House of Commons Library

By Lorraine Conway

30 July 2021

Copycat websites charging for government services

Summary

Image Credits

Keyboard and wallet – no attribution required / image cropped.

Disclaimer

Feedback

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

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

"Copycat" websites offer processing services that are provided cheaper or free of charge through official government sites. Often, they charge a substantial premium for providing those services. For example, searching on the internet to apply for a passport, change the address of a driver's licence, or book a driving theory test, brings up websites for businesses which offer to check, review and forward applications for a fee. Advertisements for these businesses may feature prominently in search results.

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 consumers will be paying for a service which they could obtain from Government for free or at a lower cost. Unfair and misleading practices are prohibited by the Consumer Protection from Unfair Trading Regulations 2008 (CPRs), enforced through the civil and criminal courts.

During 2013-14, copycat websites were a serious issue, with consumers complaining that some websites were imitating official government services to "trick" them into paying unnecessarily for services. In many cases, consumers, having searched on the internet, believed they were on an official site until they were charged a processing fee. Although the issue of copycat websites has never really gone away, the pandemic has provided the opportunity for a new wave of scams, including fake coronavirus websites.

The draft Online Safety Bill, announced in the Queen's Speech, was published on 12 May 2021. This draft Bill sets out a new regulatory framework for online safety, including user-generated fraud. The Government had not intended to include "financial harms" within the new regulatory framework. 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.

This briefing paper provides an overview of the legal position. It also considers the involvement of Trading Standards, the Advertising Standards Authority (ASA) and the Government Digital Service (GDS) in monitoring, and in some cases taking action against, copycat websites. It also looks at the occasions when the issue of copycat websites has been raised in Parliament either during debates or as Parliamentary Questions.

1 Background

1.1 Copycat websites

In recent years, people have complained about private companies that 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 a "reviewing and forwarding service", even in circumstances where the item might be obtained free elsewhere. The charge is seen to be a fee for providing the service rather than a cost attributed to the item itself. In other words, many of these websites are legitimate – it is not against the law for a company to offer a similar service to an official body.

However, it is illegal to deliberately mislead the public and to obtain money by fraud. In other words, businesses must be clear about the product or service they are offering, and they should not trick consumers into spending money for services they do not want.

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 duplicate a government websites (e.g the DVLA, HMRC, or the 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.

1.2 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 Financial Services Compensation Scheme (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.[1]

1.3 Coronavirus: rise in copycat websites

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. 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.

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.[2]

[1] Financial Services Compensation Scheme, The worrying rise in online financial scams, 12 May 2021
[2] UK Finance, Fraud – The Facts 2021 – The Definitive Overview of Payment Industry Fraud

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 Consumer protection: online scams 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.
>
> Criminals are also adapting to the rise in online shopping and remote working by impersonating parcel delivery companies, e-commerce platforms or broadband providers.[3][4]

Further detailed information is provided in a separate Library briefing, "Consumer protection: online scams".

[3] UK Finance, Fraud – The Facts 2021 – The Definitive Overview of Payment Industry Fraud

[4] HC Deb, 28 April 2021, c.1662WH

2 Relevant legislation

The Fraud Act 2006 provides for a general criminal offence of fraud with three ways of committing it:

- 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 to gain a dishonest advantage, which is often financial, over another person".[5] Depending on the circumstances, online fraud might include copycat or cloned websites designed to trick the individual and take their money.

The Consumer Protection from Unfair Trading Regulations 2008 (known as the "Unfair Trading Regulations") have significant importance in the marketing and selling of goods and services. The Regulations prohibit businesses in all sectors from engaging in unfair commercial practices with consumers and set out rules that determine when commercial practices are unfair. They also ban misleading omissions and aggressive sales tactics. **There is a duty to trade fairly and honestly with consumers.**

In the main, the Unfair Trading Regulations apply to business-to-consumer sale contracts and apply to the whole of the UK. The regulations are enforced by Trading Standards through the civil and criminal courts. Further detailed information is provided in a separate briefing paper, "Consumer Protection from Unfair Trading Regulations 2008".

The Advertising Standards Authority might also investigate adverts on misleading websites. If there is evidence of a breach of the Code of Non-broadcast Advertising and Direct & Promotional Marketing (known as the "CAP Code"), the ASA can impose sanctions (see below).

[5] What is fraud and cybercrime? Action Fraud

3 Identify and report a copycat website

3.1 How to identify a copycat website

An investigation into scams by the consumer body Which? (September 2013) revealed that half of those who come into contact with copycat websites are fooled by them. Which? suggests the following tips on how to spot a copycat website:

- **Is it a paid search engine advertisement?** These are the boxed adverts displayed at the top of search engine result pages. Quite often, the official site is the first or second non-paid-for link that appears below the ads.
- **Read the homepage** - Before filling out an application form, take a couple of minutes to visit the homepage and read the text there. It may even say that the site is not officially affiliated with the official body.
- **Check the web address** – An ".org" web address is no guarantee that it is an official website. Any website claiming to be an official government website should have a ".gov.uk" address.
- **Https vs http** - Although it's not always a guarantee, the consumer should check for "https://" at the beginning of the website address. On pages where you are entering personal information, this indicates that there is encryption in place to protect your personal details; websites just with "http://" don't encrypt the user's personal details.

Instead of searching for government services via a search engine, consumers are advised by Trading Standards to go to GOV.UK and use the search function there. It is the most secure place to find government services and information online. If a consumer does use a search engine, they are advised to look out for the differences between natural search results and paid-for search results.

3.2 How to report a copycat website

As already mentioned, it is not unlawful for a business to offer a similar online service to an official body. It is not illegal to provide a "reviewing and forwarding service", even in circumstances where the item might be obtained free elsewhere. However, it is illegal to deliberately mislead the public and to obtain money by fraud.

Copycat or cloned websites intending to defraud people, should be reported 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 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.

In respect of wider trading practices, for example, where a company is charging people extortionate prices for false services, complaints should be made directly to Trading Standards (via the Citizens Advice online portal). The consumer could also report the site to the relevant government department or agency (e.g the DVLA, HMRC, or Passport Office).

If the victim of a copycat website 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.

General information on how to Avoid and report Internet Scams and Phishing can be found on GOV.UK.

3.3 Can I obtain a refund?

If a consumer is misled into using a copycat website, obtaining a refund may be difficult. The following options may be available (much would depend on the exact circumstances of the case):

- The consumer could contact the relevant site and insist on a refund on the basis they were misled.
- If the sum lost was over £100 and the service was paid for using a credit card, the consumer might be able to make a claim under section 75 of the Consumer Credit Act 1974. Under this section, the credit card company is jointly and severally liable for any misrepresentation by the retailer or trader. This means it is just as responsible for the services supplied, allowing the consumer to also put their claim to the credit card company (although they cannot recover their losses from both).
- If the consumer paid for the online service using a debit card, it might be worthwhile approaching their card provider to see if the sum paid

could be reimbursed using "**chargeback**". Chargeback (also referred to as a "payment dispute") occurs when a cardholder (i.e consumer) questions a transaction and asks their card-issuing bank to reverse it.

A consumer might also wish to seek proper legal advice from their local Citizens Advice Bureau (CAB). The Citizens Advice website contains a useful search tool to help people to find their nearest CAB, there is also the Citizens Advice Consumer Helpline. A CAB adviser may be able to assist the consumer in drafting a formal letter to the relevant site insisting on a refund. If appropriate, Citizens Advice may refer the case on to Trading Standards and action may be taken against a rogue trader.

4 What is being done to combat copycat websites?

4.1 Public awareness campaigns

From time-to-time, Trading Standards join with Citizens Advice to operate "Scam awareness" campaigns. The aim being to increase public awareness and to provide practical advice on how to avoid being scammed. Action Fraud also highlights on its website 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.

4.2 Trading Standards

In respect of wider trading practices, for example, where a company is charging consumers above and beyond official service prices, complaints should be made to the relevant local authority Trading Standards Services.

National Trading Standards (NTS) was set up by the Government in 2012 as part of its changes to the consumer protection landscape. The remit of the NTS is to provide leadership, support, and resources to help combat consumer and business detriment locally, regionally, and nationally. In March 2014, the NTSB received additional funding of £120,000 to investigate copycat websites. In the March 2015 Budget, George Osborne, then Chancellor of the Exchequer, said the Government would give the NTSB an extra £250,000 to help it crack down on copycat websites masquerading as legitimate government services. The NTS issues periodic advice to consumers on how to avoid copycat websites including, "Wise up to the web – avoid being conned by deceptive websites".

The National Trading Standards eCrime Team, funded by the NTS Board, provides a national resource to support all local authority areas in England and Wales tackling internet scams. This team will also investigate and take action against copycat websites. There are separate arrangements in place in Scotland.

4.3 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.[6]

4.4 Advertising Standards Authority (ASA)

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 certain circumstances, the ASA will investigate adverts that appear on copycat websites. Its role is to make sure all advertisements are "legal, decent, honest and truthful" and are not misleading. However, there is no direct action the ASA can take to prevent copycat websites from operating all together.

The Code of Non-broadcast Advertising and Direct & Promotional Marketing (known as the "CAP Code") sets out the rules for non-broadcast advertisements. **All advertising and promotional claims that appear on a website must comply with the CAP Code.** The ASA's remit includes acting on and investigating complaints about advertisements as well as proactively monitoring and taking action against adverts that breach the CAP Code.

In recent years, the ASA has received complaints from members of the public about copycat websites. Typical concerns are:

- It is unclear from the website whether they're an official service.
- The company has appeared above the official body on Google search results.
- Copycat sites charge fees for services that could have otherwise been free or cheaper.
- The consumer did not realise until after the transaction that they would have to pay a handling fee in addition to paying for the service.

Under the CAP Code, an advert should not imply that a business is offering an official service or that it is affiliated with a government office if that is not the

[6] National Cyber Security Centre, "Phishing: how to report to the NCSC", 21 April 2020

case. This might be implied by the company name and/or URL address, the use of certain words such as "official" or "Gov", or from the overall appearance of the site. Nor should the advert imply that the business can save the consumer money if they are, in fact, charging more than the official body. Costs should be clear, transparent, and upfront. This means that if they are charging a compulsory handling fee they should make that clear.

If a complaint about an advertisement is upheld, the advertiser must withdraw or amend the advertisement and not use the same advertising approach again. The ASA can act against a misleading advert on a copycat website, and has various sanctions at its disposal, including:

- a name and shame section on its website,
- 'ad alerts' advising CAP members to withhold advertising space, and
- methods for seeking the removal of a company's paid for search advertisements.

All ASA adjudications are published.

The ASA has already taken action against adverts that appear on copycat websites and are in breach the CAP Code. For example, adverts that implied an affiliation to HM Passport Office, the General Register Office, the UK Intellectual Property Office, and HM Land Registry.

Any formal complaint about the misleading content of an online advertisement should be addressed to the ASA. Full contact details are given on the ASA website, together with an online complaints form.

4.5 Information Commissioner's Office

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.

4.6 Government Digital Service

The Government Digital Service has been working with Google, the largest search engine in the UK, to identify advertisements that mislead consumers. As a result, Google has taken down a series of sponsored adverts from companies running copycat websites. Google is continuing to monitor

misleading adverts and has said it will close the accounts of repeat offenders.[7]

4.7 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. For example, in May 2020, Google introduced a stricter policy on free government services to ensure they are the ones listed first on searches.

Google has plans to verify the identity of all advertisers on its platforms, a process it calls advertiser identity verification.[8] 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.[9]

On 28 April 2021, during a Westminster Hall debate on online scams, Ruth Edwards MP spoke about Google's proposed verification process:

> 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

[7] Google, Advertising Policies Help- Misrepresentation
[8] Google, Advertiser identity verification and ad disclosures FAQ
[9] Ibid

> '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 them being scammed said the advert was not removed by the social media site.[10]

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.[11]

[10] HC Deb, 28 April 2021, c.162-3WH
[11] HC Deb, 28 April 2021, c.163-4WH

5 Government 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".[12] Two important initiatives are outlined below.

5.1 Online advertising programme

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.[13] 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 (CDEI), 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.[14] According to the CMA, competition is not working well in this market, leading to substantial harm for consumers and society as a whole. It recommended that the Government pass legislation to establish a new pro-competition regulatory regime.

The CDEI conducted a review into Online Targeting[15] and Bias in Algorithmic Decision Making[16] as part of their project to strengthen the governance of data driven technology. The ICO has also carried out research into Adtech and Real Time Bidding to ensure that people have confidence in how their data is being used.[17]

[12] HC Deb, 28 April 2021, c.166WH
[13] Online advertising – Call for evidence
[14] Competition and Markets Authority (CMA), Online platforms and digital advertising market study, press notice, 3 July 20120
[15] Centre for Data Ethics and Innovation, Online Targeting: Final report and recommendations, 4 February 2020
[16] Centre for Data Ethics and Innovation, CDEI publishes review into bias in algorithmic decision-making, 27 November 2020
[17] Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019

5.2 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".[18] 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.[19] 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.[20]

However, there were calls to bring online fraud within the scope of the draft Bill. For example, in April 2021, a joint statement[21] drafted by the Fraud Advisory Panel[22] with the support of various fraud prevention organisations including the Cifas,[23] collectively called for a complete re-think of the UK's online defences.

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 scope of this draft Bill had been widened to include financial harms caused by online fraud.

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

---

[18] DCMS & Home Office, "Online Harms White Paper", April 2019, CP 57

[19] DCMS & Home Office, "Online Harms White Paper: Full Government Response to the Consultation", December 2020, CP 354

[20] Ibid, p.25

[21] Joint Position Statement Preventing Fraud on Social Media, April 2021

[22] Fraud Advisory Panel advise government, business and the general public on fraud prevention, detection and reporting

[23] Cifas is a cross-sector fraud sharing organisation

the regulatory framework. In a written statement, Oliver Dowden, Secretary of State for DCMS, explained why the draft Bill now brings user-generated fraud into scope of the regulatory framework:

> 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.[24]

The draft Bill will be subject to pre-legislative scrutiny, which the Minister said he hopes will start as soon as possible.[25]

Scope of the draft Bill

The draft 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 to 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.

[24] HC Deb 12 May 2021 c.6-8WS

[25] HC Deb 12 May 2021 c8WS

6 Parliamentary debates and PQs

6.1 Debates

The issue of copycat websites was raised during Second Reading of the Consumer Rights Bill[26] on 28 January 2014. Stella Creasy, then Shadow Minister for Consumer Affairs, commented on the lack of clarity about prices and gave various examples including the processing fees charged by unofficial websites. The relevant extract is reproduced below:

> **Stella Creasy**: Many consumers experience the frustration of signing up for services or goods and then finding that the terms and conditions are varied because the prices are not clear. A constituent wrote to me this week about a website called Tax Return Gateway, a copycat of a Government website that looks suspiciously like the real deal. My constituent was charged £500 for filling in her tax return, and only after she had paid it was she told that that was the fee for the service, not the tax return itself. Such sites exist for a whole range of public services, including passport applications, visa programmes and driving licences. It seems a simple principle that people should be told the price before they purchase something, but again, the Bill will do nothing to provide for that.
>
> **Mr MacNeil:** The hon. Lady raises an important point. There are scam versions of Driver and Vehicle Licensing Agency sites, and many people do not understand what they are purchasing, far less the costs of it. They do not realise that they are only getting a form to apply for a road tax disc or whatever.
>
> **Stella Creasy:** The hon. Gentleman is absolutely right, and if the Bill met the test of providing the best consumer rights framework that this country can have, such scams would be addressed. Again, we find the Bill wanting on that point, and we will look to address such challenges in Committee.
>
> **Chris Kelly (Dudley South) (Con):** Does the hon. Lady agree that Members should encourage their constituents simply to use the Government's own website at gov.uk, and not to google other alternatives that can lead to scam sites?
>
> **Stella Creasy:** The hon. Gentleman's question reveals one challenge that we face. I would love to sit at a computer with him, google those

[26] Now the Consumer Rights Act 2015, it came into force on 1 October 2015

> websites and see whether he could tell the difference. Making that difficult is one thing that the companies in question do. Itis fair to ask how we can empower consumers, but itis also fair to ask what we can do to ensure that someone knows precisely what they are buying. That does not need to be an unreasonable requirement on terms and conditions, but the Bill does not address that challenge.[27]

The matter was raised again in Public Bill Committee.[28] In speaking to amendment 69 in Schedule 2, Stella Creasy argued that when a consumer has been mis-sold a service because they believe they are using an official site that should be considered an example of unfair behaviour and be open to legal challenge.[29]

The Consumer Minister, then Jenny Willott, agreed that misleading websites that try to palm themselves off as legitimate Government websites needed to be stopped. To this end, the Government had committed an additional £120,000 to the National Trading Standards Board to investigate rogue traders. The Minister said that the Government was also working with search engines to take down misleading websites as they are identified.[30] Amendment 69 was subsequently withdrawn. The Opposition agreed to give the Government time to see if its new approach would work.[31]

On 8 September 2016 there was a Westminster Hall debate on "Scamming: vulnerable individuals", introduced by Julian Knight MP. During the debate, the issue of copycat websites was mentioned by Stuart C. McDonald MP in the context of the losses incurred by consumers:

> Tragically, as we have heard, this is the picture all across the country, with the average victim being 74, and the average loss £1,000, but with many losing much more, yet only 5% of victims report being scammed to the authorities. I have been astonished to learn about the scale of the problem—the number of people losing out, the financial losses resulting, the range of industries affected, the different types of scam, and the techniques and technologies employed, from vishing to phishing and cold calling to copycat websites.[32]

More recently, on 28 April 2021, there was another Westminster Hall debate on "Online scams: consumer protection". Introducing this debate, Ruth Edwards MP highlighted the issue of copycat websites or so-called "clone scams". She said:

---

27 HC Deb 28 January 2014 c.784-785

28 Amendment 69 in Schedule 2, see PBC 6 March 2014 c479

29 PBC Deb 6 March 2014 c485

30 PBC Deb 6 March 2014 c485

31 Ibid

32 HC Deb 8 September 2016 c.519-520

> Clone scams exploit people's trust in reputable brands by carefully mimicking their websites and online presence and even researching and impersonating their sales managers. When they also carry the stamp of an advert, be that on Google, Facebook or any other online platform, many consumers believe that the platform carrying the advert has checked out the company that posted it and that therefore it is an official advert from the company in question. But the truth is that that is rarely the case, because online platforms currently have no legal obligations to protect users against fake or fraudulent content, and that is the primary issue that I would like to address in the debate today.
>
> In the last 18 months, we have been living through a public health emergency, but the pandemic has also had a really profound effect on the way adversaries operate online. We have seen everything: nation state espionage on vaccine programmes, the spread of misinformation and a huge increase in online scams.
>
> […]
>
> Action Fraud figures show that, in the year to June 2020, 85% of all fraud was cyber-enabled. Reports of clone scams increased by nearly 30% between March and April—just in the space of a month—last year. Victims lost more than £78 million to clone scams in 2020. It is hard to put those sorts of figures in the context of individuals, but the average loss for victims is about £45,000.[33]

Stephen Timms MP raised the issue fake websites being used to perpetrate pension fraud:

> Pensions Scams Industry Group estimates that 40,000 people […] were scammed out of pension savings in the five years after the introduction of the pension freedoms and lost £10 billion between them. […] losing pension savings after a lifetime of work is a devastating experience, […] most of the problem is online. In September, Aviva told the Work and Pensions Committee that in the previous six months – since the start of lockdown – it had identified 27 fake websites purporting to be Aviva trying to defraud pension-age customers of their investments.[34]

In response, Victoria Atkins, the Parliamentary Under-Secretary of State for the Home Department, outlined what the Government was doing to combat online fraud. She said:

> As this year has demonstrated, more and more people are online at home, and we are acutely aware of the importance of staying safe in the virtual world. We are focusing the Government's efforts on tackling fraud and online scams in three key areas: prevention;

[33] HC Deb, 28 April 2021, c.161-2WH

[34] HC Deb, 28 April 2021, c.165WH

> catching the criminals responsible; and supporting the victims of these despicable crimes.
>
> Prevention involves not just victims, the industry and tech companies, but all of us. That is how we will be able to tackle these crimes. We must ensure the private and public sectors prioritise these types of frauds. That is critical to preventing the harms that we have heard about and the economic damage to our businesses and disrupting the organised criminals who perpetrate these crimes. To do that, the Government are taking steps to ensure that fewer people fall foul of these scams.
>
> The National Cyber Security Centre has been at the forefront of that effort. Last year, it launched a new suspicious email reporting service, which makes it easier for the public to highlight suspicious emails and websites. The service has already led to more than 5.5 million reports, and more than 41,000 scams and 81,000 websites have been taken down.
>
> Importantly, we also need to help the public spot these scams.
>
> [...]
>
> Last year, we launched a new gov.uk page to help keep the public safe online. I recommend it to colleagues, who can perhaps disseminate it through their constituencies. 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 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.[35]

6.2 Parliamentary Questions (PQs)

The issue of unofficial websites charging for processing Government services has also been raised in various PQs. For example, on 21 January 2014, the following exchange took place between David Davis MP and Mark Harper MP:

> **Mr David Davis:** To ask the Secretary of State for the Home Department what recent assessment she has made of the prevalence of copycat websites for passport applications and renewals; what estimate she has made of the costs to consumers of using such

[35] HC Deb, 28 April 2021, c.165-166WH

> websites; and what steps she is taking to inform the public about such websites.
>
> **Mr Harper**: The website www.gov.uk is the only provider of the British passport and passport applicants should use the official Government website.
>
> All third-party sites stating that they are offering passport services are required to carry a clear disclaimer that they are not an official passport site or affiliated in any way to Her Majesty's Passport Office. The Government Digital Service is leading a cross-government exercise with organisations such as the Office of Fair Trading, the Advertising Standards Authority, search engine providers and various trading standard bodies to curtail the activity of websites that advertise their services in misleading ways, using existing consumer protection legislation. Where Government have become aware of websites make misleading claims in their advertising they have brought these complaints to the attention of the Advertising Standards Authority.
>
> Her Majesty's Passport Office also continues to work with the Association of British Travel Agents to raise public awareness of third-party websites.
>
> **Mr David Davis:** To ask the Secretary of State for the Home Department if she will meet Google to discuss the profits they make from copycat websites which charge for passport renewals and appear above Government department and agency websites in search results.
>
> **Mr Harper:** The website www.gov.uk is the only provider of the British passport and passport applicants should use the official Government website.
>
> The Government Digital Service is leading a cross-Government exercise with organisations such as the Office of Fair Trading, the Advertising Standards Authority, search engine providers (including Google) and various trading standards bodies to curtail the activity of websites that advertise their services in misleading ways.
>
> Ministers are planning to meet Google early this year to discuss Google's enforcement of its own terms and conditions for advertising on its search results pages.[36]

On 8 January 2015, Ed Vaizey, then Culture Minister, said that the Government was "committed to stopping" copycat websites:

> **Mr Vaizey:** We have taken a lot of action. We have worked closely with the search engines to ensure that they implement their terms

[36] HC Deb 21 January 2014 cc.101-102W

> and conditions on copycat website advertising, and the click-through to Government websites has increased by 30%. There is a problem with blocking transactions for websites that charge. A lot of Government services are free, and we would not necessarily know whether other websites were charging. We know what Transport for London has done and we continue to keep the issue under review.[37]

Mr Vaizey went on to say that the Government had "made progress with strengthening search engine terms and conditions and started to move away from copycat websites having prominence and seen an increase in people using Government websites." [38]

On 25 October 2016, Craig Whittaker MP asked what steps the Government is taking to monitor copycat websites that offer government services. Chris Skidmore MP provided the following written answer:

> Copycat websites undermine trust in online services, and this government is committed to stopping them. We're taking action on three fronts.
>
> First, we are taking action to shut down such sites and prevent them from appearing in search engines. We are working with search engine providers to ensure they implement their terms and conditions on copycat website advertising, increasing the click-through to Government websites by 30%. Security teams in departments across government are also actively monitoring the internet for bogus sites and taking action accordingly.
>
> Secondly we improve the consistency and quality of Government websites, so that consumers can recognise and trust official sources of information.
>
> Finally, we are working closely with other bodies such as the Advertising Standards Authority (ASA), the National Trading Standards Board (NTSB) and Which? to raise awareness of this issue and ensure action is taken where appropriate.[39]

[37] HC Deb 8 January 2015 c371

[38] HC Deb 8 January 2015 c372

[39] PQ 25 October 2016 UIN 50062

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary