Written Evidence: September 2021

Joint Scrutiny Committee on the draft Online Safety Bill

Introduction

Which? welcomes the publication of the draft Online Safety Bill and the announced intention to include fraud within its scope. It is right that the government recognises that the major online platforms we interact with every day have a legal responsibility to protect their users from this type of criminal activity.

However, we have several concerns regarding the draft Bill as currently written, and the government's approach to tackling fake and fraudulent content that can lead to a scam more broadly.

At Which? we regularly undertake investigations and consumer research which uncover harms to consumers. Our work in the area of online safety has exposed that online fraud perpetuated by fake and fraudulent content is one of the most frequent and damaging types of consumer harm experienced online.

We welcome the opportunity to share this insight and to provide written evidence to the Joint Scrutiny Committee. Our response below focuses on the questions most relevant to consumers.

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

Scams and fraud are now some of the most prevalent forms of crime in the UK[1], with reported incidents up by 33% over the past year, resulting in a total loss to victims of £2.3bn.[2] In addition to the financial impact of being scammed, Which? research has found this type of crime to have serious consequences on victims' emotional and physical wellbeing.[3]

Consumers are not adequately protected from fraud online. Whilst online platforms have taken some voluntary measures to address this, they have not done enough to protect consumers and to stop fraudsters from exploiting their sites in the first place. The draft Bill

[1] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
[2] https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/
[3] https://www.which.co.uk/news/2021/03/devastating-emotional-impact-of-online-scams-must-force-government-action/

should give online platforms a legal responsibility to identify, remove and prevent fake and fraudulent digital content that leads to a scam, in order to meaningfully protect consumers from illegal activity and harm.

Without the inclusion of this type of illegal content in scope of the draft Bill, the policy aim of *"making the UK the safest place to be online"* is entirely unattainable.

Furthermore, it is imperative that the draft Online Safety Bill ensures that existing laws around legal liabilities of online platforms which benefit and protect consumers are not prejudiced by its implementation.

With this in mind Which? proposes an amendment to the draft Bill to ensure that consumer laws, such as the Consumer Protection from Unfair Trading Regulations 2008[4], are not inadvertently undermined by the legislation. Under **Clause 18 - Duties of care: supplementary** an amendment reading: "(2A) This Chapter is without prejudice and subject to any enactment or rule of law that imposes on providers of search services a more extensive duty or liability in relation to the prevention of harm to, or provision of redress for, individuals" should be inserted on page 17, after line 34.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

As it is currently drafted, **Section 9(3)** of the draft Bill imposes:

> *(3) A duty to operate a service using proportionate systems and processes designed to—*
>
> *(a) minimise the presence of priority illegal content;*
> *(b) minimise the length of time for which priority illegal content is present;*
> *(c) minimise the dissemination of priority illegal content;*
> *(d) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.*

The language around take down times is ambiguous and is unlikely to make clear to services in scope what their obligations are. It also places the emphasis on removing content once it has already been posted. Which? wants to see the creation of *"systems and processes"* that stop illegal content from appearing on online platforms in the first place, and enable content to be blocked from being reuploaded. The emphasis here must be on a proactive approach

[4] https://www.legislation.gov.uk/uksi/2008/1277/contents/made

of identifying, blocking and preventing the misuse of online platforms by the networks of criminal and 'bad actors', rather than a solely reactive approach of identifying and removing illegal content which has already been posted and therefore already exposed consumers to potential harm.

Whilst there may be a view that identifying fake and fraudulent content can be easily done by looking at the content of the post/advert, we understand that this is highly unreliable. Methods such as forensic linguistics and discourse analysis are in their infancy when it comes to fraud detection, making identifying fake and fraudulent content based on language unreliable at this stage. However, Which? understands that there are a range of technical measures that are currently used in the detection of illegal and harmful content online such as behavioural analytics, Open-Source Intelligence (OSINT) and hash-sharing databases that enable identification of criminal behaviour more reliably than the monitoring of content. Crucially these methods focus on looking for patterns of behaviour; patterns which tend to identify networks as opposed to individuals. We understand that these methods are used by a range of businesses already, but at present are not being deployed by the platforms to a standard or level to meaningfully tackle the problem of fake and fraudulent content. With a requirement for platforms to collaborate with each other on information sharing and working together to develop ways to identify and solve the problem of the networks of criminal and 'bad actors' we believe the prevention of criminal activity before the event, not after, has real potential to tackle the issue of fraud and scams online.

Identifying the networks of criminals and 'bad actors' can also be undertaken by requiring verification processes for businesses seeking to advertise. Which? expect to see the requirement for platforms to undertake verification of advertisers, ahead of paid-for adverts being published, for example using the Know Your Business Customer (KYBC) principle. By using the KYBC principle, platforms can ensure that anyone paying for adverts are legitimate and seek to engage with consumers in a good faith. Which? believes that KYBC verification would act as a protection mechanism and would reduce fake and fraudulent content appearing on platforms.

At present, online platforms rely in part on consumers reporting fake and fraudulent content to them and yet reporting tools are often hard to find and fail to keep consumers informed. Where illegal content does end up on online platforms, platforms should provide easy-to-use reporting tools for consumers. Online platforms reporting tools are often difficult to find, not always user-friendly and do not provide enough information, if any, on how the report will be handled. In many cases there is no explicit option to report content for being fake or fraudulent. Which? research uncovered in the case of the Facebook scam ad reporting tool, only 30% of survey respondents were aware of the tool, with only 10% having used it.[5] One of the reasons given for low use was the lack of confidence that reports would be acted

[5] https://www.which.co.uk/policy/digital/6514/connectingfraudsters

upon. When fake and fraudulent digital content does appear online, there should be improved tools and signposting to reporting tools across the platforms.

Which? also questions the general approach of the draft Bill to moderating content given that it focuses on user-generated content, the definition in the draft Bill reads:

(3) "User-generated content", in relation to a user-to-user service, means content—
(a) that is—
(i) generated by a user of the service, or
(ii) uploaded to or shared on the service by a user of the service, and
(b) that may be encountered by another user, or other users, of the service by means of the service.

Further detail is provided in the draft Online Safety Bill: Explanatory Notes in **point 235:**

Subsection (3) defines *"user-generated content"* as *"content that is generated by a user of the service, or uploaded to or shared on the service by a user of the service, and which may be encountered by another user (or users) by means of the service. For example, this would include anything posted on a forum or social media network; a direct message from one user to another; or a file stored in shared cloud storage."*

The definition is overly broad and Which? questions how content moderation could meaningfully work at this scale without amounting to general monitoring obligations on online platforms; obligations which would profoundly undermine protection of consumers' rights to privacy[6], data protection[7], and freedom of expression.[8] Furthermore, it is clear from the explanatory notes that the scope of user-generated content extends to communications and storage of data which consumers would consider to be 'private' and 'secure' (whether subject to encryption or not).

The battle to prevent fraud online is absolutely critical, but must not lead unintentionally to a reduction in protections for consumers. The government must be absolutely clear therefore that any *"systems and processes"* employed to tackle fraud perpetrated through user-generated content will be accompanied by robust protections to ensure that consumers rights to privacy, data protection and freedom of expression are not undermined.

[6] Article 8, European Convention on Human Rights
[7] Rights of the data subject, Data Protection Act 2018
[8] Article 10, European Convention on Human Rights

The draft Bill specifically includes CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

Whilst we welcomed the announcement that measures to tackle fraud will be in the legislation[9], it is not clear on the face of the draft Bill exactly how fraud will be tackled. The government needs to make absolutely clear how the legislation will cover this. Given the scale and severity of the harm, and to ensure that consumers benefit from the highest standards of protections that the draft Bill proposes, Which? believes that fraud should be designated as priority illegal content.

The draft Bill indicates in **44 Regulations under Section 41** that:

(1) When deciding whether to specify an offence, or a description of offence, in regulations under section 41, the Secretary of State must take into account—

(a) the prevalence on regulated services of content that amounts to that offence or (as the case may be) offences of that description,

(b) the level of risk of harm being caused to individuals in the United Kingdom by the presence of such content, and

(c) the severity of that harm

As previously stated, fraud is experienced by consumers on a huge scale and the impact can be devastating. When determining whether the content amounts to an offence, Which? has analysed case studies of fraud and scams reported to us through our consumer advice lines and has found that the fraud consumers experience online are criminal offences under a range of existing English and Welsh laws including:

- Fraud Act 2006
- Consumer Protection from Unfair Trading Regulations 2008
- Companies Act 2006
- Financial Services and Markets Act 2000
- Computer Misuse Act 1990
- Malicious Communications Act 1988
- Communications Act 2003

The following case studies, published by Which?, detail some of the scams consumers have reported to us to show how this type of illegal content should fit into the scheme of the draft Bill.

---

[9] https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

Case studies relating to fake and fraudulent digital content

Purchase scam case study[10]
Which? was contacted by an individual who had been scammed following engagement with an advert on Facebook for a Little Tikes clearance sale. The advert linked to a website that was convincingly branded to look like the official Little Tikes website, the individual paid £105 for a climbing frame which never arrived and the website has since disappeared.

Legal analysis
This example is likely to amount to an offence under Sections 1 and 2 of the Fraud Act 2006, in the making of a false representation. It may also be an offence of fraudulent trading under Section 993 of the Companies Act 2006, or (if a sole trader) under Section 9 of the Fraud Act 2006. The creation of a fake website for use in a scam could be an offence of making articles for use in frauds under Section 7 of the Fraud Act 2006 (which specifically includes any data held in electronic form). There are also several potential offences under the Consumer Protection from Unfair Trading Regulations 2008, including under regulation 8 (general requirement of professional diligence) and regulation 9 (misleading actions).

Investment scam case study[11]
A consumer contacted Which? informing us that she had lost a total of £70,000 to scammers impersonating two legitimate firms; Prudential and Macquarie Bank, following an online search for a better savings rate. Despite checking the firms out and finding them well established, the sites were impersonations which conned her out of £75,000. She told Which? that she was "totally mortified" by the experience and needed help from her GP.

Legal analysis
This may amount to criminal offences under Financial Services and Markets Act 2000 (such as Section 23 offence of carrying on (or purporting to do so) a regulated activity without being either authorised to do so or exempt.

[10] https://press.which.co.uk/whichpressreleases/nearly-one-in-10-have-fallen-victim-to-scam-adverts-on-social-media-or-search-engines-as-platforms-fail-to-adequately-protect-users-which-finds/

[11] https://press.which.co.uk/whichpressreleases/fraudsters-run-riot-as-search-engines-fail-to-adequately-protect-users-from-scams-which-reveals/

Impersonation scam case study[12]
In 2020, the Which? Money helpline heard from someone who lost almost £8,000 after calling a phone number supplied on a fake Revolut Google advert. He received an email from the bank asking him to resubmit his ID because it had expired. Aware that these emails can be dangerous, he searched for a Revolut number on Google and called the number provided to confirm its authenticity. The person he spoke to said he could confirm his identity digitally there and then. Confident that he had called the right number and was speaking to a Revolut adviser, he was transferred to a manager and downloaded a remote-access tool called TeamViewer QuickSupport. This tool gave them access to his mobile phone, on the understanding that they needed to verify his account transfer limits using a dummy account within his Revolut app. Ultimately, the scammers transferred a total of £7,938 out of his account.

Legal analysis
This may amount to fraud, unfair trading, and financial services offences. There are likely to be offences here committed under the Computer Misuse Act 1990 (Sections 1-3) and the Data Protection Act 2018 (Sections 170-173).

Whilst Which? believes that fraud should be designated priority illegal content given the severity of the harm, Which? also has significant concerns about *how* priority illegal content will be handled by the draft Bill. As the draft Bill is currently written, priority illegal content will be designated in secondary legislation. We have strong reservations about the lack of transparency and the undemocratic nature of this process and recommend that any secondary legislation introduced must be subject to effective and meaningful scrutiny by both Houses of Parliament.

Which? proposes that, for certainty and transparency, a core list of offences constituting priority illegal content (similar to the list in Schedule 3 of child sexual exploitation and abuse related offences) is included in the Bill itself, by means of a Schedule if appropriate. Additional offences could then be specified in regulations where justified in due course if evidence of new forms of harmful illegal behaviour emerges. However, regulations concerning priority illegal content under **Section 41** should always be subject to affirmative Parliamentary scrutiny procedures and the draft Bill should be amended to reflect this. Which? therefore proposes that under **Clause 132 - Regulations** the addition of a line in subsection 4 *"(c) regulations under section 41"* and the deletion of line 33 *"(a) regulations under section 41,"* on page 112 and line 1 "*(a) section 41,*" on page 113.

[12] https://www.which.co.uk/news/2020/05/revolut-customers-targeted-with-scam-texts-and-malicious-google-ads/

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

As it is currently written, the draft Online Safety Bill will apply to user-generated content *"except- (f) paid-for advertisements".* Which? is strongly opposed to this exclusion.

Paid-for advertising on online platforms is a primary method used by criminals to target consumers and engage them in a scam[13], as it gives them instant access to large numbers of target audiences and is the way in which many consumers fall victim to scams[14], as illustrated in the case studies above. Prominent types of scams enabled by paid for adverts include investment scams, pension scams and purchase scams.

Which? investigations have repeatedly uncovered impersonator ads appearing in Google search results for the insurance and investment firm Aviva[15] and financial technology and banking company Revolut.[16] These impersonator ads would be likely to amount to criminal offences, for example under the Fraud Act 2006, the Financial Services and Markets Act 2000 or the Consumer Protection from Unfair Trading Regulations 2008.

Which? also undertook an investigation which demonstrated how easy it is for a fake or fraudulent advert to appear on Facebook and Google.[17] The ease and speed with which a series of adverts for a fake product could be created, posted and be seen by consumers was alarming, with adverts for fake products going live quickly with very few checks and gaining many impressions. The investigation exposed a clear lack of effective controls by Facebook and Google to identify, remove and prevent fake and fraudulent content from appearing on their sites. The changes Google made earlier this year with regard to verification, will not have resolved this issue - if an advert can go live within a matter of hours and stays live for 30 days before the verification process is fulfilled, consumers still remain vulnerable to exposure of widespread criminal acts.

This criminal activity can result in people losing devastating and life changing amounts of money. One victim lost almost £100,000 after clicking on an online investment advert featuring fake celebrity endorsements from Martin Lewis and Deborah Meaden,[18] while another lost £160,000 after clicking on an ad for an 'Aviva' investment scheme. Losses to clone investment scams - that involve fraudsters setting up adverts and websites replicating

[13] https://www.which.co.uk/news/2021/03/investment-scammers-run-riot-on-search-engines-while-victims-pay-the-price/
[14] https://www.which.co.uk/news/2021/03/investment-scammers-run-riot-on-search-engines-while-victims-pay-the-price/
[15] https://www.which.co.uk/news/2020/09/browser-beware-how-scam-advertisers-use-google-to-lure-their-victims/
[16] https://www.which.co.uk/news/2020/09/google-fails-to-stop-scam-ad-targeting-revolut-users-for-a-third-time/
[17] https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/
[18] https://press.which.co.uk/whichpressreleases/which-calls-for-action-over-emotional-and-financial-toll-of-online-scams-as-tech-giants-fail-to-adequately-protect-users/

those of legitimate firms - average £45,000.[19] Yet online platforms continue to profit from fraudulent activity on their sites.

The case for including fraud that is enabled through paid-for advertising online in the draft Online Safety Bill is overwhelming, with industry, consumer groups and law enforcement[20], regulators[21], key Select Committees[22] and The Bank of England[23] all agreeing that urgent action is needed to require online platforms to do more to tackle fraud and scams.

The exclusion of paid-for advertising therefore must be removed from the draft Online Safety Bill.

Which? proposes two amendments to **Clause 39 – Meaning of "regulated content", "user-generated content" and "news publisher content",** specifically to delete Line 3 on page 35:

"(f) paid-for advertisements (see subsection (7)), and"

and lines 34-41 on page 35:

(7) An advertisement present on a user-to-user service or (as the case may be) in search results is a "paid-for advertisement" if—

> *(a) the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and*
> *(b) the placement of the advertisement is determined by systems or processes (human or automated) that are agreed between the parties entering into the contract relating to the advertisement.*

Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

In order for this legislation to best serve consumers it must include robust enforcement powers, including sufficient information gathering powers for regulators. Regulators must be able to hold firms responsible for the criminal activity that takes place on their platforms and as such, the draft Bill should be amended to include a criminal liability for senior managers.

[19] https://www.which.co.uk/news/2021/03/investment-scammers-run-riot-on-search-engines-while-victims-pay-the-price/
[20] https://conversation.which.co.uk/wp-content/uploads/2021/05/Open-Letter-Scams-and-the-Online-Safety-Bill.pdf
[21] https://www.fca.org.uk/publication/business-plans/business-plan-2021-22.pdf
[22] https://committees.parliament.uk/publications/6956/documents/72760/default/
[23] https://committees.parliament.uk/publications/5304/documents/52929/default/

An amendment to **Clause 115 - Review** of the draft Bill deleting lines 1-4 (subparagraph (b)) on page 102 and to insert in **Clause 140 - Commencement** on page 118/119 after line 6 "(ja) section 71 (jb) section 73" and deleting lines lines 19-24 will introduce senior manager liability and ensure senior manager liability provisions are brought into effect immediately.

The draft Bill should also be amended to include a requirement for businesses to have a nominated legal representative in the United Kingdom, to reduce barriers to enforcing against an online business.

This can be achieved in **Clause 127 – Extra-territorial application** on page 110 with the insertion after line 2 of:

> "(4A) The provider of a regulated service within the meaning of subsection 3(5) or 3(6) but which does not have its main or principal establishment in the United Kingdom must nominate in writing a natural or legal person as its representative in the United Kingdom for the purpose of assisting with compliance with the provisions of this Act on behalf of the provider.
> (4B) The provider must provide its nominated legal representative with the necessary powers and resources to assist with compliance with the provisions of this Act and the legal representative may be held liable for any failures in this respect, without prejudice to any liability of the provider or any other person."

Lessons learned from financial services regulation, especially the senior managers' liability and certification regimes, demonstrate that making senior managers personally liable for compliance acts as an effective way to ensure firms, including those that operate internationally, remain accountable for the criminal activity their companies facilitate. Without these amendments it is unlikely regulators will be able to carry out their statutory duties successfully.

Furthermore, to support Ofcom in its role, Which? is calling for expert groups such as consumer groups like Which?, and others with relevant expertise such as technical specialists, academics, and NGOs to be consulted to ensure protections for consumers are meaningful and evidence based. There are a number of ways in which the draft Online Safety Bill should be amended to provide for this.

The draft Bill currently gives the Secretary of State a 'Henry VIII' power to amend Schedule 1 by regulations to add to the categories of user-to-user and search services that are exempt from the requirements of the draft Bill. However we believe this should only be employed after consultation with the regulator and relevant bodies, such as Which? and those representing other consumer or internet user groups. An amendment should be made

to reflect this in order to ensure a reasonable safeguard for consumers. **Clause 3 - Meaning of "regulated service"** should have inserted on page 3 after line 8:

> "(8A) Before making any regulations under subsection (8), the Secretary of State must consult OFCOM and bodies representing the interests of:
> (a) individual users of regulated services;
> (b) consumers;
> (c) members of the public; and
> (d) particular groups of such users, consumers or members of the public."

Similarly, Ofcom should be required to consult appropriate stakeholders in relation to carrying out their functions, as it is required to do in other situations. For example, Ofcom is required to consult members of the public under section 271 of the Communications Act 2003 on amending public service remits. The draft Online Safety Bill should contain a similar requirement. Which? proposes the addition to **Clause 97 - Guidance about enforcement action** on page 89 at the end of line 18 of:

> ", which must include bodies representing:
> (i) individual users of regulated services;
> (ii) consumers;
> (iii) members of the public; and
> (iv) particular groups of such users, consumers or members of the public."

Consumer representatives should also be included as an eligible entity that can make super-complaints to Ofcom as consumer organisations are a key source of information about widespread instances of harm to users of online services that would be regulated by this legislation. As such Which? recommends the following amendments to the draft Bill, in **Clause 106 - Super-complaints** on page 96, in line 13 after 'services' insert ",consumers", in line 14 after 'users' insert ", consumers", at the end of line 33 insert "consumers" and in line 34 after 'users' insert ", consumers." Also, in **Clause 107 - Super-complaints: procedure** insert the sentence "which must include the requirement that OFCOM must respond to complaints under section 106 within 90 days" at the end of line 3 on page 97.

About Which?

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member subscriptions. We're not influenced by third parties – we never take advertising and we buy all the products that we test.

For more information, please contact Katie Lips at katie.lips@which.co.uk.

September 2021

Annex (proposed amendments to the draft Online Safety Bill)

Ask: require consultation before exempting services **Where:** Part 1 - Overview and key definitions **Clause 3 - Meaning of "regulated service"** **Amendment:** Page 3, after line 8 insert: "(8A) Before making any regulations under subsection (8), the Secretary of State must consult OFCOM and bodies representing the interests of: (a) individual users of regulated services; (b) consumers; (c) members of the public; and (d) particular groups of such users, consumers or members of the public."
Ask: insert without prejudice clause **Where: Clause 18 – Duties of care: supplementary** **Amendment:** Page 17, after line 34 insert: "(2A) This Chapter is without prejudice and subject to any enactment or rule of law that imposes on providers of search services a more extensive duty or liability in relation to the prevention of harm to, or provision of redress for, individuals".
Ask: remove the exclusion of 'paid-for advertising' **Where:** Part 2 — Providers of regulated services: duties of care Chapter 6 - Interpretation of Part 2 **Clause 39 – Meaning of "regulated content", "user-generated content" and "news publisher content"** **Amendment:**

Page 35, leave out line 3 (subparagraph(f))

Page 35, leave out lines 34-41 (paragraph (7))

Ask: require consultation for the regulator

Where:

Part 4 - OFCOM's POWERS AND DUTIES IN RELATION TO REGULATED SERVICES

Chapter 6 - Enforcement powers

Clause 97 - Guidance about enforcement action

Amendment:

Page 89, at the end of line 18 insert:

", which must include bodies representing:

(i) individual users of regulated services;
(ii) consumers;
(iii) members of the public; and
(iv) particular groups of such users, consumers or members of the public."

Ask: Which? to be given super-complaint powers

Where:

Part 5 - APPEALS AND SUPER-COMPLAINTS

Chapter 2 - Super-complaints

Clause 106 - Super-complaints

Amendment:

Page 96, line 13, after 'services' insert ", consumers"

Page 96, line 14 after 'users' insert ", consumers"

Page 96, line 33 at end insert "consumers"

Page 96, line 34 after 'users' insert ", consumers",

Ask: Which? to be given super-complaint powers

Where:

Part 5 - APPEALS AND SUPER-COMPLAINTS

Chapter 2 - Super-complaints

Clause 107 - Super-complaints: procedure

Amendment:

Page 97, at the end of line 3, insert:

"which must include the requirement that OFCOM must respond to complaints under section 106 within 90 days".

Ask: introduce senior manager liability

Where:

Part 6 – SECRETARY OF STATE'S FUNCTIONS IN RELATION TO REGULATED SERVICES

Clause 115 - Review

Amendment:

Page 102, leave out lines 1-4 (subparagraph (b))

Ask: introduce requirement for a nominated legal representative in the United Kingdom

Where:

Part 7 – GENERAL AND FINAL PROVISIONS

Clause 127 – Extra-territorial application

Amendment:

Page 110, after line 2, insert:

"(4A) The provider of a regulated service within the meaning of subsection 3(5) or 3(6) but which does not have its main or principal establishment in the United Kingdom must nominate in writing a natural or legal person as its representative in the United Kingdom for the purpose of assisting with compliance with the provisions of this Act on behalf of the provider.

(4B) The provider must provide its nominated legal representative with the necessary powers and resources to assist with compliance with the provisions of this Act and the legal representative may be held liable for any failures in this respect, without prejudice to any liability of the provider or any other person."
Ask: subject regulations to parliamentary scrutiny procedures **Where:** Part 7 – GENERAL AND FINAL PROVISIONS **Clause 132 - Regulations** **Amendment:** Page 112, after line 24, insert: "(ca) regulations under section 41," Page 112, leave out line 33 (subparagraph(a)) Page 113, leave out line 1 (subparagraph(a))
Ask: ensure senior manager liability provisions are brought into effect immediately **Where:** Part 7 – GENERAL AND FINAL PROVISIONS **Clause 140 - Commencement** **Amendment:** Page 118, after line 6, insert: "(ja) section 71 (jb) section 73" Page 118, leave out lines 19-24 (paragraph 4)