HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 9214, 20 May 2021

Consumer protection: online scams

By Lorraine Conway

Contents:

Contents

Summary

Online scams come in many forms and through different channels. Advances in technology have enabled scammers to become increasingly sophisticated in their online methods. For example, phishing emails and copycat websites can trick individuals into giving out their personal bank details. Although anyone can be the victim of a scam, vulnerable people (such as the elderly and those with learning difficulties or dementia) are especially susceptible. All scams should be reported to Action Fraud and to Trading Standards (via the Citizens Advice online portal). However, many scams go unreported due to the victim's embarrassment or shame.

On 28 April 2021, during a Westminster Hall debate on online scams, Victoria Atkins, the Parliamentary Under-Secretary of State for the Home Department, said that the Government recognised the impact that fraud can have and is having on victims:

> According to the latest figures, fraud accounted for over a third of all estimated crime in the year ending September 2020 and, […], behind the statistics there is the trail of misery that these losses can encompass. Victims suffer both financial loss and emotional harm. There can be consequences for their livelihoods, their homes and their families' futures. We also know that the money that has been stolen from them can often go on to fund other serious and organised crimes.

The Government had previously not intended to include financial harms in its upcoming regulatory framework for online safety. However, regulators, such as the Financial Conduct Authority (FCA) and the Financial Services Compensation Scheme (FSCS), called on the Government to extend the scope of the Bill. It was argued that failing to tackle online scams would leave gaping holes in consumer protection, impacting on some of the most vulnerable people in society.

On 12 May 2021, the draft Online Safety Bill, announced in the Queen's Speech, was published. Crucially, it has been widened in scope to include user-generated fraud.

This Commons Library briefing paper is concerned with online scams. In addition to looking at the scale of the problem, it considers the different types of scams, who are the targeted victims, and what is being done to combat them.

1. Introduction

Amidst all the advantages of the internet, online shopping, and electronic banking for customers, the undoubted 'fly in the ointment' is the prevalence of online fraud. The 2019 Financial Cost of Fraud report estimates the cost of fraud to the UK equates to £130 billion each year.[1]

The Fraud Act 2006 provides for a general criminal offence of fraud with three ways of committing it, which are by false representation, by failing to disclose information and by abuse of power. Colloquially, "fraud" may be described as a scam, swindle, con, hoax, trick, or extortion. Regardless of how it is described, the intent is the same, to use "trickery is used to gain a dishonest advantage, which is often financial, over another person".[2] Online fraud can be anything from identity theft, online transactions, dating scams, copycat websites and more, all designed to trick the individual and take their money.

The compromise of personal and financial data remains a significant driver behind fraud losses:

> Customer details are being stolen through data breaches by third parties outside the financial sector, while sophisticated "digital skimming" attacks are being used to steal card data when consumers are shopping online. Criminals also continue to use social engineering techniques to trick customers into divulging their personal information or transferring money.[3]

According to the Office for National Statistics, people are more likely to be the victim of fraud or cyber offences above any other crime. Anyone can be the victim of online fraud, suffering significant financial harm. However, where the targeted victim is vulnerable, for instance the elderly, the emotional impact of fraud can be significant and long lasting.

This paper deals only with online scams, however, the following Library briefing papers may also be of interest:

- Regulating online harms (CBP 8743)
- Junk mail (CBP 5762)
- Nuisance calls: unsolicited Sales and marketing, and silent calls (CBP 6033).

1 The Financial Cost of Fraud 2019, Jim Gee and Professor Mark Button, Crowe and University of Portsmouth, [online] (accessed 20 May 2021)
2 What is fraud and cybercrime? Action Fraud [online] (accessed 20 May 2021)
3 App Scams Voluntary Code: Seven launch signatories to the code continue "no blame" interim funding to 31 March 2020, UK Finance, undated, [online] (accessed 20 May 2021)

2. Statistics: how big is the problem?

Most online scams will appear in statistics as cybercrimes or fraud. The Office for National Statistics has analysed the "Nature of fraud and computer misuse in England and Wales: year ending March 2019" and has summarised the main points as follows:

- The Crime Survey for England and Wales (CSEW) shows that there were an estimated 3.8 million incidents of fraud in the year ending March 2019, with evidence of a rising trend that is also seen in other data sources.
- While fraud victimisation showed little variation across different demographic groups, the likelihood of being a victim was generally lower in older age groups and greater in higher income households.
- In 63% of fraud incidents, there had been no contact between the victim and the offender; the most common methods of contact were online or by email (14%) or by telephone (11%).
- In 76% of fraud incidents, the victim incurred a financial loss and of these, the majority of victims (58%) lost less than £250.
- Around one in seven (15%) fraud incidents were reported to Action Fraud or the police; the most common reason given for not doing so was that the incident was reported to financial authorities instead. The CSEW also showed there were an estimated 1.0 million incidents of computer misuse in the year ending March 2019, having fallen over each of the last two years.
- Around one in five (21%) computer virus incidents resulted in access to files or data being lost and in around one in eight (12%) incidents, a demand for money to release files or data was made.
- The majority of adults took precautions to keep safe online (for example, deleting suspicious emails without opening them) and the proportions of adults taking such precautions has risen.[4]

Key statistics on fraud and cybercrimes reported to Action Fraud are available in a new interactive dashboard, the data is updated each month. Action Fraud figures show that, in the year to June 2020, 85% of all fraud was cyber-enabled.[5] Victims lost more than £78 million to clone scams in 2020.[6]

Authorised push payment (APP) scams, in which the victim transfers money into the bank account of the criminal, remain the second largest type of payment fraud (after card fraud), both in the volume of scams

4 Office for National Statistics, "Nature of fraud and computer misuse in England and Wales: year ending March 2019 – Summary of the various sources of data for fraud and computer misuse and what these tell is about victims, circumstances and long term trends ", [online] (accessed 20 May 2021)
5 HC Deb 28 April 2021 c161WH
6 Ibid

and value of losses.[7] According to UK Finance (a trade body for the banking and finance industry), 66,247 cases of APP fraud were reported in the first half of 2020 with losses of £207.8 million.[8] It is estimated that in 2017, only 25% of the funds lost to APP scams were successfully returned to victims.[9] The Financial Services Compensation Scheme (FSCS) is currently reporting at least one phishing attempt and one fake investment website per day, which it believes is the tip of the iceberg.[10]

In its report on payment industry fraud, Fraud – The Facts 2021, UK Finance analysed the level of cybercrime based on its analysis of 26.5 billion transactions from July to December 2020. An extract from this report, in which various trends are identified, is reproduced below:

> Sadly, the pandemic environment has provided rich pickings for fraudsters, in the form of new-to-digital consumers, heightened vulnerabilities and anxieties, as well as new channels to exploit.
>
> Within the Digital Identity Network, we've seen transaction volumes across financial services grow by 29 per cent globally and 15 per cent in the UK (always considered a frontrunner in its online banking maturity curve). We've also seen growth in online banking registrations across web and mobile during the first UK lockdown period.
>
> Interestingly, corresponding attack rates are down overall, year-on-year, indicating that fraudsters are turning their attention to other, potentially easier targets, such as new lines of credit and Covid-19 stimulus packages, that are not recorded in the Digital Identity Network.
>
> In addition, the UK online banking profile within the Digital Identity Network is more mobile than ever, with more than 85 per cent of transactions originating from a mobile device. From a fraud perspective, banking via a mobile app is the safest way to transact – with a much lower attack rate than either mobile or desktop browser transactions. The main point of vulnerability remains the device registration; compromise here leads to the keys to the kingdom.
>
> This broad picture, however, belies the fact that organised, networked fraud plays a pernicious role in the UK financial services landscape, both at a macro level in the form of organised mule rings, and at a micro level, of individual fraudsters using scams to dupe unsuspecting customers.[11]

---

7 Fraud – The facts 2020 – The definitive overview of payment industry fraud, UK Finance, (undated) [online] (accessed 20 May 2021)
8 Ibid
9 Ibid
10 Financial Services Compensation Scheme (FSCS), The worrying rise in online financial scams", 12 May 2021, [online] (accessed 20 May 2021)
11 UK Finance, Fraud – The Facts 2021 – The Definitive Overview of Payment Industry Fraud, [online] (accessed 20 May 2021)

3. Common types of online scams

Online scams come in many forms. Scammers might contact a victim via email, social media (Facebook, Twitter etc), or messaging services. Often, scammers will direct the victim to a fake website or trick them into downloading malware, which corrupts their computer. According to the National Crime Agency (NCA), fraud is the most commonly experienced crime in the UK and "data breaches continue to be a key enabler of fraud".[12] Some examples of common online scams are provided below.

3.1 Authorised push payment (APP) scams

As already mentioned, APP scams are when customers are tricked into authorising a payment to an account that they believe belongs to a legitimate payee – but is in fact controlled by a criminal. APPs are made at the request of the customer and can be carried out over the phone, online, or in person. Other examples of APP scams include:

- "malicious payee" (e.g. tricking someone into purchasing goods which don't exist or are never received), or
- "malicious redirection" (e.g. a scammer impersonating bank staff to get someone to transfer funds out of their bank account and into that of a criminal).

A new industry voluntary code, the Contingent Reimbursement Model Code for Authorised Push Payment Scams (known as the CRM Code), launched in 28 May 2019, provides consumer protections against APP fraud. Detailed information is provided at **Section 4.3** of this paper.

3.2 Phishing

Phishing emails or social media messages try to trick a person into giving out personal information or bank details. Examples of phishing emails identified by the consumer body Which? include:

- **Security scams**, which usually involves an unsolicited phone call supposedly from a "security expert" offering to fix a person's PC.
- **Government scams**, whereby fraudsters send convincing emails that pretend to be from a government agency (such as HMRC). The scammers ask the potential victim to provide their bank details, usually by clicking on a link.
- **Trusted organisations**, whereby scammers contact a person claiming to be their bank or other organisation (such as PayPal, Amazon, or eBay). The scammer will claim the victim's account has been compromised and ask them to verify their security details to keep the account open. Usually there is a link in the message that directs the victim to a fake website (which can look exactly like the real organisation's site) where they will be asked to log in. This gives the scammer the victim's account details and

[12] National Crime Agency, Fraud, (undated) [online]

passwords, enabling them to access his/her bank account or online shopping account.

3.3 Computer virus online scam

A scammer contacts the potential victim by email urging them to follow a link or open an attachment. If the victim acts on this instruction, and clicks on the link or attachment, it releases a virus which attacks the victim's computer. The virus effectively enables the scammer to access the computer and scan it for private data.

3.4 Copycat websites

Some private companies set up websites deliberately designed to look like official government sites and then charge people for services that are available directly from the Government either at no cost or for a much lower fee (e.g. renewing a driving licence or passport). It is not unlawful to provide reviewing and forwarding services, but businesses should make it clear on their websites that they are not affiliated to the Government and that people will be paying extra for this service. The Advertising Standards Authority (ASA) may investigate misleading websites and, if there is evidence of wrongdoing, impose sanctions.

In some cases, phishing emails, instant messaging, or posts on social media (e.g. Facebook and Twitter) direct a potential victim to a copycat site. To facilitate the deception, scammers will create duplicates of government websites (e.g. DVLA, HMRC, Passport Office). Some scams involve sending an email purporting to be from HMRC saying a tax refund is due, the recipient is then instructed to click on a link to a fake website where their personal data is harvested.

3.5 Clone sites

Clone scams exploit people's trust in reputable brands by carefully mimicking their websites and online presence. When adverts appear on Google, Facebook or other online platform, many consumers believe that it is an official advert from the company in question.

Brand cloning also involves financial products. The FSCS states that criminals clone well-known financial services brands to produce fake adverts, documents, and websites. They then use targeted online adverts and false price comparison websites to reach people searching for products such as pensions and ISAs. The FSCS describes how this approach tricks people into transferring their money to scammers:

> These same fraudsters often use the FSCS logo or protected badge without our permission to deceive their targets into believing that their non-existent products are protected.
>
> Other scammers impersonate FSCS and offer compensation for losses the customer never had or for products that FSCS does not protect or that do not exist. They trick people into paying for compensation that will never arrive by taking a fee for a claim they will never process for a loss that never existed.
>
> Action Fraud recently reported that more than £78 million was lost to brand cloning scams in 2020, which amounts to an

> average – and life changing – loss of £45,242 per victim. The FCA issued more than 1,000 scam warnings in 2020 and 40% of these involved clones or impersonations of legitimate financial services brands.[13]

3.6 Investment scams

According to the FSCS, scam investments are often marketed through internet search engines and social media, and "low interest rates help to drive consumers to look for higher returns, which makes them more vulnerable to adverts and websites offering attractive rates of return."[14] The FSCS states that it is particularly concerned by the increasing number of search results and online advertisements for fake investment bonds touted by fake firms.[15]

3.7 Online pension scams

Losing pension savings is a devastating experience, and many pension scams operate online. The Pension Scams Industry Group (PSIG), a voluntary body set up to combat pension scams, estimates that 40,000 people were scammed out of pension savings in the 5 years after the introduction of the pension freedoms and lost £10 billion between them.[16]

The FSCS is also concerned about the number of online adverts aimed at those in or approaching retirement. It said:

> These victims of fraud face little or no prospect of recouping their money and often face an impoverished retirement. The financial loss that fraud victims suffer is only part of the picture; the emotional damage can be devastating.
>
> The March 2021 Work and Pensions Committee report, "*Protecting pension savers – five years on from the pension freedoms: Pension scams"*, stated that £30m lost to pension scammers was reported to Action Fraud between 2017 and August 2020. The report went on to say this was "indisputably an underestimate". The opening line of the report says it all: "Most of us are at risk of becoming the victim of a pension scam".[17]

The PSIG has published "Combating Pension Scams – A Code of Good Practice" (version 2). Whilst the code has no statutory basis, schemes have been adopting its guidelines, helping to prevent transfers to unauthorised arrangements.

The difficulty is that pension scammers can advertise themselves online, they can contact potential victims through social media, and they can impersonate legitimate businesses or claim a fictitious relationship to one. In September 2020, Aviva (an insurance and asset management company) told the House of Commons Work and Pensions Committee

---

13 Financial Services Compensation Scheme, The worrying rise in online financial scams, 12 May 2021, [online] (accessed 20 May 2021)
14 Financial Services Compensation Scheme, The worrying rise on online financial scams, 12 May 2021, [online] (accessed 20 May 2021)
15 Ibid
16 HC Deb 28 April 2021 cc164-165WH
17 Financial Services Compensation Scheme, The worrying rise in online financial scams, 12 May 2021, [online] (accessed 20 May 2021)

that since the first Covid-19 lockdown in 2020 it had "identified 27 fake websites purporting to be Aviva, trying to defraud pension age customers of their investments".[18] The Association of British Insurers (ABI), an insurance industry trade association, also told the Committee that even once a fake website has been discovered "there are several obstacles to taking down the website leaving the public vulnerable to scams for a prolonged period.[19]

3.8 Stranded traveller emails

A potential victim receives an unexpected email supposedly from a friend or someone they know claiming they are stranded abroad due to some sort of disaster (e.g. an accident, mugging or ill health), and asks them to help by sending money. In fact, their friend's email account has been hacked, and this message has been sent to everyone in their address book.

3.9 Online relationship scams

A person is befriended on a social networking or dating site. Once the scammer has gained the victim's trust, they ask for money, supposedly to help get them out of a difficult situation. It is a form of extortion using "emotional blackmail".

3.10 Health scams

A person responds to an email or online advert thinking they are purchasing some miraculous pain relief tablets or other medicines. Having parted with their money, the item is not what it seems (e.g. it is a placebo or of poor quality) or is never delivered.

3.11 Money mule scams

The scammer advertises on social media a "legitimate" job acting as a money transfer agent, all the person has to do to earn a fee is provide their bank details. The scammer then uses the victim's bank details for money laundering purposes.

3.12 Covid-19 online scams

Scammers have been quick to exploit the current pandemic for financial gain. For example, a vaccination scam involves sending a phishing text message telling the recipient that they are eligible to receive the vaccine, it links to a fake NHS page which then asks for their personal information (name, address, date of birth etc) and for bank or credit card details.

Other Coronavirus-themed phishing emails deliberately play on the fears of people. Some pretend to be from local councils giving out business grants and contain links that, if clicked, give the scammer access to sensitive personal information (e/g. passwords, email logins and banking

---

18 House of Commons Work and Pensions Committee, Protecting pension savers – five years on from the pension freedoms: Pension Scams, Fifth Report of Session 2019-21, para. 65, 24 March 2021, HC 648, [online] (accessed 20 May 2021)

19 Ibid, para. 65

details). There are online scams where people think they are ordering PPE equipment (such as protective face masks or hand sanitiser) that are never delivered. There are also scams involving fake testing kits or "cures" for the virus. People who are vulnerable or isolated at home are particularly susceptible to these scams.

Another example of online fraud saw scammers upgrading consumer bank accounts to business ones so to qualify for the Government's Bounce Back Loan scheme. They then applied for multiple loans across multiple UK banks. The pandemic has clearly shown just how sophisticated online scams have become, how fast criminals can adapt to new situations, and how easy it is for people to be taken in.

Fraud from online shopping has also increased during the pandemic. According to Action Fraud, the number of cases rose by 44% to 95,531 over the year as more people turned to internet shopping with shops closed.[20] Romance scams also increased by 15% in the last year, as more people turned to internet dating during lockdown.[21]

A report by UK Finance, Fraud – The Facts 2021, provides an overview of payment industry fraud. It provides the following description of how criminals have used the Covid-19 pandemic to devise new scams:

> While families and businesses have struggled, the criminal gangs behind economic crime have been quick to capitalise from the pandemic by tailoring scams to fit our changing lifestyles due to the pandemic. These include impersonation scams that seize on people's fears about the pandemic where fraudsters pretend to be from trusted organisations such as the NHS or government departments. Criminals are also adapting to the rise in online shopping and remote working by impersonating parcel delivery companies, e-commerce platforms or broadband providers. In addition, criminals are recruiting 'money mules' to launder stolen funds by posting fake adverts on job websites and social media, targeting those looking for work or to earn easy money during the pandemic.
>
> Let's be clear, these fraudsters are not cheeky chancers, they are organised, ruthless criminals using sophisticated techniques to trick people out of their personal or financial information. As a recent report by the Royal United Services Institute (RUSI) think tank highlights, the links between fraud, organised crime and terrorism pose a significant and growing threat to our national security.[22]

During a recent Westminster Hall debate on online scams, Victoria Atkins, the Parliamentary Under-Secretary of State for the Home Department, addressed the emergence of new Covid-19 scams. She said:

> We know that, sadly, in the midst of the pandemic, with the enormous human cost that it has had for so many people, fraudsters are seeking to take advantage of even that. We have been working with partners from across law enforcement and health to track and mitigate the threat of fraud around the pandemic. That has included a series of public messaging

---

20 "Pet and shopping scams surge during pandemic", BBC News, 12 May 2021, [online] (accessed 20 May 2021)

21 Ibid

22 UK Finance, Fraud – The Facts 2021 – The Definitive Overview of Payment Industry Fraud, [online] (accessed 20 May 2021)

campaigns to inform the public of fraudsters who are seeking to exploit the vaccine roll-out and tell them how we can all remain vigilant against such attempts.[23]

[23] HC Deb 28 April 2021 c.166WH

4. Victims of online scams

4.1 Who are they?

Scammers will target anyone, people of all ages and from all walks of life can be victims. It is often thought that older people are the most likely to fall for scams, but data published by the Office for National Statistics (ONS) suggests that older people (aged 65+) are actually significantly less likely to be victims of fraud than other age groups.[24] The relevant extract is reproduced below:

> Unlike many other types of crime, fraud, by its nature, is often committed anonymously, with the offender not having a specific target in mind. As such, there tends to be considerably less variation in fraud victimisation rates across different demographic groups than with other crime types. For example, there is no statistically significance difference in the likelihood of men or women being victims.
>
> However, over the last three financial years (up to the survey year ending March 2019), some demographic groups have been consistently more or less likely to be victims of fraud according to the Crime Survey for England and Wales (CSEW).
>
> Age
>
> As with other crime types, adults aged 65 years and over were less likely to be a victim of fraud than those in younger age groups. An estimated 4.8% of adults aged 65 to 74 years and 3.6% of adults aged 75 years and over were victims of fraud in the year ending March 2019, compared with 6.5% and above for all other age groups. Unlike other crime types, though, there is little variation in victimisation rates across other age groups (adults aged 16 to 64).[25]

People are often too embarrassed to admit they have fallen for a scam. According to the FSCS, "some people are more aware of scams than others and the true amount of harm caused is likely to be much higher than we think."[26] Research from Aviva in July 2020 found that half of people targeted by scams did not report them.[27]

Scams deliberately take advantage of people's fears. People are especially vulnerable to "get rich-quick schemes" if they are in a difficult financial situation, such as coping with redundancy. Online training scams specifically target people hoping to improve their employment chances, but the scam defrauds them of their money instead. Some scammers target people struggling on benefits by offering to help them apply for interest-free government loans. Once in receipt of the victim's personal details the scammers use them to apply for an advance loan of universal credit which the scammers take, leaving the victim in debt.

Although anyone can fall for an online scam, "vulnerable" people – those with mental health problems, learning difficulties or dementia -

---

24 Office for National Statistics, "Nature of Fraud and Computer Misuse in England and Wales: Year Ending March 2019", 19 March 2020, [online] (accessed 20 May 2021)
25 Ibid
26 Financial Services Compensation Scheme, The worrying rise in online financial scams, 12 May 2021, [online] (accessed 20 May 2021)
27 Ibid

are especially susceptible to fraudsters. Once scammed, victims must deal with banks and law enforcement bodies to try and recover their money.

In addition to financial loss, victims of online scams can suffer psychologically and emotionally – they suffer unseen harm. According to the consumer body Which? there are 300 to 350 fraud reports each week in which victims show signs of severe emotional distress:

> Action Fraud data, shared with Which?, identifies 300-350 fraud reports a week where victims show signs of severe emotional distress – equalling up to 18,000 reports a year. Each is reviewed by trained staff to identify a course of action, which can include dispatching emergency services to the victim's home. Worryingly, Action Fraud received 241 phone calls between January and November 2020 where a 'threat to life' was flagged. This means call operatives must attempt to keep callers talking until police or an ambulance crew arrive. Phone calls and web forms triggering concerns for wellbeing account for up to 6% of the 300,000 reports Action Fraud receives each year. While Action Fraud reports are not solely online scams, it is an area where Which? has repeatedly found consumers falling prey to increasingly sophisticated criminals. [28]

Scams involving false investment opportunities are particularly devastating when they involve the life savings of individuals. Data published by Lloyds Bank in February 2021 found that one in four investment scam victims in the past year were aged over 55, losing nearly £26,000 on average.[29]

Which? describes the case of an 80-year old gentleman who could not sleep for weeks after losing his retirement savings of £50,000 to scammers.[30] The person behind the scam pretended to be a real investment company, assuming the name of a real investment manager at that company. After checking his credentials, the victim had no reason to suspect a scam. The victim was eventually reimbursed under the terms of the CRM Code, after his bank decided he had done his due diligence and was not at fault.

Which? wants urgent action to be taken to stop fake and fraudulent content that leads to scams and consumer online harms. Which? thinks the Government must give online platforms legal responsibility for preventing content appearing on their sites that leads to scams.[31] It is also calling on the Government to outline its plans to tackle scams on online platforms.[32]

4.2 How to report an online scam

If a person suspects that a fraud has been committed, they should report the incident to Action Fraud. Action Fraud is the UK's national crime reporting centre, investigating cases of fraud. It gathers information on scams and passes it onto the National Fraud Intelligence

---

28 "Devastating emotional impact of online scams must force government action", Which? 10 March 2021, [online] (accessed 20 May 2021)
29 Financial Services Compensation Scheme, The worrying rise on online financial scams, 12 May 2021, [online] (accessed 20 May 2021)
30 Ibid
31 Ibid
32 Ibid

Bureau for analysis by the police. Whilst not every report results in a police investigation, it does add to the general body of intelligence on how scams work and who may be perpetrating them. If a victim of a scam has lost money, the theft can also be reported to their local police.

If the victim of a scam has lost money using their credit or debit card, or has sent money through an account transaction, they should immediately notify their bank or payment provider. The quicker they do this, the greater the chance of recovering their money. The bank or payment provider can also put in place additional security measures.

A victim of a phishing email should report the incident to the internet service provider that sent the email. They may be able to close the account that the scammer was sending from.

The Information Commissioner's Office (ICO) is responsible for taking enforcement action against organisations that persistently ignore their obligations under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Further information is available on the ICO website.

Finally, victims of an online scam can seek advice from Citizens Advice Consumer Helpline. If appropriate, Citizens Advice may refer the case on to Trading Standards and action may be taken against a rogue trader.

4.3 Will victims get their money back?

The issue of compensation for victims of online scams is complex, and much depends on the unique circumstances of the case. While some victims are successful, others may find it difficult to make their claim heard by their bank (or other payment service provider) and battle to recoup their losses.

The truth of the matter is that individuals who have been scammed do not always get their money back, especially if they have parted with cash or made a bank transfer or if the scammer is located abroad. Consumer groups complain that the odds of victims successfully recovering all they have lost is low, and they are often left with a distrust for the regulatory system.[33]

The various options available to victims to try and recover their money are summarised below:

- If a victim of an APP scam has made a **bank transfer** (e.g. authorising the transfer of money into another bank account) than they should contact their bank (or building society) immediately to report it. It is important to do this as soon as possible, as the bank may still be able to stop the transaction or trace the money.

  Signatory firms to the CRM Code make a commitment to reimburse customers who lose money where they were not to blame for the success of a scam. The Code was developed by a

[33] "Devastating emotional impact of online scams must force government action", Which? 10 March 2021, [online] (accessed 20 May 2021)

Steering Group comprising of representatives from consumer groups and payment service providers (PSPs). On 1 July 2019, the Lending Standards Board (LSB), the primary self-regulatory body for the banking and lending industry, took over responsibility for the governance and oversight of the CRM Code. To date, nine firms (payment service providers (PSPs)) are signed up to the Code, representing over 85 per cent of APPs.[34]

On 20 April 2021, the LSB published updates to the CRM Code, following its review[35] earlier in the year. The updates include the introduction of governance and oversight requirements into the Code with effect from 14 June 2021. Amendments have also been made to the wording of the Code in respect of the "no-blame funding pot". References to the no-blame fund now makes it clear that firms can self-fund no-blame scam cases. These amendments are effective immediately.

Under the Code, when a signatory bank is informed of a scam they must investigate the case. The customer should be reimbursed if they meet the standards expected of them (i.e. they have not been "grossly negligent"). If a customer is unhappy with their bank's assessment of their case, they can lodge a complaint with the Financial Ombudsman Service.

Even if the bank is not a signatory to the CRM Code, the victim should still report the online fraud to their bank as soon as they discover it; the bank should have policies in place to assist them. They can also lodge a complaint with the Financial Ombudsman if they are unhappy with how any of the banks involved in the APP scam have acted.

- If an **unauthorised transaction** has been made on a person's card then they may be able to recover the money from their bank. The Payment Services Regulations 2009 and rules found in the Banking Conduct of Business Sourcebook place obligations on banks and building societies to provide a refund in certain circumstances.
- Under section 75 of the *Consumer Credit Act 1974* (as amended), a credit card company is jointly and severally liable for any breach of contract or misrepresentation by the trader. However, for section 75 to apply the good or service bought must have cost over £100 and not more than £30,000. Section 75 might be useful where goods or services never materialise, and the trader has disappeared.
- If an individual has bought a good or service with a debit card, they may be able to ask their card provider to reverse the transaction using **chargeback**. The chargeback scheme applies to all debit card transactions including goods costing less than £100, although exact rules may vary between the various networks. It is

34 App Scams Voluntary Code: Seven launch signatories to the code continue "no blame" interim funding to 31 March 2020, UK Finance, undated, [online] (accessed 20 May 2021)

35 Lending Standards Board (LSB), "Review of the CRM Code", 15 July 2020, [online] (accessed 20 May 2021)

important to note that chargeback is not enshrined in law but is part of Scheme Rules, which participating banks subscribe to.

- If the victim of a scam has paid for an item online using **PayPal**, and the item is never sent, they may be covered by PayPal Buyer Protection, but there are exceptions. For example, some online scams involve the scammer setting up a fake payment page using PayPal branding, to gather the victim's bank details.
- If a victim of an online scam sends money via a **wire payment service** (such as MoneyGram, PayPoint and Western Union), it is unlikely they will be able to get their money back.

4.4 Where can a scam victim go for help?

The following organisations may be able to help the victim of a scam:

- Anyone can report a scam or online fraud to Action Fraud using the designated website or by telephoning: 0300 123 2040. Action Fraud will provide them with a crime reference number and will send their report to the National Fraud Investigation Bureau (NFIB) for assessment. It should be noted, however, that Police Scotland have not signed up to the Action Fraud process, so victims should follow the guidance provided on the Police Scotland website.
- If the victim of a scam thinks that any of the financial institutions involved have not conducted themselves appropriately according to their obligations under any relevant legislation, they could contact the Financial Conduct Authority (FCA).
- Citizens Advice can provide support and advice on what steps to take if a person has been a victim of fraud. The Citizens Advice website provides a useful search tool to help people to find their nearest bureau. There is also the Citizens Advice consumer helpline: 0808 223 1133.
- Victim Support can provide help after a crime has been committed. It gives free and confidential support 24 hours a day via its support line: 0808 1689 111 or via an online chat.

5. What is being done to combat scams?

5.1 Public awareness campaigns

From time-to-time, Trading Standards have joined with Citizens Advice to operate "Scam awareness" campaigns. The aim being to increase awareness and to provide people with practical advice on how to avoid being scammed. The Action Fraud website also highlights the latest scams based on reports from the public.

Various charities and consumer organisations publish advice online. For example, "Age UK" has published "Staying safe online", guidance on avoiding scams. The consumer body Which? has started an online petition to "Stamp out scams", demanding that banks and businesses do more to protect consumers.

5.2 National Cyber Security Centre

The National Cyber Security Centre (NCSC) recently launched the "Suspicious email reporting service"(SERS), to make it easier for the public to report scams and harmful websites. The NCSC website states that as of 31 March 2021, more than 5,500,000 reports were received, with the removal of more than 41,000 scams and 81,000 URLs.

Information on how to report a potential phishing message to the NCSC using the SERS is available online.[36]

5.3 Bilateral fraud charters

The Government has been leading work to develop bilateral fraud charters with the banking, telecommunications and accountancy sectors.[37] The aim of the charters is "to bring greater clarity, transparency and accountability to the actions that each sector will take to target harden their systems and protect their customers from fraud".[38] For example, the Dedicated Card and Payment Crime Unit (DCPCU) is a police unit that targets and disrupts credit card fraud. It was formed as a partnership between UK Finance, the City of London Police, the Metropolitan Police, and the Home Office.

Another example is the FSCS, which is working closely with anti-scam regulatory partners and the financial services industry.[39] The FSCS has also signed a memorandum of understanding with the Serious Fraud Office (SFO) so it can share data, insights and intelligence on matters such as pension scams and fraudulent investment scams. The Government is also seeking to expand membership of the Joint Fraud

36 National Cyber Security Centre, "Phishing: how to report to the NCSC", 21 April 2020 [online] (accessed 20 May 2021)
37 HC Deb 28 April 2021 c66WH
38 Ibid
39 Financial Services Compensation Scheme, The Worrying rise in online financial scams, 12 May 2021 [online] (accessed 20 May 2021)

Taskforce to involve a wider network of stakeholders in fraud prevention activity.

5.4 Financial services initiatives

The main regulator, the FCA has a statutory objective of "securing an appropriate degree of protection for consumers". It seeks to do this through active investigation, the prosecution of suspect activity, and through consumer information/education programmes, such as the ScamSmart scheme. FCA data shows that scams activity is increasing: the FCA issued 80% more scam warnings in 2020 than in 2019.[40]

As already mentioned, the voluntary CRM Code sets a new criterion for banks to judge whether customers caught by APP scams should be reimbursed. The Code only covers transfer between UK accounts; overseas accounts are not covered. The Payment Systems Regulator has ruled the CRM Code should be voluntary rather than mandatory, but most high street banks have signed up to it.

In addition, a separate name-checking service, called "confirmation of payee" (CoP), works by making sure the name of the account someone is sending money to matches the name they have entered. The aim is to help prevent losses due to accidentally misdirected payments and certain types of APP fraud. The Payment Systems Regulator required the UK's six biggest banking groups (involved in about 90 per cent of bank transfers) to put the measures in place by 31 March 2020. Other financial institutions have also chosen to implement CoP.

Victims of a scam are advised to contact their banks with any questions on how CoP works or any issues with CoP when making a payment. If no resolution is offered by the bank, or there are significant issues impacting the CoP service, customers are advised to contact Pay.UK who is responsible for maintaining the rules and standards for CoP.

5.5 Initiatives taken by online platforms

Online platforms currently have no legal obligation to protect users against fake or fraudulent content. However, platforms have pursued initiatives of their own.

As outlined in its letter to the FCA dated 26 February 2021, Google updated its financial services policy in July 2020 to make financial services advertisers subject to its business operations verification process.[41] This requires advertisers to provide further information about their business model, services offered and relationships with other brands or third parties. In December 2020, following continued conversations with the FCA, Google announced that it has the right to

---

40 Financial Services Compensation Scheme, The worrying rise in online financial scams, 12 May 2021, [online] (accessed 20 May 2021)

41 Letter from Ronan Harris, Managing Director Google UK & Ireland to Charles Randell CBE and Nikhil Rathi, Financial Conduct Authority, 26 February 2021, [online] (accessed 20 May 2021)

pause a financial services advertiser's account while they complete business operations verification.[42]

In late 2020, Google also updated its unreliable claims policy to restrict the rates of return a firm can advertise and ban the use of terms that make unrealistic claims.[43] According to Google, this update prohibits firms from making unrealistic promises of large financial return with minimal risk, effort, or investment.

Google has plans to verify the identity of all advertisers on its platforms, a process it calls advertiser identity verification.[44] This requires advertisers to submit personal legal identification, business incorporation documents or other information that proves who they are. It will then use this information to generate an in-ad disclosure that shows their name and location when their ads run. Google explained its timetable for implementing this process as follows:

> We are pleased that the UK has been prioritised for this process, which began in January. While the rollout is gradual and phased, we are prioritising areas with the highest impact on user risk.
>
> We know that our adversaries are sophisticated and dynamic and so we believe a layered approach, incorporating a spectrum of verification along with other tactics to locate and remove bad actors, is important. Just as we are learning and iterating on our approach so too are these bad actors. That is why continuously evaluating our methods and solutions is so important, so that we can continue to improve the efficacy of our policies.[45]

Ruth Edwards MP commented on Google's verification process during a Westminster Hall debate on online scams on 28 April 2021:

> If a verification process is to be effective, it needs to take place before any adverts are served. Leaving them up for 21 days while checks are completed provides a free-for-all for scammers. An experiment undertaken last year by Which? shows why. It created a fake water brand, Remedii, and an accompanying online service offering pseudo health and hydration advice, called Natural Hydration. It advertised both using Facebook and Google. Which? reported that:
>
> > "With barely any checking, Google promoted ads for our website and fake mineral water to users who searched for popular terms, such as 'bottled water'. Our ads gained nearly 100,000 impressions over a month."
>
> That shows how fast fake ads can reach a wide audience. A lot of damage can be done in 21 days.
>
> Just this week, in a user survey published by Which?, a third of victims who reported a fraudulent ad on Google said that the advert was not taken down by the search engine, while a quarter of victims who reported an advert on Facebook that resulted in

---

42 Google, Account pausing for business operations verification, December 2020, [online] (accessed 20 May 2021)
43 Google, Update to Misrepresentation Policy (December 2020), [online] (accessed 20 May 2021)
44 Google, Advertiser identity verification and ad disclosures FAQ, [online] (accessed 20 May 2021)
45 Ibid

> them being scammed said the advert was not removed by the social media site. [46]

Ruth Edwards did not think it unreasonable to require platforms to spend money on helping to protect people from the harm caused by fraudulent adverts, "especially given that adverts are targeted at users based on their recent web activity and behaviour.[47]

46 HC Deb 28 April 2021 cc162-163WH
47 HC Deb 28 April 2021 cc163-164WH

6. Government's position

It is the Government's view that a collaborative and innovative response to online fraud is needed to keep pace with the "changing threat and new technologies".[48] Two important initiatives are outlined below.

6.1 Online advertising programme

In the UK, the content and placement of online advertisements is currently regulated by the Advertising Standards Authority (ASA) under a self-regulatory system. The Competition and Markets Authority (CMA) may also address misleading advertising in appropriate cases, for example where it points to systemic failures in a market. The Information Commissioner's Office (ICO) also regulates compliance with relevant data protection legislation. In addition to these regulatory bodies, relevant trade bodies are also developing processes that aim to solve some of the market challenges.

In February 2019, the Department for Digital, Culture, Media and Sport (DCMS) issued a call for evidence on online advertising regulation. It asked whether standards on the placement and content of advertising are being effectively applied and enforced online so that consumers have limited exposure to harmful or misleading advertising.[49] Owing to the pandemic, the deadline for submissions was extended to 4 May 2020.

The DCMS consultation was intended to supplement work by the CMA, the Centre for Data Ethics and Innovation, and the ICO. On 1 July 2020, the CMA published its market study final report on Online Platforms and the Digital Advertising Market in the UK.[50] The CMA found that competition is not working well in these markets, leading to substantial harm for consumers and society as a whole. It recommended that the Government passes legislation to establish a new pro-competition regulatory regime.

In addition, the Centre for Data Ethics and Innovation (CDEI) conducted a review into Online Targeting[51] and Bias in Algorithmic Decision Making[52] as part of their project to strengthen the governance of data-driven technology. The ICO is also carrying out a review into Adtech and Real Time Bidding as part of their aim to ensure that people have confidence in how their data is being used.[53]

During the recent Westminster Hall debate on online fraud, Stephen Timms said:

---

48 HC Deb 28 April 2021 c.166WH

49 Department for Digital, Culture, Media and Sport, Online advertising – call for evidence, 18 March 2020, [online] (accessed 20 May 2021)

50 Competition and Markets Authority (CMA), Online platforms and digital advertising market study, press notice, 3 July 20120, [online] (accessed 20 May 2021)

51 Centre for Data Ethics and Innovation, Online Targeting: Final report and recommendations, 4 February 2020, [online] (accessed 20 May 2021)

52 Centre for Data Ethics and Innovation, CDEI publishes review into bias in algorithmic decision-making, 27 November 2020, [online] (accessed 20 May 2021)

53 Information Commissioner's Office, Update report into adtech and real time bidding 20 June 2019, [online] (accessed 20 May 2021)

> A call for evidence on online advertising closed a year ago, but as yet nothing at all seems to have come out of that and asking us to wait for yet further consultation before anything is done would be hopeless. The FSCS,[54] the FCA[55] and, I understand, the Governor of the Bank of England are urging that scams should be included in the online safety Bill, so I hope the Minister can encourage us on that.[56]

6.2 Draft Online Safety Bill

Background

The Online Harms White Paper, published in April 2019, sets out the Government's ambition "to make the UK the safest place in the world to go online, and the best place to grow and start a digital business".[57] It described a new regulatory framework establishing a duty of care on companies to improve the safety of their users online, overseen and enforced by an independent regulator.

In December 2020, the Government published its Full Response to the consultation.[58] The response noted that economic and financial harms to individuals, including online fraud, would be excluded from the intended scope of the new regulatory framework:

> The Government has determined that the fraud threat will be most effectively tackled by other mechanisms and as such the legislation will not require companies to tackle online fraud. We are working closely with industry, regulators and consumer groups to consider additional legislative and non-legislative solutions. This ongoing programme of work aims to effectively address the harms posed by all elements of online fraud in a cohesive and robust way. [59]

There have been calls on the Government to bring online fraud within the scope of the draft Bill. For example, a joint statement, drafted by the Fraud Advisory Panel with the support of various fraud prevention organisations including the Cifas, was published in April 2021.

It was announced in the Queen's Speech on 11 May 2021 that the Government would introduce a draft Bill to give effect to the regulatory framework outlined in the White Paper. The draft Online Safety Bill was published the following day, on 12 May 2021, together with Explanatory Notes.

The draft Bill is seen as landmark legislation in that it will end the era of self-regulation. It is intended to protect users of online content-sharing platforms from harmful material by imposing statutory duties on providers of regulated services and by appointing Ofcom as the independent regulator to oversee the regulatory framework. In a written statement, Oliver Dowden, Secretary of State for DCMS, explained that

---

54 Financial Services Compensation Scheme (FSCS)
55 Financial Conduct Authority (FCA)
56 HC Deb 28 April 2021 c165WH
57 DCMS & Home Office, "Online Harms White Paper", April 2019, CP 57, [online] (accessed 20 May 2021)
58 DCMS & Home Office, "Online Harms White Paper: Full Government Response to the Consultation", December 2020, CP 354, [online] (accessed 20 May 2021)
59 Ibid, p.25

the scope of the Bill had been widened to include financial harms caused by online fraud. He said:

> Since the publication of the full Government response in December 2020, there has been significant concern about the exclusion of online fraud from the legislation. This Government understand the devastating effect that online fraud can have on its victims, so today we are announcing that the Online Safety Bill brings user-generated fraud into the scope of the regulatory framework.
>
> This change will aim to reduce some specific types of damaging fraudulent activity. In tandem, the Home Office will be working with other Departments, law enforcement and the private sector to develop the Fraud Action Plan, including the potential for further legislation if necessary.[60]

The draft Bill will be subject to pre-legislative scrutiny, which the Minister said he hopes will start as soon as possible.[61]

Scope of the draft Bill

The Bill will apply to providers of internet services which allow users to upload or share user-generated content or otherwise to interact online ('user-to-user services') and on providers of services which allow users to search all or some parts of the internet ('search services'). In other words, the draft Bill focuses on fraudulent behaviour carried out via user-generated content on online services.

Online fraud and scams via advertising, emails or cloned websites still fall outside the scope of the draft Bill, although they could be caught by the broader obligations on platforms to protect against illegal content.

Responses to the draft Bill

Cifas (a not-for-profit fraud prevention membership organisation) welcomed the inclusion of user-generated fraud in the draft Online Safety Bill as a positive step "in protecting the UK public and the business community from one of the most prevalent online harms".[62] However, it said more needs to be done to tackle other aspects of online fraud currently excluded from the Bill:

> "The Bill places responsibility on platforms with regards to user-generated content but excludes other types of online fraud. I look forward to the release of the Home Office Fraud Action Plan and how this will address fraud currently excluded from the Online Safety Bill, such as through advertising, emails and cloned websites.
>
> "Fraud in the UK has reached epidemic levels and recent research commissioned by Cifas and RUSI has highlighted the strong link between fraud and other high harm crimes such as people and drug trafficking, and terrorist financing. We need to act fast to disrupt criminal operations and ensure that online platforms are taking the appropriate steps to do so."[63]

---

60 HC Deb 12 May 2021 c7WS
61 HC Deb 12 May 2021 c8WS
62 Cifas, "Cifas responds to the inclusion of fraud in the Online Safety Bill", press notice, 12 May 2021, [online] (accessed 20 May 2021)
63 Ibid

UK Finance was also disappointed that the draft Bill would not protect people from all fraud that takes place online:

> As more of us have shifted online because of the pandemic, we've seen a spike in money mule activity, investment and purchase scams over the last year because criminals can target people directly in their homes across online platforms. Whilst the Bill includes fraud via user generated content on social media sites and dating apps, it won't cover cloned websites and online adverts which fraudsters pay for.
>
> UK Finance has called on the Government to include all economic crime within the Bill when it is formally introduced. It argues that "not doing so leaves a large proportion of the public at high risk of being scammed online, because criminals are experts in adapting their tactics to exploit any loopholes". [64]

Lloyds Banking Group also called on the Government to do more to fight the "financial fraud pandemic". It said:

> "While the Online Safety Bill will help keep people safer online, financial fraud remains the missing piece of the puzzle and we would urge this to be included as the Draft Bill is progressed.
>
> We're working behind the scenes 24/7, investing more than £100million in our defences to stop the majority of attempted fraud. The Bill needs to reflect the role of big tech to help stop scams from happening in the first place, otherwise fraudsters will continue ruining lives and disappearing with victims' cash."[65]

64 UK Finance, "UK Finance responds to the Government's drat Online Safety Bill", press notice, 12 May 2021, [online] (accessed 20 May 2021)

65 "Online Safety Bill to Clamp Down on Fraud", Credit Connect, 13 May 2021, [online] (accessed 20 May 2021)

7. Select Committee inquiries

The All-Party Parliamentary Group (APPG) on Financial Crime and Scamming was launched in October 2017. The stated aim of the APPG is to challenge the response to fraud from law enforcement, government, and the public, private and charity sectors. It is also intended to act as a channel for expert briefings on financial crime and scamming to parliamentarians.

On 6 January 2021, the Work and Pensions Select Committee heard oral evidence[66] from the Pensions Regulator, the City of London Police, the FCA and the National Economic Crime Centre as part of its inquiry into the impact of pensions freedoms and the protection of pension savers. The Committee heard evidence on the scale of pension scams. All those who gave evidence considered that the true extent of pension scamming is likely to be higher than the £30 million reported by Action Fraud as having been scammed from individuals over the last three years. The FCA said that Google and Facebook were acting too slowly in curbing online scams and other measures may have to be considered.[67]

The Home Affairs Select Committee has also been looking at issues around online crime, online fraud, and online harm and abuse as part of its ongoing work on the Home Office response to the coronavirus crisis. During an oral evidence session on 3 June 2020, Graeme Biggar CBE, Director General, National Economic Crime Centre, said that more needs to be done by everyone to combat online fraud, a view endorsed by Commander Karen Baxter, Head of Economic Crime, City of London Police. The relevant extract is reproduced below:

> **Graeme Biggar**: I think everyone should be doing more on fraud. I do not think we are tackling this as seriously as we need to across the entire country. That is absolutely in my organisation as well as everywhere else, but definitely in social media companies, too.
>
> […] There are lots and lots of demands on social media companies, and I recognise that, but it really matters, and they do need to be doing more. We are seeing messages circulated on Instagram and Facebook that are advertising things that turn out to be scams. We are seeing search results coming up on Google that put very prominently investment opportunities that turn out to be scams. They are not being taken down quickly enough. A whole series of things need to be done in the social media sector as well as in other sectors—the banking sector, the retail sector, the insurance sector and so on. Absolutely, yes, they should be doing more.[68]

---

66 Formal meeting (oral evidence session): Protecting pension savers – five years on from the pension freedoms: Pension scams, Committee Work and Pensions Committee, 6 January 2021, [online] (accessed 20 May 2021)

67 "FCA: social media must do more against online scams", Money Marketing, 6 January 2021, [online] (accessed 20 May 2021)

68 Home Affairs Committee, Oral Evidence: Home Office Preparedness for Covid-19 (Coronavirus), HC 232, para. Q.692, 3 June 2020, [online] (accessed 20 May 2021)

8. Parliamentary debates and PQs

8.1 Debates

- Westminster Hall debate, Online scams: consumer protection, HC Deb 28 April 2021, cc161-168.
- Westminster Hall debate: Online scams, HC Deb 10 November 2020, cc357-363WH.
- Westminster Hall debate: Telephone and online scams, HC Deb 4 June 2019, cc1-20WH.
- Backbench business debate: Scamming: Vulnerable Individuals, HC Deb 8 September 2016, cc507-530.

8.2 Parliamentary Questions

There have been many Parliamentary Questions (PQs) on the issue of online fraud and consumer protection. By way of illustration only, a small selection is reproduced below.

On 19 April 2021, Kevin Foster MP, Parliamentary Under Secretary of State, provided the following written answer to a PQ asked by Karin Smyth MP on what assessment the Government had made of trends in the level of online fraud during the Covid-19 outbreak:

> The Government is aware fraudsters are exploiting the pandemic to commit opportunistic crimes such as fraud. We are regularly monitoring the number of cases being reported to the police and these – at present- remain very low.
>
> Despite a difficult fiscal backdrop, as part of the 2020 Spending Review, the Government committed a further £63m to the Home Office to tackle economic crime, including fraud. This is in addition to funding the Home Office commits each year to the National Crime Agency, National Economic Crime Centre and police forces, including the City of London Police as the national lead force for fraud and the operator of the Action Fraud and National Fraud Intelligence Bureau services.
>
> Our efforts to tackle online scams have been ramping up, including working with the National Cyber Security Centre to establish a new Suspicious Email Reporting Service which was launched in April 2020. This service allows the public to report potential scams safely and effectively. As of 28 February 2021, the number of reports received stand at more than 5,000,000 with the removal of more than 36,000 scams and 71,000 URLs.
>
> The best way to deal with these scams is for the public to be well informed on how to protect themselves. We have launched a gov.uk page containing easy-to-follow steps for people to spot potential frauds and the steps they can take to avoid them. It also signposts advice and support to those who may unfortunately have fallen victim.
>
> We continue to encourage anyone who has been a targeted by a scam to report it. Action Fraud is the central police reporting point

> for all victims of fraud and can be contacted by phone on 0300 123 2040 or through their website. [69]

On 13 April 2021, Kevin Foster MP provided a written answer to a PQ asked by Stephen Timms MP. Mr Timms asked the Secretary of State for the Home Department what estimate she has made of the growth in the number of scams facilitated by content hosted on online platforms through adverts or user- generated content in the last twelve months:

> Fraudsters have shown they can and will exploit any vulnerability to commit their crimes, including through the use of technology and the internet. We are working with law enforcement and industry to close down these vulnerabilities.
>
> Last year, the National Cyber Security Centre launched the Suspicious Email Reporting Service which has already led to tens of thousands of harmful websites and scams being shut down. We are also seeking to expand membership of the Joint Fraud Taskforce to involve a wider network of stakeholders in our fraud prevention activity.
>
> We are also considering other routes to ensure the public are safe from all forms of online fraud, including legislation. The Department for Digital, Culture, Media & Sport is leading efforts on the Online Advertising Programme which will consider further regulation of online advertising to tackle harms including fraud.[70]

On 2 March 2021, Debbie Abrahams asked the Government what recent assessment it has made of the adequacy of the regulatory framework governing the responsibility of online platforms, including search engines and social media sites to protect their users against scam content on their sites. On 9 March 2021, Caroline Dinenage, Minister of State for Digital and Culture in the DCMS provided the following written response:

> We are deeply concerned about the growth and scale of online scams. My officials work closely on this matter with other government departments, including the Home Office as the government department responsible for tackling fraud, as well as with industry, regulators and consumer groups. Through an ongoing programme of work, the Government is considering additional legislative and non-legislative solutions to effectively address the harms posed by all elements of online fraud in a cohesive and robust way.
>
> Within my department, the Online Advertising Programme will be considering further regulation of online advertising to tackle harms including fraud. The Government will launch a public consultation on measures to enhance how online advertising is regulated in the UK this year.[71]

On 22 February 2021, Caroline Dinenage provided a written answer to a PQ asked by Chi Onwurah MP on what discussions the Secretary of State for DCMS has had with the Home Secretary on the potential merits of expanding the scope of the proposed Online Safety Bill to tackle online scams and fraud. She said:

---

69 WPQ 19 April 2021 UID 175912
70 WPQ 13 April 2021 UID 174717
71 WPQ 9 March 2021 UID 161765

> The Secretary of State for Digital, Culture, Media and Sport and the Home Secretary are jointly responsible for the online harms programme. The Government has set out its position on the scope of the online safety bill in the full government response to the Online Harms White Paper.
>
> The Ggovernment is committed to tackling online scams and fraud. We are working tirelessly across government and with industry, consumer groups, law enforcement and regulators to pursue fraudsters, close down the vulnerabilities they exploit and make sure people have the information they need to spot and report scams.[72]

[72] WPQ 22 February 2021 UID 152524

BRIEFING PAPER
Number 9214
20 May 2021

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer