AI has a significant effect on a consumer but would caution against a blanket right to reject all AI use. Such an approach may increase costs, require firms to maintain parallel non-AI processes, and reduce the potential benefits of responsible AI adoption.

In addition, TISA encourages regulators to provide practical guidance, illustrative use cases, innovation sprints, showcases and a cross-regulator AI sandbox through the DRCF. AI use cases often raise issues across financial regulation, data protection and consumer protection simultaneously, and coordinated regulatory engagement will be important in reducing fragmentation.

Regulators should also seek alignment with emerging international standards and supervisory frameworks, including ISO 42001, to support consistency and reduce the risk of regulatory arbitrage.

Overall, TISA believes that consumer protection should not depend solely on consent or consumer opt-outs. These may be useful safeguards in appropriate circumstances, but they should complement, rather than replace, firms' responsibility to deliver fair outcomes through appropriate governance, testing, monitoring and accountability.

`

Question responses:

17. What tools can industry offer to consumers or otherwise implement (risk governance frameworks, impact assessments or others) to manage AI risks?

Industry can implement a range of governance, risk management and assurance measures to manage AI risks. These include adopting recognised frameworks such as ISO42001, the international standard for AI management systems, which provides a structured approach to AI governance, accountability, risk management and continual improvement.

Firms should establish AI governance policies and procedures, integrated with existing business continuity planning (BCP) and operational resilience frameworks, to ensure AI-related risks are identified, assessed and managed throughout the AI lifecycle.

It is also important that firms continue to comply with and apply existing regulatory and legislative requirements, including UK GDPR and data protection obligations, the FCA Consumer Duty, consumer protection legislation, the Equality Act 2010, the Senior Managers and Certification Regime (SM&CR), and operational resilience requirements, as these frameworks already provide important safeguards that are relevant to the use of AI. Organisations can draw on other established resources, such as the ICO's AI and data protection risk toolkit, to support good governance, accountability and compliance when developing and deploying AI systems.

In addition, organisations can undertake AI impact assessments to evaluate potential risks and harms before deployment, supported by ongoing internal and external audits to provide assurance that controls remain effective and are operating as intended.

Robust third-party due diligence and testing should be applied where AI systems, models or data providers are sourced externally, while bias, fairness and performance testing can help identify and mitigate discriminatory outcomes and other unintended consequences.

Firms should also implement continuous monitoring and oversight processes to detect model drift, performance degradation and emerging risks over time.

18. Should consumers be able to opt-out of AI, and if not, what is the legal basis for the use of their data?

A balanced approach would be to allow consumers to opt out of AI-driven decision-making where appropriate, particularly where decisions have a significant impact on individuals. However, a blanket right to opt out of all AI use may not be practical or proportionate, particularly where AI is used to support operational processes, fraud detection, cybersecurity, or service efficiency.

In some cases, widespread opt-outs could undermine the benefits of AI and lead to increased costs, potentially resulting in cross-subsidisation, whereby consumers who are willing to use AI-enabled services bear the costs associated with maintaining parallel non-AI processes.

Where firms use personal data in connection with AI, they should ensure there is a clear and appropriate legal basis for processing under existing data protection legislation, such as consent, contractual necessity, legal obligation or legitimate interests, as applicable. Firms should also be transparent about how AI is used,

provide meaningful information to consumers, and ensure compliance with existing requirements including UK GDPR, consumer protection legislation and the FCA Consumer Duty.

19. What tools, frameworks or standards can regulators leverage to safeguard consumer protection? Can these be easily adapted or transferred on a cross-sectoral basis?

Regulators can build on existing frameworks rather than creating an entirely new AI-specific regime. The FSMA framework should be applied to AI-enabled products and services, ensuring that firms remain subject to the same regulatory expectations regardless of whether outcomes are delivered through traditional processes or AI systems.

Where large technology providers seek to offer regulated financial services directly to UK consumers, they should be required to establish an appropriate UK legal entity and obtain FCA authorisation where they are conducting regulated activities.

The official sector should also work with industry to develop model contractual clauses for AI procurement and third-party provider relationships. Contract law is likely to provide the fastest and most practical mechanism for addressing issues such as accountability, liability, transparency, data usage and governance responsibilities, particularly where policy and legislative change can take considerable time to implement.

Applying the existing financial services regulatory framework to AI would ensure that established requirements, including Consumer Duty, prudential requirements, governance arrangements, SM&CR, operational resilience requirements and wider conduct standards, continue to apply. This approach would provide consistency, promote consumer protection and avoid the need to develop an entirely separate regulatory framework for AI, while ensuring that firms remain accountable for the outcomes generated by AI systems used in the delivery of regulated services.

20. What types / modes of guidance or other regulatory tools are most helpful to industry for achieving compliance – e.g. detailed guidance, sandboxes and others. If any effective international examples come to mind, please refer to these.

Firms need clear, practical guidance from regulators, particularly as AI technologies continue to evolve. Greater clarity on the safe deployment of AI would help firms apply regulatory expectations with confidence. In particular, illustrative use-case studies would enable firms and compliance teams to understand how outcomes-based regulation operates in practice, reducing uncertainty and supporting the responsible adoption of AI.

TISA strongly supports the use of innovation tools such as regulatory sandboxes, innovation sprints and showcases. These initiatives enable firms to test new technologies and business models in a controlled environment, engage directly with regulators, and accelerate the adoption of innovative solutions while managing associated risks.

We would recommend the development of a cross-regulator AI sandbox through the Digital Regulation Cooperation Forum. AI use cases in financial services often raise questions relating to data protection, consumer protection, competition, governance and financial regulation simultaneously. A joint sandbox would enable firms to test innovative AI solutions in a controlled environment while engaging with multiple regulators through a single process

We believe that a trusted kitemark or FCA-backed accreditation for AI-powered services could help consumers identify regulated and trustworthy providers, increasing confidence in the use of AI within financial services. A recognised accreditation framework would provide assurance that AI tools have been

developed and deployed in accordance with relevant regulatory standards and consumer protection requirements.

We recognise the EU AI Act's risk-based framework as a useful international reference point for the regulation of AI. In particular, the Act's classification of certain applications as "high-risk" provides a structured and proportionate approach to identifying, assessing and mitigating potential harms arising from AI deployment in sensitive, consumer-facing contexts.

As AI-driven decision-making becomes increasingly prevalent within financial services, TISA believes that elements of the EU's risk-tiering approach could help inform future policy development. A risk-based framework may support regulatory clarity while ensuring that oversight remains proportionate to the potential impact on consumers and markets.

TISA supports further exploration of industry-led protocols and model contractual frameworks for AI deployment. For example, standardised agreements governing AI agents could help establish clear expectations regarding delegated authority, accountability, governance responsibilities and consumer protections.

Widely adopted industry standards could improve consistency across the market, reduce legal and operational uncertainty, and provide firms with a common framework for managing AI-related risks. Over time, such protocols could also help deter poor practice and raise minimum standards across the industry, making it more difficult for bad actors to operate outside established norms and expectations.

21. What is the current application of AI standards, if any, and is there international best practice?

The current application of AI standards within financial services is still evolving, although a number of recognised frameworks are emerging as leading practice. In particular, ISO 42001, the international standard for AI management systems, provides firms with a structured approach to AI governance, accountability, risk management, monitoring and continual improvement. Organisations are also increasingly drawing on broader governance and risk management frameworks, such as the NIST AI Risk Management Framework, to support the development and deployment of trustworthy AI systems.

Given the global nature of AI development and deployment, international coordination will be essential. We are aware that IOSCO has issued a supervisory toolkit, and we would encourage UK regulators to actively support and help shape international standard-setting initiatives. A coordinated international approach would promote consistency in expectations across jurisdictions, reduce compliance complexity for firms operating cross-border, and help minimise the risk of regulatory arbitrage, whereby firms or providers seek to exploit differences between regulatory regimes.

Wherever possible, regulators should seek to align AI expectations with existing financial services frameworks and internationally recognised standards, ensuring firms can adopt AI safely while maintaining consumer protection, market integrity and operational resilience. A principles-based, internationally coordinated approach is likely to be more effective and durable than a fragmented set of jurisdiction-specific requirements.

22. Is informed and meaningful 'consent' the right lever to ensure a consumer is protected and aware of risks?

We would question whether informed and meaningful consent is currently being obtained consistently in practice, particularly where consumers are presented with lengthy terms and conditions, complex privacy notices or multiple consent requests that can be difficult to understand. While consent can play an important

role in protecting consumers, it should not be relied upon as the sole mechanism for managing AI-related risks.

Instead, firms should focus on providing clear, concise and intelligible disclosures that explain how AI is being used and highlight any material risks or implications for consumers upfront. Information should be presented in a manner that is accessible and meaningful to consumers, enabling them to make informed decisions without requiring them to navigate lengthy or highly technical documentation. Attention should be given to explaining where AI has a significant influence on customer outcomes, recommendations or decisions.

More broadly, consumer protection should not depend solely on individual consumers understanding and consenting to risks. Firms should remain responsible for delivering fair outcomes through appropriate governance, oversight and controls, consistent with existing requirements such as the Consumer Duty, regardless of whether a consumer has provided consent. In this regard, improved transparency and consumer understanding are important, but they should complement, rather than replace, firms' accountability for the safe and responsible use of AI.

23. Are there any other levers (e.g. cooling-off periods, right to opt-out of using AI, 'cookies'-like requests)?

We do not consider a cooling-off period to be a practical or proportionate response to AI use in financial services. In many cases it would introduce additional friction into customer journeys, delay access to products and services, and potentially frustrate consumers without materially improving outcomes. Any such requirement would also need to be applied consistently across the market to avoid creating an uneven playing field between regulated firms and unregulated providers.

A more proportionate approach may be to provide consumers with a right to opt out of certain uses of AI, particularly where AI is used to personalise services, recommendations or decision-making. However, any opt-out mechanism should be accompanied by appropriate safeguards to ensure consumers are not disadvantaged as a result. In particular, firms should not be permitted to engage in unfair treatment, exclusion, or unjustified price discrimination solely because a consumer has elected not to use an AI-enabled service.

More generally, consumers should be offered meaningful transparency and choice wherever this can be achieved without undermining service delivery. The experience of providers such as DuckDuckGo demonstrates that consumers can benefit from having genuine alternatives and greater control over how their data is used. Any future framework should therefore support consumer choice and transparency while ensuring that equivalent services remain available regardless of whether consumers choose to engage with AI-enabled features.

24. Are there existing examples in other sectors or jurisdictions who utilise tools efficiently?

California provides examples in financial services (financial advice) where AI tools are being deployed to support professional decision-making. In these sectors, AI is generally used to augment, rather than replace,

human judgement, with requirements for governance, oversight, accountability and consumer protection remaining in place. These models demonstrate how regulators can allow innovation while applying appropriate safeguards in higher-risk use cases.

The European Union's approach also provides useful lessons, particularly through its emphasis on a risk-based framework, whereby the level of regulatory scrutiny is linked to the potential harm posed by an AI system. While the UK may not wish to replicate this approach in full, the focus on proportionality, governance and accountability offers valuable principles that can be adapted to financial services.

25. Can outcomes-based approaches, analogous to 'Consumer Duty' type frameworks, where firms are expected to actively consider and deliver fair outcomes, be a vehicle for consumer protection?

Yes, an outcomes-based approach, similar to the Consumer Duty, could be an effective vehicle for consumer protection in the context of AI. It would allow firms flexibility to innovate while requiring them to actively consider, monitor and deliver fair consumer outcomes. Such an approach is also more likely to remain effective as AI technologies evolve than highly prescriptive rules.

However, for this model to succeed, the official sector must be confident that it is capable of being supervised and enforced in practice. Firms need clarity on regulatory expectations and how compliance will be assessed. There should also be greater precision around consumer redress frameworks, so that consumers, firms and regulators all have certainty regarding accountability, liability and routes to redress where AI-related harm occurs. Provided these issues are addressed, an outcomes-based approach could offer a proportionate, technology-neutral framework that promotes both innovation and consumer protection.

26. Who should be held accountable, and to what extent, for AI risks materialising? Consumer, firms (including integrators, developers), or regulators?

Accountability for AI risks should be determined through a clear framework developed by the official sector in collaboration with industry, technology providers and consumer representatives. This is a complex area requiring careful consideration of liability, oversight, third-party dependencies and consumer redress.

Firms should remain accountable for the consumer outcomes delivered through their products and services, including where AI solutions are provided by third parties. At the same time, responsibilities across the AI value chain should be clearly defined.

Regulatory frameworks should not incentivise or permit circumstances that lead to widespread consumer harm. Where regulatory requirements, supervisory approaches or regulatory gaps contribute to such outcomes, regulators should also be subject to appropriate scrutiny and accountability. Clear accountability and redress arrangements will be essential to maintaining consumer trust.

27. Do 'tolerable risks' exist for consumers in these contexts, and if so, how should policymakers/regulators define and operationalise? What about industry?

We do not believe there is a need to create a separate concept of "tolerable risk" for AI in financial services. The existing regulatory framework already establishes the standards and risk tolerances for regulated activities in the UK, including requirements relating to consumer protection, conduct, governance, operational resilience and prudential risk.

Policymakers and regulators should therefore have confidence in these existing frameworks and seek to apply them consistently to AI-enabled services. If firms use AI tools to provide regulated activities, those tools

and the firms deploying them should be held to the same standards and expected to deliver the same consumer outcomes as traditional processes.

28. What metrics, thresholds or proxy indicators are feasible?

See refer to question 27 answer.