Written evidence submitted by the Association of British Insurers

ABI response to Digital, Culture, Media & Sport Sub-Committee on Online Harms & Disinformation Inquiry on Government's approach to harmful online content

About the Association of British Insurers

The Association of British Insurers is the voice of the UK's world-leading insurance and long-term savings industry. A productive and inclusive sector, our industry supports towns and cities across Britain in building back a balanced and innovative economy, employing over 310,000 individuals in high-skilled, lifelong careers, two-thirds of which are outside of London.

Our members manage investments of nearly £1.7 trillion, collect and pay over £16 billion in taxes to the Government and support communities across the UK by enabling trade, risk-taking, investment and innovation.

We are also a global success story, the largest in Europe and the fourth largest in the world.

The ABI represents over 200 member companies, including most household names and specialist providers, giving peace of mind to customers across the UK.

Executive Summary

1. Consumers' confidence is being eroded by the ongoing proliferation of online financial scams, including those predicated on impersonation of financial services providers. Both the insurance and long-term savings sectors are impacted by financial scams perpetrated via online paid-for advertisements, which can deprive vulnerable consumers of their life savings and leave deep emotional scars. While the inclusion of user-generated fraud within the Bill's scope is welcomed, it represents only a small proportion of online financial scams.

2. The government is wrongly gambling on the Online Advertising Programme, about which little is currently known, providing a framework for regulating paid-for advertisements. To date, advertising regulation has focused on the advertiser and content, rather than the publisher of the advert. The current approach has failed to stem the tide of scams, so it is right that statutory duties need be placed upon the tech companies hosting adverts. However, an initial consultation is not expected until the end of the year and this shift of approach will inevitably require an extended period of rigorous scrutiny, as well as legislation, before it comes to fruition. Moreover, unlike the Bill which gives Ofcom the power to impose eye-watering fines, it remains to be seen how robust any sanctions will be. In the meantime, many more consumers will be the victims of online fraud.

3. If the government is serious about meeting the Bill's central objective of making the UK "the safest place in the world to be online", then it must apply the Bill to paid-for advertisements and clone investment fraud.

4. The definition of 'harm' included in the draft Bill is vague. While we strongly agree that it is entirely appropriate that the risk of 'physical' or 'psychological' harm should be taken into account, using the well-established concept of a 'reasonable person' (rather than 'ordinary sensibilities') as the assessment standard would promote greater certainty.

5. Duties of care are the Bill's main regulatory mechanism for promoting online safety. It follows that such duties much be clear and avoid imposing conflicting requirements. Firms require clear guidance to be spelled out in codes of practice as to how they should approach potential conflicts and tensions and clarity as to whether responsibility for resolving them lies with themselves or the regulator.

6. The ABI is supportive of the appointment of Ofcom as the regulator for online safety. It is imperative that Ofcom is equipped with both adequate resources and technical expertise in order to regulate effectively and develops networks that enable it to engage and cooperate effectively with other regulators with online expertise so that there is a fully joined-up approach to the digital economy

7. The UK regime should look at principles and measures contained in overseas regimes and, in particular, how such regimes have evolved over time, with a view to conducting regular reviews to ensure the UK regime remains 'fit for purpose' in the fast-paced, ever changing digital world.

Consultation response

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

8. The content of the draft Bill largely reflects a change of focus, with the government looking to narrow and limit the scope and impact of the Bill. It is notable that the Bill references 'safety' on 294 occasions, compared to 195 mentions of 'harm'.

9. The government has emphasised that, during the COVID pandemic, digital technologies have brought huge benefits, including helping people to work remotely and stay in touch with family and friends. Moreover, the government has stressed that the framework of the new regime forms part of its pro-innovation approach to regulating the digital technologies.

10. The Bill imposes significant and multi-layered duties of care on user-to-user and search services with links to the UK, as well as duties focused on record-keeping and transparency. The duties relate mainly to illegal content which, in turn, largely encompasses child sexual exploitation and abuse (CSEA) and terrorism content – both topics with an obvious synergy with 'safety'.

11. The shifting focus to 'safety' aligns with the government's position in looking to exclude paid-for advertisements from the scope of the Bill. The inclusion of advertisements within scope would increase the compliance burden and costs for some tech businesses, as well as the regulator. But as the government recognised when it committed to tackling user-generated scams through the Bill, the costs to such businesses would be insignificant compared to the current cost of online scams including individuals losing their life savings[1]. Furthermore, if paid advertisements are not deemed in scope of the Bill, they will be regulated by the Online Advertising Programme. Given that the systems and processes the tech businesses would have to implement are unlikely to be substantively different from those for user generated content, including adverts within the

[1] DCMS. The Online Safety Bill. 2021

Bill would probably lead to significant cost and time savings for those businesses, as well as a clearer, more coherent regulatory regime.

Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

12. 'Harm' is defined vaguely in the Bill.

13. *"The provider […] has reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on a child (adult)"* .

14. We believe that the potential financial impact of any content should be included within the definition of harm. With the average victim of an investment scam losing over £45,000[2], financial harm should be included in the definition, not least because of the knock-on impact falling victim to a scam can have in an individual's mental health[3].

15. We strongly agree that it is entirely appropriate that the risk of 'physical' or 'psychological' harm should be taken into account. However, we note that harmful content for adults (other than designated priority content) includes content where the service provider has reasonable grounds to believe that there is a risk of the content having a significant adverse physical or psychological impact on an adult with ordinary sensibilities. The explanatory note clarifies that this would include short or long-term depression and anxiety. A similar definition is applicable to content that is harmful to children.

16. These are very subjective issues, requiring the provider to make value judgements. In particular, what would amount to an 'indirect' impact? Use of such nebulous language is likely to result in confusion for regulated services and an inconsistent approach across the technological sector and potentially put providers at risk of breaching 'freedom of expression' requirements.

17. Rather than use the vague concept of 'ordinary sensibilities' as the assessment standard, using the well-established standard of a 'reasonable person' (as adopted in criminal/tort cases in English courts) would promote greater certainty.

Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

18. We note and welcome that some tech companies have begun to implement due diligence measures[4] designed to prevent online scam advertisements. However, these are purely voluntary measures and further action is required to mandate these and supplementary obligations.

---

[2] Action Fraud 2020

[3] https://www.moneyandmentalhealth.org/publications/online-scams/

[4] E.g. Google has introduced measures that aim to ensure that advertisers are properly vetted before adverts are posted, and that adverts promoting unrealistic rates of return on investments are filtered out.

19. In July 2021, the DCMS published guidance[5] designed to help tech companies of various sizes find the information needed to build safe digital products from the development stages through to the user experience. The guidance outlines four safety by design principles, alongside a seven-point (non-mandatory) checklist on how to practically implement them.

20. The combination of tech companies effectively 'marking their own homework' through transparency reports, coupled with a vague definition of 'harmful content' gives rise to concern. The guidance asserts that companies should be careful to ensure that platform design does not limit a user's ability to make informed choices e.g. through using algorithms to recommend content that is harmful to a user, which they have no or limited control over changing. We believe that the Principle: '*Users are empowered to make safer decisions'* is therefore a vitally important check and balance.

What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

Uncertainty of Scope

Financial Scams

21. Consumers' confidence is being eroded by the ongoing proliferation of online financial scams, including those predicated on impersonation of financial services providers[6].

22. We strongly assert that paid-for advertising that promote online financial scams should be brought within scope of the Bill. This view is backed by a coalition[7] of consumer groups, charities and industry bodies, as well as the FCA, Bank of England, City of London Police, Work and Pensions Committee and Treasury Committee.

23. Both the insurance and long-term savings sectors are impacted by financial scams perpetrated via online paid-for advertisements, with the problem exacerbating during the pandemic as people look at ways of boosting their income or returns through attractive investment opportunities or making savings by securing cheaper motor insurance.

Connected call services ('Google Ad spoofing')

24. Following a road traffic accident, vulnerable motorists initiating a claim from the roadside on their smart phone are having their claims 'hijacked' by claims management services (CMS) 'impersonating' their insurer[8] through misleading websites. Scammers use psychological tactics to befriend, reassure and pressure

[5] https://www.gov.uk/government/collections/online-safety-guidance-if-you-own-or-manage-an-online-platform
[6] Impersonation scams now account for 37%of all FCA warnings issued since 2010.
[7] ABI, Age UK, Carnegie UK, The City UK, Innovate Finance, Investment Association, Money and Mental Health Policy Institute, Money Savings Expert, The People's Pension, PIMFA, UK Finance, Victim Support, Which?
[8] This may be either their own insurer or an at-fault driver's insurer to report a claim.

victims at a time of stress, while all the time collecting personal information for financial gain.

25. One insurer has seen the number of cases escalate from 3 pw (Q1 2018) to a peak of 40 pw (Q4 2020)[9]. A number of case studies are included in APPENDIX A.

26. The impact of these scams is significant and wide-ranging. Victims can be induced to enter into funding agreements where the CMS will take a sizeable cut of any damages awarded (e.g. up to 35%); unfavourable credit hire agreements (with rates 90% higher); inflated car recovery and storage fees; payment of unnecessary excesses to the repairer; fabricated rehabilitation fees; some victims can have their vehicles sold for salvage without consent; and others have incurred speeding fines relating to a time that the vehicle was supposed to be under repair/in storage.

27. Even when the victim directs the call to their actual insurer, it may be via a premium rate phone number, the costs of which escalate quickly[10].

28. In addition, insurers incur significant expenditure to outbid CMS's on mobile browser ad listings. One insurer experienced a 780% increase in google ad spend (H1 2021 compared to H2 2020) and the insurer's spend in June 2021 was 3611% higher than for January 2020. The position has now become untenable[11]. Moreover, since 2019, the FCA's google ad spend has exceeded £2m (including £240,000 in the first 4 months of 2021).

Clone investment scams

29. These scams occur when an investor is duped into believing that they are purchasing a genuine investment product from a reputable brand (the website of which has been cloned). Many insurers, banks and investment firms have been impacted, with scammers often using real employee names to reassure victims, many of which will be vulnerable inexperienced investors (rather than existing customers). A detailed explanation of how a typical scam is perpetrated is set out in APPENDIX A.

30. Beyond cloning, investment scams that do not abuse an existing brand and its reputation are even more common. While these do not affect our members directly, the scams result in extremely poor customer outcomes which harm trust in the entire industry, with funds that would be better off in a legitimate pension or investment.

31. Between September 2019-September 2020, Action Fraud received more than 17,000 reports of investment fraud, amounting to £657.4m in reported losses – a 28% increase on the same period the previous year. In 2020, Action Fraud reported that £78m was lost to brand cloning scams, amounting to an average and potentially life-changing loss of over £45,000 per victim[12]. One insurer has had 1284 bond

[9] The figures would be far higher. Many consumers remain oblivious to being scammed, are too embarrassed to report or the claims have been submitted by solicitors (though initiated by claims management services) so will not be included.

[10] Research by Which? found that a thirty minute call costs £112.50 on Sky; £124.50 on Three and £127.50 on Vodafone,

[11] CMCs' have improved their bid promotion strategy to enable their ads to be positioned even more prominently in the listings.

[12] In H1 2020, the Payment Services Regulator estimated losses to authorised push payment scams of £208m. UK Finance reported total losses of £479m in 2020.

scams reported to it[13], of which 174 cases suffered a financial loss (of over £7m). Additional costs are incurred by legitimate financial services providers in monitoring and responding to scam attempts, as well as potential reputational damage to the investment sector.

32. Aside from financial loss, victims of online scams can suffer deep emotional distress. People who have experienced mental health problems are three times more likely to have fallen victim to an online scam than the wider population (23% compared to 8%)[14]. Four in ten (40%) online scam victims have felt stressed and three in ten (28%) have felt depressed as a result of being scammed[15]. People with mental health problems also have lower typical incomes and comprise half of those in problem debt[16], meaning if a scam does result in financial losses, the harm caused can be severe.

33. Some clone investment fraud case studies are included in APPENDIX A.

34. The insurance and long-term savings industry have taken proactive measures to mitigate the financial scam threat, through consumer awareness campaigns, intelligence sharing and cross-industry engagement. And the FCA is ratcheting-up its proactive monitoring of the internet to aim to capture suspicious advertising within 24 hours after it first appears.

35. Yet existing laws have failed to keep pace with the criminals. Tech companies are currently under no obligation to identify the legitimacy of those placing adverts nor to take down harmful content. Moreover, they're spurred by the fees received for hosting fraudulent adverts, as well as fees they receive from the FCA and insurers to post warnings on platforms. As such, they essentially profit from these scams thrice.

36. The introduction of the draft Online Safety Bill presents the government with the perfect opportunity to play catch-up. While the inclusion of user-generated fraud is helpful, its impact in practice will be limited (see next Question: *'Limited impact of inclusion of user-generated fraud')*.

37. The government is gambling on the Online Advertising Programme, about which little is currently known, filling the void. To date, advertising regulation has focused on the advertiser and content, rather than the publisher of the advert. The current approach has failed to stem the tide of scams, so it is right that statutory duties need be placed upon the tech companies hosting the adverts. However, an initial consultation is not expected until the end of the year and this shift of approach will inevitably require an extended period of rigorous scrutiny, as well as legislation, before it comes to fruition.

38. Moreover, unlike the Bill which gives Ofcom the power to impose eye-watering fines, it remains to be seen how robust any sanctions will be. In the meantime, many more consumers will be the victims of fraud.

<u>Private messaging</u>

39. It is understood that services such as email, SMS and MMS are out of scope. However, it remains unclear whether 'private messaging' will fall in or out of scope.

---

[13] 28 Nov 2019-13 Aug 2021
[14] https://www.moneyandmentalhealth.org/press-release/vulnerable-people-online-scams/
[15] Holkar M, Lees C. Caught in the web. Money and Mental Health Policy Institute 2020
[16] Ibid

Definition of illegal content

40. The draft Bill does not specify 'illegal content' beyond terrorism and CSEA. The accompanying literature references racist hate crime and financial fraud – such as romance scams and fake investments. It is unclear what would constitute 'financial fraud', a term which would benefit from a clearer definition that is suitably wide to capture all online financial frauds – not just those relating to investment scams.

41. There are currently carve-outs in the Bill for Online Advertising and for clone investment scams, which we believe should be removed.

Thresholds for categories of service

42. We support the flexible approach which gives regulated services duties that correspond to their classification as Category 1, 2A or 2B, thereby ensuring that compliance obligations broadly align with the potential to create harm.

43. However, the draft Bill is light on detail. A proportionate approach would be further cemented through the provision of more detail in secondary legislation and codes of practice regarding the 'threshold conditions' or factors that are to be taken account of in determining categories of service. The secondary legislation should be laid at the earliest possible opportunity to engender greater certainty and allow regulated services sufficient lead in time.

Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

Exclusion from scope of paid-for advertisements

44. The exclusion of paid-for advertisements from scope of the Bill is not justified.

45. The government has stated that it wishes the Bill to focus on online activities that cause "emotional or physical harm". As we have outlined in addressing the previous question, the ABI is only too aware of the huge psychological damage caused to individuals who are conned into giving their life savings to a criminal. And, tragically, this can lead some victims to take their own lives.

46. If the government is truly serious about meeting the Bill's central objective of making the UK "the safest place in the world to be online", then it must bring paid-for advertisements within scope.

Limited impact of inclusion of user-generated fraud

47. In the wake of strong arguments made by the financial sector, the Bill helpfully captures user-generated fraud, such as social media platforms hosting content posted by a ghost broker peddling fake motor insurance. However, Action Fraud figures[17] show that less than 10% of online investment fraud losses emanate from social media platforms, so the vast majority of scams perpetrated via paid-for advertisements would not be caught.

[17] https://www.actionfraud.police.uk/news/new-figures-reveal-victims-lost-over-63m-to-investment-fraud-scams-on-social-media

48. Moreover, adopting different regulatory approaches to two types of content that people struggle to tell apart will, in practice, make monitoring, reporting and redress extremely difficult. The exclusion of scam adverts also creates grey areas and perverse incentives for scammers to create ad content[18].

Clarity of duties of care

49. Duties of care are the Bill's main regulatory mechanism for promoting online safety. It follows that such duties much be clear and avoid imposing conflicting requirements. This is challenging given that regulated services must conduct risk assessments relating to illegal content, while complying with duties relating to the right to freedom of expression and privacy. Category 1 Service providers have additional duties to protect adults from harmful content and protect 'content of democratic importance; and 'journalistic content'.

50. Firms require clear guidance to be spelled out in codes of practice as to how they should approach potential conflicts and tensions and clarity as to whether responsibility for resolving them lies with themselves or the regulator.

Ofcom: resourcing and expertise

51. While ABI is supportive of the appointment of Ofcom as the regulator for online safety, given that service providers are required to make judgement calls on issues such as harmful content, they will inevitably rely on Ofcom for direction. It is imperative that Ofcom is equipped with both adequate resources and technical expertise in order to regulate effectively.

52. Ofcom must also develop networks that enable it to engage and cooperate effectively with other regulators with online expertise so that there is a fully joined-up approach to the digital economy. The creation of the Digital Regulation Cooperation Forum – comprised of OFCOM, the Competition and Markets Authority and the Information Commissioner's Office - is a positive step forward for regulatory dialogue in the digital arena. The UK Plan for Digital Regulation, which sets out the government's overall vision for governing digital technologies should also help to shape a more coherent regulatory landscape.

What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

53. The government has stated its intention to engage with international partners to learn from their experiences and build consensus around shared approaches to tackling online harms that uphold the UK's democratic values and promote a free, open and secure internet.

54. The government expects Ofcom to take an international approach - working with other international regulators – to ensure effective enforcement and promote best practice at a global level.

---

[18] For example, while the government intends the Bill to cover online romance scams, some dating apps allow people to pay to promote their profile, potentially taking the content outside the Bill's scope.

55. Many overseas countries are developing new regulatory approaches[19] to tackle online harms, prompted by the growth of online pollution[20] globally. However, many overseas pieces of legislation tend to focus on one aspect of online harms. For example, Germany's Network Enforcement Act 2017 requires online platforms (with >2m registered users) to remove 'manifestly unlawful content' which contravenes specific elements of the German Criminal Code (e.g. holocaust denial and hate speech). Similarly, in May 2020, France adopted law to tackle the spread of hate speech. In Australia, an e-safety Commissioner has been appointed with responsibility for promoting the online safety of all Australians – the focus being on the provision of information to make consumers more aware of scams and to establish a complaints service on cyber bullying for young people.

56. The proposed UK regime appears to be more comprehensive than many overseas approaches in that it recognises that online harms occur that fall short of the criminal standard and aims to enforce some online activity which is not illegal but does cause harm (in addition to criminal law). Each piece of overseas legislation may, however, contain principles and measures that help to inform the UK approach, and many appear to be subject to regular review. In learning lessons, the UK must look at how overseas regimes evolve over time, with a view to conducting regular reviews to ensure the UK regime remains 'fit for purpose' in the fast-paced, ever changing digital world.

57. There is merit in the UK government – as well as regulated service providers – tracking the progress of the EU's proposed Digital Services Act (DSA). While the focus of the DSA is on online intermediaries' obligations in relation to the removal of illegal (not harmful) content, illegal content is more widely drawn than under the draft Bill (extending, for example, to infringing intellectual property rights). The DSA will likely form the key framework from which a global model can emerge on how online platforms are expected to deal with illegal user content. We note that the DSA will apply where there is a 'substantial connection to the EU', so certain providers will find themselves in scope of both and having to put in place appropriate processes which comply with both the EU and UK regimes.

58. Services that have 'links to the UK' fall within scope of the Bill. It is vital that the UK cooperates effectively with overseas peers, firstly, to ensure that in-scope services emanating from overseas are compliant; and, secondly, so that UK consumers are not potentially prejudiced by international providers looking to prevent access by UK users in order to avoid the legislative burden of the Bill. We note that UK is a member/signatory to a number of international initiatives[21] and this should help to engender collaboration and cooperation.

ABI September 2021

[19] For example, the EU GDPR; Germany's Network Enforcement Act; Australia's Violence Amendment Act; California's Consumer Privacy Act.
[20] Disinformation; manipulation; harassment; privacy breaches
[21] e.g. the International Advisory Committee to the Global Internet Forum to Counter terrorism

APPENDIX A

CASE STUDIES

The following case studies represent a snapshot of the cases some of our members have seen on both the general insurance and long-term savings side of the industry.

Connected call services

Insurer A

Customer called **A** to complain that they were charged £46.93 by their phone company to report an accident to **A**. Investigations revealed the customer had googled "Insurer A phone number" and was directed to a premium rate number which charged £3.63 pm.

Almost a week after the road traffic accident, the customer contacted **A** for an update. **A** had no claim reported so had been unable to progress repairs to the insured's car. Investigations revealed paramedics who attended the scene of the accident googled **A**'s Claims Number to assist the insured following the accident. The customer called the number but was directed to a claims management company (CMC) from the advert impersonating **A**. The customer is elderly and had put his trust in the CMC thinking it was **A** so had signed documents to provide him with credit hire and repairs which he would have been personally liable for. **A** has since taken over conduct of this claim for the insured and dealt with his repairs under the terms of his policy.

The customer googled **A**'s claims number from the scene of the accident and unwittingly dialled a number for a CMC thinking it was **A** due to the advert wording. The CMC arranged recovery of the car from the scene of the accident. The customer subsequently called **A** to complain about delays in settlement of their total loss claim but **A** had no knowledge of the claim. **A**'s investigations revealed the CMC had put the customer in a replacement credit hire car and sold the customer's own car without their knowledge. The customer went on to receive a speeding fine and parking tickets for his car that he thought was being stored securely by **A**.

The customer clicked the top link on smart phone, which took them to a website which auto-dialled a CMC (that the customer thought was **A**). The operative said he worked in 'claims', but was careful to avoid explicit reference to **A**. The customer quickly received a Docusign link to legal documents which they were urged to complete straightaway. The customer's son became suspicious and the customer phoned **A** and was advised that no claim had been reported. **A** immediately called a recovery company to get the vehicle returned. The customer was subsequently bombarded with confusing calls from the CMC which was vague as to its identity. **A** then received a claims notification form stating that the customer had instructed the CMC to handle claim. The CMC also tried to sign-up the customer to a Damages-Based Agreement (DBA) and an 'After the Event' legal expenses policy, despite the customer already having cover.

Insurer B

Having googled **B** at the scene of accident, the claimant then received a call from who she believed was **B** but was actually an accident management company (AMC). The claimant was later apparently threatened by the AMC and told **B** she could not deal with B as she was engaging with solicitors. The claimant suffered anxiety, sleep loss and significant weight loss as a result of pressure being applied by the AMC to pursue the claim against **B** or settle it herself. **B**'s claims handler did as much as possible to assist the claimant. The claim is now closed. Court proceedings were not issued against **B**.

The claimant had their claim 'hijacked' by an AMC. The claimant submitted documents that the AMC sent to **B** that differed from the documents the claimant had in their possession. The claimant signed an agreement for a courtesy car (which they believed **B** would pay for) but was provided with a credit hire car which the AMC said the claimant would have to pay for. Note also that the hire car claimed for was different (Range Rover, not Ford Kuga – with daily rates £100 higher). The insurers involved cooperated to defeat the AMC's claims and support the victim.

Insurer C

The customer thought they had called Insurer **C** to log their claim but had contacted an accident management company. There were delays authorising the repairs. The customer called **C** for an update. **C** advised the customer that it had not instructed the AMC. The customer is a carer for an extremely vulnerable person and desperately required their vehicle to provide the necessary care.

The customer thought they had called **C** but had contacted an AMC. Despite later speaking with **C**, the customer decided to continue to process the claim using the AMC as they were concerned they would incur costs with the AMC for cancelled services (e.g. credit hire; ongoing personal injury services). There was a three-week delay in the AMC handling the claim, which the insurer could have prevented if permitted to intervene.

<u>Investment scams</u>

The following scenario describes a typical investment fraud case:

Typically, if someone searches for an investment opportunity online by searching key-word phrases such as 'high return investments' or 'best rate ISA' into a search engine, there are two scenarios that can occur, with both potentially leading to harm:

First, if a consumer clicks on one of the adverts that appears, they will often be taken to an 'investment' comparison website. The site will often contain a disclaimer at the bottom

of the webpage, which states that the content of the financial promotion is not authorised under the Financial Services and Markets Act 2000, but that if the individual wishes to participate in the promotion, they must declare themselves as 'high-net worth' or 'sophisticated' under Section 48 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005.

After inputting their contact details, someone will get in touch offering an investment opportunity, which is generally high-risk and often has extremely high fees and charges attached. While there are many legitimate reasons for 'high-net worth' and 'sophisticated' individuals to be exempt from certain requirements around financial promotions, and while this is not against the law, it is concerning that consumers are not being made fully aware of the significance of certifying themselves as 'high-net worth' or 'sophisticated', or indeed are not being made aware at all that they are certifying themselves as 'high-net worth' or 'sophisticated' and this is causing harm to occur.

Second, should an individual click on one of the adverts that appears, they may be taken directly to a fake website advertising a non-existent investment product, or a range of investment products, using the 'clone' of a legitimate financial services firm. This is a clear scam, and the scammer will use the same logo as that of a reputable financial services firm and may use genuine marketing materials from that firm.

Potential investments include non-existent bonds for household brand names, often with generous rates of return above 5%, but they can also be genuine commercial or government debt instruments, with genuine International Securities Identification Numbers (ISIN), but which in reality are not available to retail investors.

After the individual has input their contact details into the website, they will be contacted by someone pertaining to be calling from the regulated firm featured on the fake website. There have even been examples of individual financial advisers and investment managers from legitimate firms being impersonated by scammers, often through details obtained from the FCA register, including senior management functions entries.

The scammers will often emphasise that the investment opportunity is fully covered by the FCA and/or the FSCS and will often require a minimum investment of around £50,000, with a 'bonus' if they invest over a certain amount. Once the money is deposited into the fraudster's account, it is quickly moved again into a number of other accounts to make it much harder to trace. The victim often does not even realise they have been scammed for many months, and it is only when they do not receive their first interest payment or return on their money that they become suspicious.

Once the scam is detected, the scammers will close the site down, but may then set up a new website using the name of a different provider, advertising a slightly different investment opportunity.

Insurer D

A husband and wife aged 80, searched the internet for investment opportunities. They registered their details on a comparison website expressing interest about a **D** fixed rate bond. The rate on offer was just above or on a par with the best rates going at that time (so they had no thoughts of "it's too good to be true")

They received a call from a UK based person claiming to be from **D**. They had no cold calling concerns as they had been expecting some contact. Cloned emails and documentation were sent over several days which followed a "normal" sales pattern i.e. prospectus, fund guides, application forms. The emails and brochures were very professional and looked completely legitimate.

They decided to invest £30,000 and completed an application form and provided copies of their ID. They later received login details (which worked), mails confirming checks had been undertaken and finally a request for payment, along with receipts after payment made and policy documentation. There was nothing to suggest there was anything untoward. There was no pressure to pay by a certain date. Any calls they made were answered professionally and there were no red flags.

8 months later, still unaware of the scam, the consumers received a letter from Trading Standards explaining they had been scammed and that a separate firm had been appointed to help them retrieve their money. The consumers called the firm and were convinced to pay a further £3,000 in order to secure the release of their initial funds. It was only when they tried to pay the additional £3,000 that their bank informed them the letter was a scam. Trading Standards also confirmed the letter was fake.

The consumers contacted **D** who confirmed they did not have a £30,000 investment with them. **D** advised the consumers to follow up with their bank and also the police. The consumers explained that the investment had been earmarked to be used to visit family in the US and were deeply distressed that they could have lost it all. Further guidance was given to the consumers by **D** after their bank initially said they would not reimburse them with the original £30,000. The bank later paid this sum back to the consumers.

Insurer E

E spoke to an 84 year old lady a number of times to provide support. She lost £20,000 to the scam and has talked about having violent nightmares since this occurred. The lady had talked to **E** about the loss of her husband in 2019 and how she has always tried to be self-sufficient. From the conversations with her, it's clearly been a distressing time and she has talked about the lack of trust and the suspicion she now holds.

An elderly couple lost £160,000 to the scam earlier in the year. **E** provided them with all the support information and, using that, they were able to get their full amount returned by their bank. **E** spoke to the wife recently to follow up on the scam, to which she advised that the day before the money was recredited, her husband suffered a stroke, which they both firmly believe was brought on by the stress they have experienced because of the scam.

A consumer invested £50,500 into a fictitious product. He contacted **E** and had thought for months it was genuine and was planning to use the invested money to buy his house. **E** provided support and all relevant information regarding the scam and is pursuing with his bank. The bank account that the individual paid was previously identified and reported to

the bank as part of the scam.

Insurer F

Mr S entered his contact information into a website which he believed to be legitimate following an internet search. Mr S was then contacted by an individual asking whether he was interested in investing in investment bonds.

Mr S stated that he wasn't interested in bonds, but rather that he was interested in investment platforms. A few weeks later he was contacted again and was offered the chance to invest using an investment platform.

Following the phone conversations with a fraudster, he then invested £5000 into the platform. He was given a website address and was able to 'track' his investment on the platform. Initially the website suggested that his investments had made large gains. He was contacted again to invest more.

Due to the individual's background in IT, Mr S thought he would use his knowledge to review the website where the investment platform was based; following this in depth review he was able to identify that the investments and prices he was seeing were fictional and through this he realised he was a victim of a scam.

Mr S tried to contact the individuals who had contacted him previously and the website where he had made the investment; sadly, this proved impossible, and he was unable to regain his lost funds.

Mr S was an ex-serviceman who was severely disabled and was receiving daily physiotherapy. Having provided his information, it is widely believed that Mr S is on a list of vulnerable individuals whom fraudsters would contact to continue to commit fraud.

Mrs K used a search engine to research potential investments. She searched for 'investment bonds' and through an advert identified a bond from a well-known supermarket which was purported to be sold by **F** within the search engine results.

She clicked the link provided on the website, which had a similar brand identity to that of **F.** She entered her contact details and was promptly contacted by an individual pertaining to be from **F**, wanting to discuss the investment bonds.

Mrs K was interested and was promptly sent literature by the individual which had a similar look to literature provided by **F**. After considering the proposition, Mrs K invested £80,000 into the bond. She was advised that the investment would pay interest payments in twelve months.

After 12 months, Mrs K hadn't received the interest payments so decided to contact **F**. It was at this point that the fraud was identified and sadly, **F** had to advise Mrs K that she did not hold an investment with **F** and had been a victim of a scam.

Mrs K is an elderly, vulnerable individual who had invested £80,000 into an 'investment bond' without her family's knowledge, and the loss severely impacted her retirement plans. **F** provided and guidance to Mrs K and her family on the next steps

Mr J is an elderly retiree who searched the internet for investment ideas. Following an internet search, he clicked on an advert for investment bonds which caught his attention due to the rate of interest being offered.

Clicking the link, the website looked like that of a legitimate financial services firm, **F**. The website appeared to promote bonds in leading supermarkets which were paying good rates of interest. All an investor needed to do was to enter contact information and a representative would be in touch as to how they could make an investment.

Mr J entered his information and was shortly contacted by a representative who provided information on the investment bond and stated they would send through literature for Mr J to consider. The documentation received looked legitimate and seemed to have the requisite regulatory notifications.

Mr J decided to invest £50,000 as this was the minimum investment amount into one of the bonds on behalf of his wife, Mrs J. There was a delay as the third party stated there were inconsistencies between the information sent by Mr/Mrs J and the bank. Mrs J provided a scanned copy of her bank statement. The investment was then made, and the money was sent to the third-party bank details as detailed in the application.

In the intervening period, **F** became aware that its brand was being cloned and placed a warning on its website. Mrs J noticed the warning and contacted **F** to be sadly told that her and her husband had been the victim of a scam.

F provided support to Mrs J as to what she could do and who she should report the loss to. It is worth considering that the Js also provided bank account details and their identity information and so could have become recurrent victims of impersonation fraud.

Following guidance provided by **F**, Mrs J was able to reclaim the money lost from her bank.

Association of British Insurers
September 2021