

The Rt Hon Priti Patel MP
Home Secretary
Home Office
2 Marsham Street
London, SW1P 4DF

The Rt Hon Oliver Dowden CBE MP
Secretary of State for Digital, Culture, Media and Sport
Department for Digital, Culture, Media and Sport
100 Parliament Street,
London, SW1A 2BQ

05 May 2021

Dear Home Secretary and Secretary of State,

Scams and the Online Safety Bill

We are writing to you regarding the forthcoming Online Safety Bill. We urge the Government to expand the scope of this vital legislation to include fake and fraudulent content that leads to scams. This would better protect people against the devastating financial and emotional harm caused by these crimes.

As a group of organisations championing consumers, and representing civil society and several sectors of the economy, including banking and financial services, we recognise how essential online services have become in people's daily lives as a result of changes in the past year.

There are now more people spending more time online and the benefits of this are significant. We are determined that people can continue to make the most of this shift and fundamental to this will be ensuring their safety online.

Yet there is a problem because the existing laws and regulations designed to protect consumers in the online world have failed to keep pace with criminals in this modern arena. This is particularly the case in relation to scams, where fraudsters are increasingly taking advantage of online platforms to target victims.

Online platforms play a pivotal role in enabling criminals to reach and defraud internet users through the hosting, promotion and targeting of fake and fraudulent content on their sites, including adverts that they make significant profits from. Yet platforms have very little legal responsibility for protecting their users, despite often being the best placed to tackle harmful content.

To illustrate the size of this problem, ONS data shows there were 3.7 million incidents of fraud between March 2019 and March 2020, making it the crime that adults are most likely to fall victim to in the UK, while Action Fraud figures show £1.7 billion was lost to scams in the last year.

UK Finance data shows that across scam types, there has been a significant rise in cases over the past year, with criminals adapting to target victims online. As an example, there was a 32 per cent increase in investment scam cases in 2020, which are often promoted through adverts on search engines offering higher than average returns, and a 38 per cent increase in cases of romance scams, driven by the rise in online dating during the pandemic.

These figures are likely a significant underestimate of the true value and do not take into account the fact that even when the victim is reimbursed, criminals still retain illegal proceeds, reinvesting them in further organised illegal activity, causing wider societal harm. Nor do they capture the equally devastating emotional impact that scams have on victims. Even if people are able to get their money back after falling victim, they can still experience significant emotional harm. Four in ten (42%) Money and Mental Health Research Community respondents who had fallen victim to an online scam felt that they had experienced a major negative impact on their mental health. Vulnerable people, including those experiencing mental health problems, are also more at risk of falling victim to these crimes.

Across industry, regulators and consumer groups, there is now wide-ranging consensus on the urgent need for action to tackle scams and the critical role that online platforms must take in protecting users from the harm caused by fake and fraudulent content.

We believe that fake and fraudulent content that leads to scams must be included in scope of the proposed Online Safety Bill. This would require online platforms to identify, remove and prevent fake and fraudulent content from being hosted on their sites, putting in place incentives for platforms to work together with the telecoms, banking and finance sectors to tackle economic crime.

While we recognise there are initiatives being progressed by the Government designed to tackle aspects of online fraud, there is a growing risk that current plans for future regulatory frameworks are not taking a comprehensive approach to the threats faced by consumers and do not reflect the extent or urgency of the problem.

We remain committed to working with the Government on this vital issue, toward our shared ambition for the UK to be the safest place in the world to be online, so that people and businesses continue to benefit from the shift to digital.

Copies of this letter go to the Minister for Digital and Culture, the Minister of State at the Home Office, the Minister for Pensions and Financial Inclusion, the Economic Secretary to the Treasury and the Minister for Patient Safety, Suicide Prevention and Mental Health.

Yours sincerely,

Caroline Abrahams
Charity Director,
Age UK



Huw Evans
Director General,
Association of British Insurers



Adam Farkas
CEO,
The Association for Financial
Markets in Europe (AFME)



William Perrin
Carnegie UK Trust Trustee



Catherine McGuiness
Chair of Policy and Resources
Committee
City of London Corporation



James Thomson
Deputy
Chair, City of London Police
Authority Board



Clinton Blackburn
T/Commander for Economic Crime,
City of London Police



Janine Hirt
Interim CEO,
Innovate Finance



Chris Cummings
CEO,
The Investment Association



Helen Undy
Chief Executive,
Money and Mental Health Policy
Institute



Martin Lewis
Founder of
MoneySavingExpert.com and
the Money and Mental Health
Policy Institute

MoneySavingExpert.com

Liz Field,
Chief Executive
Personal Investment Management &
Financial Advice Association



Patrick Heath-Lay
Chief Executive,
B&CE Ltd, provider of the People's Pension



Miles Celic
Chief Executive,
TheCityUK



David Postings
CEO,
UK Finance



Diana Fawcett
Chief Executive,
Victim Support



Anabel Hoult
CEO,
Which? UK



ONLINE SCAMS: Evidence of the scale, the growth and the devastating impact on victims and society

Key data at a glance

According to ONS data, there were 3.7 million incidents of fraud between March 2019 and March 2020, making it the crime that adults are most likely to fall victim to in the UK.

The incidence of online scams

- Recent nationally representative polling from Money and Mental Health Policy Institute found that 1 in 25 respondents (4%) had fallen victim to an online scam in the six months after the start of the first lockdown (between March and August 2020), equating to approximately 2 million people across the UK.
- A Which? survey of investment scam victims found that four in 10 were targeted via online methods, including 10% via search engines and 9% through adverts on Facebook.
- A separate Which? survey found that almost one in 10 people (9%) have fallen victim to a purchase scam as a result of an advert on social media. The same proportion of people (9%) had also fallen victim to a scam via an advert on a search engine.
- Money and Mental Health's research suggests six in ten people (63%) have seen an advert that leads to a scam online and half of people (50%) see them at least monthly.
- Research from Money and Mental Health shows that six in ten people (58%) report having seen user-generated content online that could lead to a scam, for instance a post from a friend or someone they follow on social media. More than four in ten people (43%) report seeing user-generated content that leads to a scam at least monthly.

The impact of online scams

- Which? analysis of Action Fraud data found that there are 300-350 fraud reports a week from victims showing signs of severe emotional distress – up to 18,000 reports a year.
- Research from Money and Mental Health shows that four in ten (40%) victims felt stressed and three in ten (28%) have felt depressed as a result of being scammed.
- Money and Mental Health's research also shows that people who have experienced mental health problems are three times more likely than the rest of the population (23% versus 8%) to have been a victim of an online scam.
- As part of Age UK research looking at the long-lasting impact of scams, they heard from older victims and their children about the effect of online fraud on family relationships, at a time when they were more vulnerable due to mental health conditions and dealing with bereavement.

Our coalition of consumer and industry voices strongly support the inclusion of fake and fraudulent content that leads to scams within the scope of the Government's upcoming Online Safety Bill.

Background

This submission sets out key evidence detailing the incidence and impact of scams that originate online, including those that are enabled by fake and fraudulent content posted on online platforms, such as search engines, social media sites and online marketplaces.

The insights included in this document are based on data, research and analysis from a range of organisations from across law enforcement, industry and civil society, including Action Fraud, the Money and Mental Health Policy Institute, UK Finance and Which?.

As a coalition of organisations, we recognise that tackling scams is complex, requiring collaboration across government departments, regulators, law enforcement and several sectors of the economy, including the banking industry, telecoms firms and the tech sector.

We also recognise that the internet is now an essential part of daily life for most people and that this has brought significant benefits. We want to ensure that people can continue to make the most of the opportunities presented by this shift while guaranteeing their safety online.

That is why we are concerned by the clear trend we have witnessed in recent years, that has seen scams shifting online. Yet our laws and regulations designed to protect consumers have failed to keep pace with the criminals. The online platforms used by scammers to target victims have very little responsibility for preventing fake and fraudulent content from being posted on their sites or targeted at individuals and are failing to adequately protect their users.

These companies, which are some of the world's leading innovators, do not currently have the right incentives, regulatory or otherwise, to use the sophisticated skills and technology they possess to be part of the solution to protecting consumers, rather than remaining part of the problem. The tech sector must do more to help protect consumers.

We believe that fake and fraudulent content that leads to scams must be included in scope of the Government's upcoming Online Safety Bill. This would give online platforms legal responsibility to identify, remove and prevent fake and fraudulent content from being hosted on their sites. If not, the Government must set out its plans for further legislative action to effectively protect consumers from scams online. We are concerned that current initiatives do not reflect the scale or urgency of the issue.

The case for including the devastating financial and emotional harm caused by scams in this vital legislation is overwhelming. We share the Government's objective of making the UK the safest place in the world to be online. Expanding the scope of the Online Safety Bill to cover content that leads to scams would represent a significant step toward this.

The incidence of scams enabled by content on online platforms

Online platforms play a critical role in enabling criminals to reach and defraud internet users through content hosted on their sites. Recent nationally representative polling from Money and Mental Health found that 1 in 25 respondents (4%) had fallen victim to an online scam in the six months after the start of the first lockdown (between March and August 2020), equating to approximately 2 million people across the UK.

Consumers now face a staggering and growing variety of scams when navigating the digital world, with scammers using an increasingly sophisticated range of tactics and guises as the "hook" to dupe people, as well as different channels to target victims, including both paid-for and free content on online platforms.

Prominent types of online scams include investment scams, romance scams, pension scams, insurance scams and purchase scams. Scammers use an array of tricks online such as fake celebrity endorsements to lure in victims, as well as setting up fake websites and impersonating legitimate ones.

A series of recent surveys carried out by Which? and Money and Mental Health indicates the scale of scams that are being enabled by content posted on online platforms. This includes:

- A survey of investment scam victims found that four in 10 were targeted via online methods, including 10% via search engines and 9% through adverts on Facebook.
- A separate Which? survey found that almost one in 10 people (9%) have fallen victim to a purchase scam as a result of an advert on social media. The same proportion of people (9%) had also fallen victim to a scam via an advert on a search engine.
- Money and Mental Health's research suggests six in ten people (63%) have seen an advert that leads to a scam online and half of people (50%) see them at least monthly.

As well as fake adverts, research from Money and Mental Health shows that six in ten people (58%) report having seen user-generated content online that could lead to a scam, for instance a post from a friend or someone they follow on social media. More than four in ten people (43%) report seeing user-generated content that leads to a scam at least monthly.

The volume of scam-enabling content that has been found on online platforms underlines why they must be required to introduce improved systems for preventing fake and fraudulent content from appearing on their platforms.

The impact of scams enabled by content on online platforms

Scams and fraud are now the most prevalent types of crime in the UK, not only resulting in growing numbers of people losing life-changing sums of money but also taking a significant emotional toll on victims and even causing serious harm to people's mental and physical health.

Types of scams that are commonly enabled online¹

Investment scams

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. These scams are often promoted through adverts on search engines offering higher than average returns and lead to cloned or fake websites impersonating investment firms.

- In 2020, more than £135 million (an increase of 42% from 2019) was lost to investment scams, affecting nearly 9,000 victims.
- The nature of the scams means that the sums involved in individual cases can be high, so while investment scams accounted for only 6% of the total number of APP scam cases, they accounted for 28% of the total value of all APP fraud.
- Criminals have been increasingly preying on people's financial insecurities during the pandemic through investment scams promising high returns. Some criminals may initially pay out returns on their victim's investment to convince them to invest more.

Purchase scams

In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media platform.

- Purchase scams were the most common form of APP scam in 2020, with the 78,720 cases accounting for 52 per cent of the total number of APP scam cases.
- A total of £57.1 million was lost to purchase scams in 2020, with the vast majority of losses being from personal accounts.

Romance scams

In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media, dating websites and apps or gaming sites, and with whom they believe they are in a relationship.

- A total of £21.2 million was lost to romance scams in 2020 (an increase of 17% from 2019), affecting nearly 9,000 reported victims (32% higher than 2019) - driven by the rise in online dating during the pandemic.
- The nature of the scam means that the individual is often convinced to make multiple, generally smaller, payments to the criminal, as indicated by an average of around five payments per case.

The emotional harm on victims

An often overlooked yet no less significant consequence of scams is the emotional impact they have on victims. A Which? review of 15 research papers and datasets from across the world found that serious emotional harm from fraud can occur irrespective of whether the victim lost money or was reimbursed and that the emotional impact is often considered to be as or more significant than the financial losses suffered by consumers.

¹ All figures used in this section refer to fraud statistics and data published in UK Finance's Fraud – The Facts 2021 report (available [here](#))

These findings are supported by Which? analysis of Action Fraud data that found there are 300-350 fraud reports a week from victims showing signs of severe emotional distress – up to 18,000 reports a year.

In relation to online scams specifically, research from Money and Mental Health Policy Institute shows that four in ten (40%) victims felt stressed and three in ten (28%) have felt depressed as a result of being scammed.

Criminals target vulnerable consumers

Criminals target vulnerable consumers in particular, employing grooming techniques to do so. This is evidenced by research from Money and Mental Health, which shows that people who have experienced mental health problems are three times more likely than the rest of the population (23% versus 8%) to have been a victim of an online scam.

This targeting is also seen in the types of scam-enabling content that people have commonly reported seeing during the pandemic, including posts about financial assistance, fake mental health treatments and Covid-19 cures or vaccines, suggesting that scammers are targeting those who are struggling financially or with their mental and physical health.

A survey of Money and Mental Health's Research Community (comprised of people with lived experience of mental health problems) found that four in ten (42%) respondents who had fallen victim to online scams felt that they had experienced a major negative impact on their mental health, with one scam victim reporting, "My depression got worse as I felt so stupid for falling for it and it put me further in debt. I attempted suicide shortly after that."

This is of serious concern at a time when more consumers are more vulnerable due to the coronavirus crisis and the changes to people's lifestyles this has brought - that scammers have been quick to adapt to.

Unless online platforms are required to actively tackle this problem, the harm consumers suffer from scams they are exposed to online will continue to grow with devastating consequences for people, in particular, those in vulnerable circumstances.

APPENDIX: BIBLIOGRAPHY

Money and Mental Health

1. Caught in the web: Online scams and mental health (December 2020) - <https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf>
2. Safety Net: Breaking the link between online financial harms and mental health problems (March 2021) - <https://www.moneyandmentalhealth.org/wp-content/uploads/2021/03/Safety-Net.pdf>

The People's Pension and The Police Foundation

1. Protecting People's Pensions: Understanding and Preventing Scams (September 2020) - <http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/preventing-pension-scams-sep20.pdf>

UK Finance

1. 'Fraud the Facts' (March 2021) - <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf>

Which?

1. 'Investment scammers run riot on search engines, while victims pay the price' (March 2021) - <https://www.which.co.uk/news/2021/03/investment-scammers-run-riot-on-search-engines-while-victims-pay-the-price/>
2. 'Devastating emotional impact of online scams must force government action' (March 2021) - <https://www.which.co.uk/news/2021/03/devastating-emotional-impact-of-online-scams-must-force-government-action/>
3. 'Nearly one in ten scammed by adverts on social media or search engines' (November 2020) - <https://www.which.co.uk/news/2020/11/nearly-one-in-ten-scammed-by-adverts-on-social-media-or-search-engines/>
4. Connecting the world to fraudsters? (October 2020) - <https://www.which.co.uk/policy/digital/6514/connecting-fraudsters> Which? research into consumers' awareness of and attitudes towards the risk of scams on social media.
5. 'Your life for sale: stolen bank details and fake passports advertised on social media' (April 2020) - <https://www.which.co.uk/news/2020/04/your-life-for-sale-stolen-bank-details-and-fake-passports-advertised-on-social-media/>