<u>Public Bill Committee on the Online Safety Bill – Aviva's written evidence submission</u>

About Aviva

Aviva is an international insurance and long-term savings business, which provides life insurance, general insurance, health insurance and asset management services to over fifteen million customers worldwide. Here in the UK, we are the market leading insurance business, serving one in every four households. We help more than five million people with their retirement needs and meet the pension requirements of more than 20,000 companies, ranging from large multinationals to small start-ups.

Overview

Aviva has long called for greater consumer protection from online fraud which has undermined consumer trust in financial services and put millions of people at risk of falling victim to scam adverts and fraudulent promotions online. We know fraudsters are increasingly using online platforms to target their victims, yet to date, platforms have had very little legal responsibility to protect users online. In May 2021, Action Fraud reported that over £63 million was lost to investment fraud on social media platforms, with victims reporting that they were mainly attracted to these investment scams through adverts[1].

The insurance industry is determined to do everything it can to protect consumers from being the victims of fraud. However, scams can range from non-existent motor insurance cover, being involved in a staged crash, to being offered bogus investment opportunities which could put someone's life savings at risk.

We support the aims of the Online Safety Bill and welcomed the inclusion of financial scams promoted by paid-for adverts in the scope of the Bill. This legislation could not be more urgent, as it comes at a time of significant increases in the cost of living and increased financial stress – and we know that fraudsters target and exploit people with low financial resilience.

However, to ensure the Bill delivers on the Government's ambition for the UK to be the safest country in the world to be online, we believe the provisions regarding paid-for digital advertising could be strengthened in several areas.

<u>Duties about fraudulent advertising</u>

We welcome the Association of British Insurers' (ABI) written evidence and support the recommendations they have made to strengthen provisions regarding paid-for digital advertising. We have set out some points below we believe should be addressed to ensure the Bill fully protects consumers from online fraud.

---

[1] Action Fraud | 26 May 2021 | New figures reveal victims lost over £63m to investment fraud scams on social media

Categorisation of online advertising providers

We are concerned that the current approach to categorising providers could create potential loopholes for fraudsters as each defined category would have a different duty to tackle scam advertisements, with some smaller providers not covered by the scope of the Bill.

Duties for search engines:

- In the current draft of the Bill, 'Category 1' providers, which are large 'user-to-user' sites such as Facebook and Twitter, have a legal duty to **prevent** individuals from encountering fraudulent advertisements. 'Category 2a' providers including search engines such as Google, are only required to **minimise the risk** of encountering fraudulent advertisements.
- There is a considerable risk of people encountering fraudulent adverts via search engines such as Google. For example, we know bond scam advertisements are most prevalent on search engines. Under the current scope of the Bill, there is a risk that fraudulent advertisements promoted via search engines would not get the urgent action required to protect people falling victim to this type of scam, which is particularly concerning given the impact on individuals. As an illustration, over 1,300 of these scams have been reported to Aviva, with an average loss per individual of £39,000.
- We would recommend 'Category 2a' providers are subject to the same legal duty as 'Category 1' providers to **prevent** individuals from encountering fraudulent advertisements.

'Category 2b' providers:

- Currently 'Category 2b' providers, which are smaller 'user-to-user' sites that host advertisements, are not included in the scope of the Bill. There is a risk that fraudsters will increasingly focus efforts on targeting consumers via these smaller sites if there is no legal duty for these providers to tackle paid-for fraudulent advertising.
- We would therefore recommend all providers that host paid-for advertisements are included within the scope of the Bill.

Ambiguous and unclear language

- We agree with the ABI that some ambiguous language could undermine the ambitions of the Bill.
- For example, terms such as **'minimise the length of time'** in Clause 34 (1) and **'minimise the risk'** in Clause 35 (1) are open to interpretation and place no legally defined action or duration on providers to address fraudulent paid-for advertisements.
- We recommend these examples are amended to ensure the Bill is enforceable and not open to interpretation by providers.

APPENDIX

Aviva's data shows that the most common types of fraud are:

- **The Policy Review** – a typical health and life insurance scam involves a cold call telling consumers to review their policy. The fraudsters will claim they're from a reputable insurance company or that they've been asked to do this by the regulators. They may offer lower premiums, but what they don't mention is that the lower premium also means reduced cover, often leaving the consumer with a worthless policy.
- **Pensions, Investment and Savings** – as stock markets have fallen in value and the Bank of England base rate still remains relatively low, people with investments are much more vulnerable to falling victim to scammers offering unrealistically high rates of return. People are usually offered a 'unique' investment opportunity or the chance to unlock cash in a pension.
- **Clone-firm Investment Fraud** – fraudsters set up imitation websites which look like well-known financial services brands, through which they sell bogus products. Victims of this type of fraud tend to be people approaching retirement age, who have access to their pension pot and are looking for better interest rates for their savings. We have received over 1,300 reports of this type of scam, while over 90% of the fraud that Aviva witnessed during the pandemic involved cloned investment fraud.
- **Application Fraud** – ghost broking is at the sharp end of application fraud and is when an unauthorised insurance intermediary fraudulently takes out motor insurance policies on behalf of people looking for cheap car insurance. Ghost broking is increasingly common, with our research showing that 21% of people have been approached by someone who they suspected was not an insurance broker, but who was claiming to offer access to cheap insurance. Young people aged 16 to 24 are the age group most targeted, with 43% saying they have received this type of approach.[2]

Aviva has a number of controls in place to help prevent or limit the impact of fraud, working closely with law enforcement agencies such as the National Crime Agency to report fraudulent activity, and involving them in sector wide problems identified through appropriate intelligence sharing.

We also launched an online Fraud Hub in May 2020, at the height of the pandemic, to help protect the public and our customers from scams. It provides practical advice on spotting scams and includes a reporting service for potential or actual frauds. Our Financial Crime Unit will investigate every reported incident and will provide customers with guidance on what action they can take.

[2] Aviva PLC | Aug 2021 | The Aviva Fraud Report