AIFS0006

# Written evidence submitted by Zurich UK

## About us

Zurich UK provides a suite of general insurance and life insurance products to retail and corporate customers. We supply personal, commercial, and local authority insurance through a number of distribution channels, and through financial intermediaries for the retail market and via employee benefit consultants for the corporate market. We have several large office sites regionally and employ around 5,000 people.

We are part of Zurich Insurance Group, a leading multi-line insurer serving people and businesses in more than 200 countries and territories. Founded over 150 years ago, the Group provides insurance protection and prevention services that promote wellbeing and enhance climate resilience. The Group has about 60,000 employees, is headquartered in Switzerland and Zurich Insurance Group Ltd (ZURN) is listed on the SIX Swiss Exchange.

Zurich welcomes the opportunity to respond to the House of Commons Treasury Committee call for evidence on AI in financial services. Zurich UK utilises AI to enhance various aspects of its business operations. AI is used to streamline claims processing by automating routine tasks, which improves efficiency and reduces processing time. AI-driven data analytics helps in risk assessment and underwriting, enabling more accurate and personalised insurance policies. Customer service is also enhanced through AI-powered chatbots and virtual assistants that provide instant support and handle enquiries, improving overall customer experience. AI also aids in fraud detection by analysing patterns and identifying suspicious activities, thereby mitigating potential losses.

## Executive Summary

AI is transforming financial services by enhancing productivity and improving customer interactions. Currently, AI automates manual tasks, allowing staff to focus more on customers. Key applications include data extraction and managing unstructured data for better risk assessment. Successful AI initiatives often come from internal development, supported by strong team collaboration and innovation competitions involving FinTech firms. In the next five to ten years, AI is expected to further enhance risk understanding and management, leading to more tailored products and services. While AI will improve efficiency, human interaction will remain crucial during critical service moments, with growing customer acceptance of AI.

Despite its benefits, AI adoption faces challenges such as the need for skilled personnel and upskilling existing staff in AI management. Cybersecurity is a primary concern, requiring close collaboration with third-party vendors to mitigate AI-related risks. The complexity of AI models and reliance on external solutions introduce resilience risks that must be managed. For consumers, AI offers enhanced services, particularly for vulnerable groups, but those lacking tech access may be disadvantaged. Transparency in AI training data and processes is essential to prevent discrimination. No new regulations are needed, but establishing standards for AI professionals could enhance confidence. A regulatory framework focusing on resilience, transparency, and sustainability for third-party providers is recommended to balance innovation and consumer protection.

**How is AI currently used in different sectors of financial services and how is this likely to change over the next ten years?**

*This may include:*

- *Are there particular areas of financial services that are adopting AI more quickly and at higher rates of penetration than others? Are Fintech firms better suited to adopting AI? What percentage of trading is driven by algorithms/artificial intelligence?*
- *Are financial services adopting AI at a faster rate than other sectors in the economy?*

**Zurich Response:**

Current use cases: Currently our biggest use is to improve productivity and remove manual processing activity. This supports our frontline staff to have more time with our customers and provide quicker responses to their requests. This includes data extraction and populating legacy systems, routing emails to the right teams, reading those emails and highlighting missing information. Generative AI has made a significant difference to us being able to unlock all the unstructured data we have in our organisation and start putting it to better use. It is also helping us to better assess risk LiDAR data which previously was too large for us to manage and analyse giving us better insights to building heights and the unique risks tall buildings can present especially in fire or windstorm insurance.

Fintech: Our most successful implementations have been internally developed either by teams in the UK or by our central teams around Europe, we have a philosophy of reuse and therefore teams are actively working together to develop and share solutions across the group. We have a highly successful innovation championships which we run each year for FinTech's, start-ups and scale ups. These are often in niche areas where we do not have in-depth knowledge rather than our core business. For insurance, AI and advanced analytics are not areas that are new to us. We are deeply experienced in using ML and advanced modelling techniques to deliver insights for our business and manage risk.

How it will change 5-10 years: We see developments over the next 5-10 years deepening our ability to understand risk, help our customers manage risk and to provide more tailored products and services for our customers. It is difficult to gaze that far into the future when 5 years ago we could not have predicted how much of a difference GenAI would have made in the last couple of years and there is a lot still to explore in that space. AI will evolve rapidly, and its usage and implementation will vary across sectors and populations.

AI usage is not going to not reduce the level of service we provide our customers. Attitudes may change over time with customers being more receptive to interacting with AI services. For now, through a claim, we believe customers want to know there is a person they can speak to and can support them through their challenges.

### To what extent can AI improve productivity in financial services?

This may include:

- *Where are the best use cases for AI? Which particular transactions may benefit from AI?*
- *What are the key barriers to adoption of AI in financial services?*
- *Are there areas where the financial services should be adopting GenAI with little or no risk?*
- *Are there likely to be job losses arising from AI in financial services and if so, where?*
- *Is the UK's financial sector well-placed to take advantage of AI in financial services compared to other countries?*

**Zurich Response:**

Best Use cases: Much of our business is still conducted by email. Data comes to us from brokers in unstructured forms or each broker has their own structured way of doing things from pdfs, word documents and excel spreadsheets. AI enables us to take this data directly from the email, to structure it and to populate our various systems. This reduces our reliance on data processing teams here and offshore and ensures we can deliver a much quicker, consistent, and accurate service.

One area of increasing investment and concern is the battle against insurance fraud. GenAI tools are making it easier than ever to create fake documents to support claims whether it is fake images of damage or fake estimates from contractors. Our aim with using AI in fraud detection is to speed up detection of potential fraudulent claims and to settle honest claims quicker. We implement new tools in a slow and methodical manner to ensure false positives are minimised and all flagged claims are investigated by skilled and experienced investigators.

Barriers: We don't feel there are any barriers to adoption other than access to highly skilled staff and upskilling existing staff to understand how to implement, manage and maintain AI solutions. These are different skills to the current IT skills we have and to be able to fully benefit from technology developments we need to be continually upskilling our staff. This is where a flexible approach to the apprenticeship levy could support.

Adopting GenAI: GenAI presents little risk in extracting and structuring textual data of which insurers have vast amounts. The risk is not in the GenAI but ensuring that staff are adequately trained to understand the limitations and ensure sufficient oversight of the quality of data extraction and text generation.

Future of jobs: Financial service jobs are constantly evolving with roles from even 10 years ago not existing today and new roles appearing all the time. Firms will need to expand data, analytics and data science teams which will present new opportunities while administrator roles will continue to decline as they have with digitisation, removing the need for filing clerks and typists. The concern will be how we develop new entrants to the industry and maintain industry knowledge for business resilience if those entry level jobs are being completed by AI and the years of knowledge built up through experience is accessible through chatbots and knowledge management tools.

The ability to assess new risks is often based on human experience and being able to ask the right questions: if AI is learning from the past how we will anticipate the risks of the future? In the short to medium term, we need to be developing data and AI literacy skills among our teams. But good AI comes from identifying problems and critical thinking, therefore developing these skills is essential for the future of work. We are clear that our current approach is to augment our teams with AI, give them the tools and training to experiment, to involve them in the development and delivery. This is all aimed to ensure we alleviate any fears, ensure all colleagues can contribute to challenging whether AI is the right thing to do and ensure our teams adapt over time. A concern we are just starting to discuss is the impact on wellbeing and to what extent increasing productivity could be harmful to wellbeing and resilience.

### What are the risks to financial stability arising from AI and how can they be mitigated?

This may include:

- Does AI increase the risks relating to cybersecurity?
- What are the risks around third-party dependencies, model complexity, and embedded or 'hidden' models?
- How significant are the risks of GenAI hallucination and herding behaviour?
- Are the risks of having AI tools used in the financial sector concentrated in the hands of a few large tech companies? To what extent do the AI financial market tools rely on social media outlets? E.g. trading algorithms using social media posts?

**Zurich Response:**

Cybersecurity Risk: The cybersecurity risks associated with AI can be divided into two main areas. First, AI can boost the abilities of cybercriminals targeting Zurich's digital environments and users. Malicious actors can use AI to automate cyberattacks, making them more effective. AI helps attackers find and exploit vulnerabilities and learn how to avoid detection by security systems, such as antivirus software, and reduces the expertise required to conduct these types of attack, lowering the barrier of entry for potential attackers. Additionally, AI can create deepfake images and videos and assist in more sophisticated phishing campaigns by making it easier to research targets and create believable social engineering content.

The second area of risk involves attacks on the AI systems that an organisation uses, either for its staff or for partners and customers. In addition to standard security measures for traditional applications, such as managing vulnerabilities and controlling access, AI systems need specific protections against threats unique to AI. For example, attackers may use data poisoning to manipulate the training data of machine learning models, leading to biased or harmful outputs. They might also employ adversarial techniques, subtly altering input data to cause AI systems to make incorrect decisions that can be exploited. To address these types of attacks, organisations will need new technologies and security processes. There may be gaps in capabilities due to a lack of skills and suitable products.

Organisations should establish controls specifically designed to address the unique challenges posed by AI. This includes regular assessments of AI systems, continuous monitoring for unusual outputs, and ensuring standard IT security controls are in place. Increasing staff awareness is crucial, particularly regarding AI's capability to create fake but believable content. Employees should be educated on how AI can be used in social engineering attacks, such as generating realistic deepfake images or personalised phishing emails. This awareness can help staff recognise and respond to suspicious content, reducing the likelihood of falling victim to such attacks. Workshops on identifying deepfakes and recognising phishing attempts can be particularly beneficial. While AI poses certain risks, it also offers significant advantages that can be leveraged to strengthen cybersecurity defences.

Third-party dependencies: we have implemented specific AI questionnaires as part of our on-boarding and ongoing due diligence of third parties whether vendors or administrators. This enables us to have a better understanding of what AI is being used in products and services, the culture, and qualifications of these parties and that our Responsible AI Principles are aligned. By making the questionnaire a standard part of our due diligence we have been able to work with third parties to ensure we are comfortable with the proposed solutions. The best way to manage risk in this space is by having open dialogue between the parties.

Hallucinations and Herding Behaviour: this is a topic we are discussing as we roll-out GenAI solutions to our underwriters~~,~~ We are focused on ensuring that training is delivered regarding human-in-the-loop, and the accountability underwriters have for decision making. We ensure any in-house use of LLMs has monitoring in place, and that our focus is on implementations like RAG where hallucinations are minimised due to having a defined reference source the LLM must use. We are also discussing how we "check the checkers" and what quality control processes need to be put in place to ensure staff do not become complacent to their responsibilities and accountabilities.

Tech concentration risk: Tech concentration risk is not an AI risk but a resilience risk. Challenges include siloed data, closed eco-systems, anti-competitive pricing practices. There are also challenges around software being updated with no veto or roll-back rights which can be challenging for both AI governance, information governance and IT security. Incidentally, there are more AI models than there are cloud providers, so if cloud providers suffer operational disruption, many firms and their AI systems will also be disrupted.

Social media: Social media does not form a key part of the way we transact business. It is however used in a small way for Fraud detection. It has no automated decision-making or trading impact, and every result is independently verified by our fraud investigation team.

### What are the benefits and risks to consumers arising from AI, particularly for vulnerable consumers?

This may include:

- What benefits to consumers might arise from using AI in financial services? for example, could AI be used to identify and provide greater assistance to vulnerable consumers?
- What is the risk of AI increasing embedded bias? Is AI likely to be more biased than humans?
- What data sharing would be needed to make AI more effective in financial services, and will there be a need for legislative change to achieve that?
- Are there any current or future concerns around data protection and AI in financial services?
- What sort of safeguards need to be in place to protect customer data and prevent bias?

### Zurich Response:

Consumer Impact: A primary consideration with the use of AI within insurance is digital accessibility. There is a risk with an increasing push to digitisation and automation those unable to interact with technology either through affordability or skills may be disadvantaged or charged a premium to access off-line services.

Desire is building for automated transcription tools to support contact centre agents in summarising and documenting conversations. Care needs to be used in this space to ensure non-native / regional dialect speakers are not disadvantaged as transcription tools have not necessarily been trained to manage the vast variance in the English language or industry specific terminology. There is also a desire expressed across the industry for emotion detection tools to help identify potential complaints or vulnerable customers. We have seen these tools developed by US tech firms with little diversity in their training data and an absence of representation of Europeans. We also need to be aware that we do not all express our emotions in the same way, and this could lead to false negatives as well as false positives.

AI/ML can find patterns in data that may not be obvious to a human analysing the same data. Transparency of training data, a requirement for explainability and significant model testing is required to ensure tools do not discriminate.

Data Sharing: Currently as an industry we do not collect protected characteristics as part of our customer onboarding process. Therefore, when developing solutions and ongoing monitoring it is difficult to check for bias. We use external data where we can, to ensure protected groups are not unfairly disadvantaged through factors such as postcode and we remove anything from our training data that could be correlated with protected characteristics. Being able to access demographic data in a more granular and regular form than the census would enable better bias detection. This would ideally be provided by the Office for National Statistics or other government agencies. Our experience of collecting demographic data from our own staff demonstrates individuals are uncomfortable with providing this information if they don't believe it will be used for their individual benefit.

Data Protection Laws**:** Data protection laws do not present a barrier to responsible AI development. Clarity on transparency and explainability requirements may better support consumers in understanding when they are interacting with AI and how the decision is being made, this needs to be balanced with intellectual property and competition law.

**How can Government and financial regulators strike the right balance between seizing the opportunities of AI but at the same time protecting consumers and mitigating against any threats to financial stability?**

This may include:

- Are new regulations needed or do existing regulations need to be modified because of AI?
- Will Government and regulators need additional information, resources, or expertise to help monitor, support, and regulate, AI implementation in financial services?

**Zurich Response:**

New regulation: we do not believe new regulation of financial services is required currently. A principled, risk-based approach aligns with current regulation.

Where we do believe there would be benefit is ensuring a standards body for qualifications for Data Scientists / AI Developers such as the IFOA or CII to ensure firms are hiring skilled professionals backed by the need for continuing professional development and a code of conduct. Currently high salaries are being requested for these in-demand jobs with little way of validating they are suitably qualified. This goes as much for hiring by firms as it does for validating the skills of third-party providers.

Beyond financial services a regulatory regime that requires resilience, transparency, explainability, and sustainability, of third-party providers would provide firms with more confidence over the use of third-party models and solutions. One solution discussed at the recent FCA AI Sprint was a Responsible AI Statement akin to the Modern Slavery Statement.

***February 2025***