The Aviva Fraud Report:

The online fraud epidemic during the pandemic

The Aviva Fraud Report uses consumer research to investigate fraud and scams which relate to pensions, savings, investments, car insurance and life insurance.

August 2021

Aviva Fraud Report 2021: Almost **9** out of **10** people (**87%**) think that the government should introduce legislation to ensure that search engines and social media sites do not mislead consumers or promote financial scams through the advertising they allow to appear on their sites.

Introduction

Welcome to the Aviva Fraud Report

In this, the second Aviva Fraud Report, we interviewed people across the UK to gather their views and experiences of fraud, particularly during the pandemic.

"The scale of online fraud has accelerated through the coronavirus pandemic, which has resulted in a deluge of opportunities for fraudsters over the past year. The current online environment, combined with the challenging economic conditions and increased financial strain on consumers, is creating the perfect storm for fraudsters to exploit the most vulnerable.

While the types of financial scams are generally the same as those before the pandemic, coronavirus has been used as the hook to lure victims. Being in lockdown has meant more people using the internet to search for, and buy, financial services and products.

The scams range from attempts to sell people unsuitable car insurance to, at worst, stealing their entire retirement savings. Imitation websites that copy-cat well-known financial services brands, and misleading adverts are now commonplace. The impact on victims is not just financial either, it has a detrimental effect on people's mental wellbeing too.

It's more important than ever that people report any suspicious communication to Action Fraud, their financial services provider or the authorities. We launched our online Fraud Hub at the height of the pandemic to help protect the public and our customers from financial scams. It includes practical advice for consumers on how to spot fraud.

The tactics deployed by fraudsters constantly evolve. As lockdown measures in the UK are eased, it's inevitable the fraudsters' tactics will continue to develop. With fraud undermining consumer trust in financial services, it's vital that the industry continues to work together with the authorities to protect the public and our customers.

We believe the Online Safety Bill presents an opportunity to protect financial services consumers at every stage of their online journey. We welcome the recent inclusion of user-generated fraud - such as that promoted on social media sites - within the scope of the regulatory framework. We also support the financial services industry in calling for the legislation to include financial scams promoted by paid-for adverts."

Rob Lee
Director of Fraud Prevention at Aviva

Contents

The victims

Clone-firm investment fraud

Action Fraud data, published by the Financial Conduct Authority (FCA), reported **£78 million stolen** in '**clone firm**' **investment scams** between January-December 2020[i].

These are based on real case studies of people who have been affected by financial crime which have been anonymised to protect the individuals' identities.

The most common types of online fraud and the experience of real-life victims

Misleading car accident claim adverts

"I was recently involved in a road traffic accident. In a state of post-accident shock, I searched for Aviva's claims number on my mobile phone to report the accident from the roadside. When I looked at the results from the search, I clicked on what I thought was a link to Aviva's claims department.

"I reported the accident and was put in touch with a company to provide a courtesy car while my vehicle was being repaired. They also arranged for the recovery and storage of my car until it could be repaired.

"The claims handler, who indicated he worked on behalf of Aviva, told me not to speak to anyone else about the claim, and provided a mobile phone number for me to text with photos of the damaged vehicle."

In fact, the customer had called an accident management company, which was one of the first results that popped up on the search engine – and a paid-for ad. Rob Lee, Director of Fraud Prevention, picks up the story from Aviva's end.

"Believing he was dealing directly with Aviva, our customer was unaware that instead of sending the vehicle to be repaired, the accident management company put his car in storage, racking up charges, so they could make extra money from a lucrative 'credit hire' contract that would see costs for the claim escalate out of control.

"The reason for this is that it is the at-fault insurer that pays for these costs. Accident management and claims management companies realise this, and so try to insert themselves into a claim to profiteer from the claims process - even going so far as to deceive the customer that they are dealing with their insurer.

"In this case, the ad that the customer clicked appeared when searches for "Aviva motor accident", "Aviva accident claims" or "Aviva claim report" were entered, and so it is understandable why the customer believed he had contacted Aviva directly.

"However, since the customer had contacted an accident management company and not Aviva, we only became aware of his claim a month later. By this point, storage costs for the vehicle exceeded £1,500 and continued to grow daily, while the cost of the replacement vehicle was around £1,300 and growing. Meanwhile – nothing was being done to help the customer settle his claim and get him back on the road.

The victims

“As soon as we learned of the claim and the customer’s circumstances, we took the necessary action to manage the claim ourselves. But before the accident management company would let us take possession of the customer’s car, they said we had to pay the storage costs, and they wanted to continue to manage the lucrative credit hire contract for the replacement vehicle.

“We have since accepted that our customer was at fault for the accident, meaning it is unlikely the storage and credit hire costs will be able to be reclaimed from the other party - regardless of the fact that they were excessive and made without our knowledge.

“Insurers should not be in the position of having to pay costs for something that we had no control over – especially when they are being managed by unknown accident management companies whose objective is to run costs up for their own profit. This pushes up the cost of insurance for everyone, and adds confusion and delay to the claims process, which is a poor outcome for the customer.”

Our customer concluded, “Like myself, most people don’t realise that when they sign credit contracts with credit hire organisations and accident management companies that they are ultimately responsible for paying those costs, even if they are insured - no matter what the accident management company might tell you.”

Aviva has seen cases where individuals were placed in credit hire contracts - some for months and even years – and when liability was finally established and it was determined that they were at fault, they faced a bill for tens of thousands of pounds. All because an accident management company was able to manage the claim before the insurer found out and trapped the customer into expensive contracts which put them at serious financial risk.

The victims

“Aviva saved me from losing £85k of my life savings to a fraudster.

I’d been contacted out of the blue by somebody claiming to be a representative from Aviva, who got me interested in investing in an Aviva Bond. After some thought, I contacted the Aviva switchboard to speak to the individual again – I gave them his name.

As I couldn’t speak to him over the phone, I was given the email address for his personal assistant (PA). I then wrote an email to the individual at Aviva and his PA.

I got an email back from his PA who seemed quite confused, having not recognised the email address for her manager.

She spoke to her manager at Aviva, who was concerned and therefore contacted me himself.

It turns out the representative who had contacted me was a fraudster pretending to be a real person working for Aviva.

Fortunately, the Aviva financial crime team contacted me just in time. I was on the verge of investing £85k of my life savings.

What’s worse is that I’d also recommended the fake bond to a friend. We both had a very lucky escape.”

Aviva in Action:

Since May 2020, Aviva has investigated over **1,300 incidents of fraud**, which have been reported to its Financial Crime Intelligence Unit. It has supported the victims of fraud and prevented others from becoming a victim.

Paul Pisano,
UK Financial Crime Director at Aviva

“**Clone-firm investment scams** are unbelievably convincing and **pretending** to be a **well-known brand name** is fundamental in persuading consumers to part with their cash and, sadly, their life savings.

The fraudsters set-up **imitation websites** which look like well-known financial services brands - often using the legitimate company name within the domain name - through which to sell bogus products to unsuspecting consumers. **Fake comparison-style websites** have also been set-up, which encourage consumers to provide information about themselves and the product they are interested in buying, under the guise of getting the best deal.

Victims of clone-firm investment scams tend to be people approaching retirement age who have access to their pension pot and are browsing the internet, in the hope of finding higher returns. They often have large amounts of cash at their disposal, and which is currently making low returns in a low-interest environment.”

Chapter 1:
Fraud during the pandemic

Aviva in Action:
Aviva launched its first fraud report in July 2020, at the height of the pandemic, to help raise public awareness of fraud.

How many people have been targeted by a coronavirus scam?

- More than **two in five** (**42%**) have received emails, texts, phone calls and other communications that mentioned coronavirus and which they suspected to be related to a financial scam.

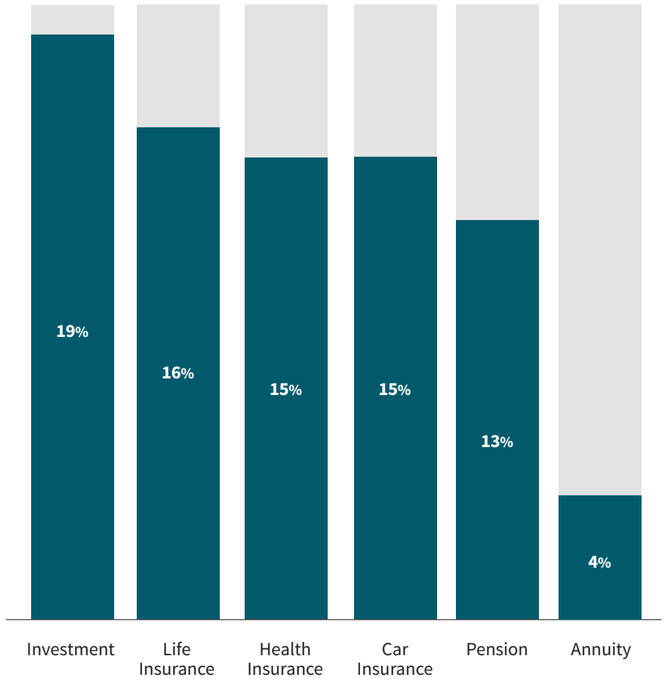
Aviva Fraud Report 2020: This is almost double the number of people who reported being targeted by a Covid-19-related scam a year ago (**22%**).

- More than **two in five** (**43%**) of those who received a communication that they suspected to be a financial scam didn't report it.

Aviva Fraud Report 2020: This is a slight improvement on last year (**46%**) but there is clearly still more work to do in encouraging people to report fraud.

- **One in eight** (**13%**) have been the victim of a financial scam which related to coronavirus:
  - 25-34 year-olds were the most common victims of fraud (**31%**) followed by those aged 16-24 (**23%**)
  - Almost nine in ten (**85%**) victims said the fraudsters pretended to be from a company they already deal with.
  - And **46%** said being the victim of a scam negatively affected their mental health, their trust in others (**45%**) and their confidence in the financial services system (**37%**).

Financial services products targeted by a coronavirus scam



% of people who reported receiving suspicious communications June 2020 – June 2021

Chapter 2:
Online fraud

How has consumer internet usage changed during the pandemic?

- Half (**50%**) of people have used the internet more – either significantly or a little - to search for products and services over the last year
- 16-24 year-olds are most likely to have increased their online shopping (**65%**)
- Two in five (**39%**) people aged 55 and over said they have also used the internet more for shopping

Lockdown has transformed spending habits in the UK and accelerated adoption of the internet, with one in two people saying they used the internet more – either significantly or a little - to search for products and services over the last year. The internet now represents about one-third of all retail sales in the UK, up from about one-fifth over the past year alone[ii].

> "The **challenges** posed by **lockdown conditions** has shifted the mindset of millions, opening the door to more people buying financial services and products online. While this brings opportunities for making it easier to buy products, it does also **open the door to fraudsters** looking to prey on the **vulnerable**."

Rob Lee,
Director of Fraud Prevention at Aviva

The internet will be age-neutral by 2028.

According to the Office for National Statistics data[iii], internet use in the UK is at a record high, with **92%** of adults recorded as recent users. And it is those aged 55-and-over – sometimes referred to as 'boomers' – who are driving the fastest pace of growth. Aviva estimates that the internet will be age-neutral by 2028, with virtually **100%** of all ages using the internet. While more younger people (**65%** of 16-24 year-olds) have increased their online shopping over the last year, there is still a number of older people who have upped their usage, too (**39%** of 55+ year-olds). It is out-of-date to think of the internet as a tool for the young.

Chapter 2:
Online fraud

Action Fraud reported in May this year that reports of investment fraud have increased significantly since the start of the coronavirus pandemic, with victims having lost over **£63m** to **investment fraud scams** on social media[iv].

Do consumers trust the internet?

More than half of internet users (53%) don't trust that the adverts on search engines are placed by a legitimate financial services company or provider. And more than half (56%) don't believe that search engines verify the authenticity of the financial product, service, or provider that they allow to be advertised on their platform. But there is a large difference in trust by age. Those aged over 55 were much less likely to trust the results of a search engine than those aged 16–24; only 29% of over-55's compared to 59% of 16–24 year-olds.

The majority (68%) of consumers use a search engine to help find financial products, services and providers online. Just over half (56%) of those who use a search engine trust the results, but two in five (40%) don't and therefore do additional checks on the company or provider.

When using the internet to search for financial products and services, more than one in nine (11%) just click on the first result that comes up. Half of people will look for a result from a company that they recognise. Only 19% will avoid clicking on the advertisements.

Has online fraud increased during the pandemic?

The scale of fraud has accelerated through the coronavirus pandemic, which has resulted in a deluge of opportunities for fraudsters over the last year. Aviva's research found two-in-five (42%) people have been targeted by a Covid-19 scam. This is a 91% increase over the last year in the number of people who reported receiving emails, texts, phone calls and other communications mentioning coronavirus, and which were suspected to be part of a financial scam.

> "There is a **clear mistrust of financial services adverts online**. However, there is **no legal responsibility** for technology firms to verify the legitimacy of the companies which pay them to publish adverts on their platforms. This potentially **leaves millions of internet users exposed** to adverts placed by **unscrupulous companies**."

Rob Lee,
Director of Fraud Prevention at Aviva

Chapter 2:
Online fraud

What is government doing to protect consumers from fraud online?

The government says the draft 'Online Safety Bill delivers the government's manifesto commitment to make the UK the safest place in the world to be online while defending free expression'[v]. It is intended to impose a "duty of care" on social media companies, and some other platforms that allow users to share and post material, to remove "harmful content". Its intention is to tackle user-generated fraud and place responsibility for fraudulent user-generated content, such as posts on social media, on online platforms.

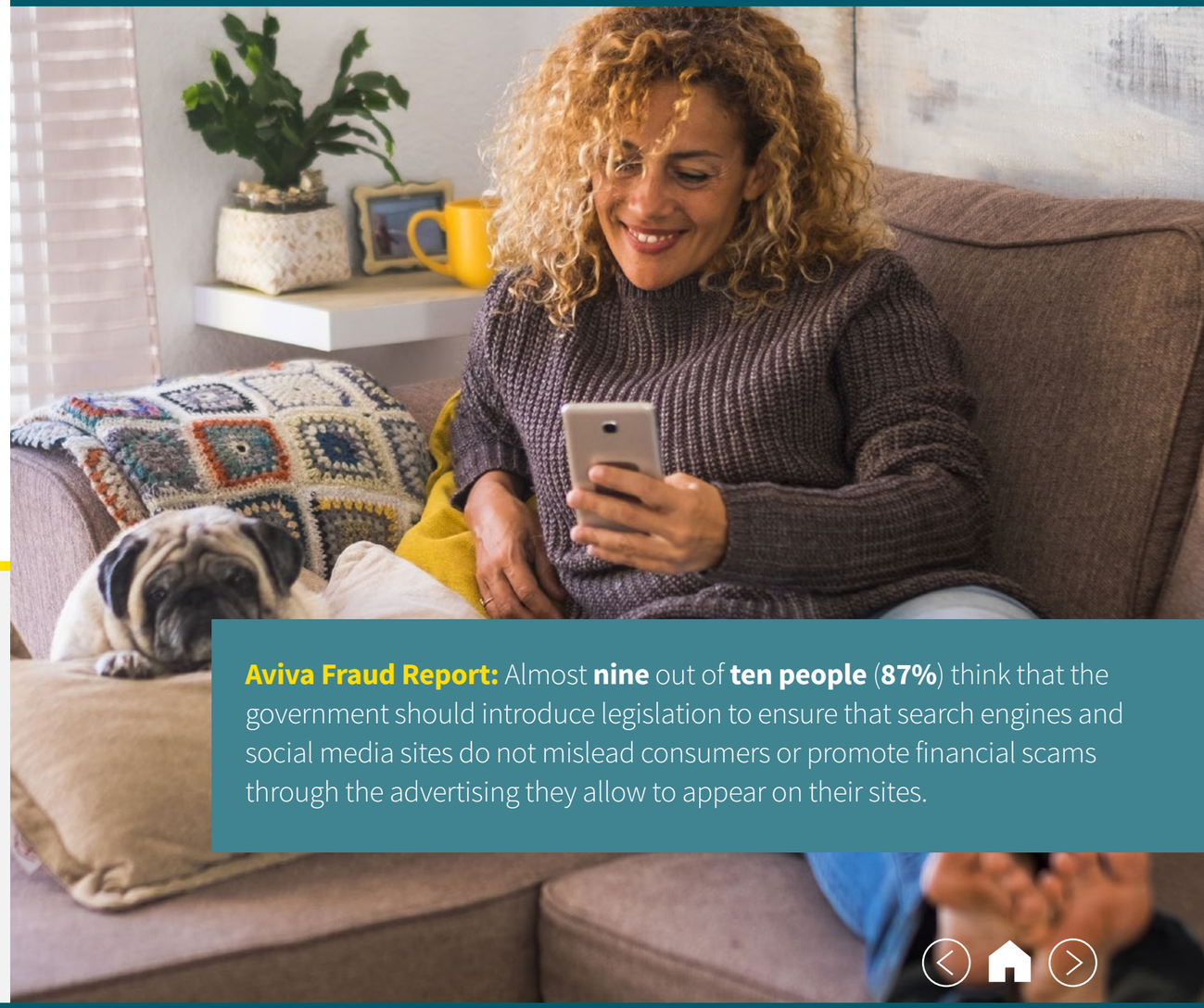
One of the largest online technology companies, Google, recently announced that from September, all advertisers selling a financial product on its platform must be authorised by the Financial Conduct Authority (FCA) or exempt. It's a welcome move, and one which further demonstrates the importance of ensuring the scope of the Online Safety Bill includes financial scams promoted by paid-for adverts.

"We believe the **Online Safety Bill** presents an opportunity to **protect financial services consumers** at every stage of their online journey. We welcome the recent inclusion of user-generated fraud - such as that promoted on social media sites - within the scope of the regulatory framework. We also **support the financial services industry** in calling for the legislation to include financial scams promoted by paid-for adverts."

Rob Lee,
Director of Fraud Prevention at Aviva

Aviva in Action:

Aviva is supporting the financial services industry in calling for the **Online Safety Bill** to include financial scams promoted by paid-for adverts.



Aviva Fraud Report: Almost **nine** out of **ten people** (**87%**) think that the government should introduce legislation to ensure that search engines and social media sites do not mislead consumers or promote financial scams through the advertising they allow to appear on their sites.

Chapter 3:
Financial resilience and fraud

Aviva in Action:
Aviva launched its online **Fraud Hub** on **www.aviva.co.uk** in May 2020, at the height of pandemic, to help protect the public and its customers from scams. It includes practical advice for consumers on how to spot scams.

Has the pandemic left people who are in debt more vulnerable to scams?

Nearly a quarter (23%) of those surveyed said their total amount of debt had increased over the past year, rising to almost one-third (32%) of 16–24 year-olds.

More than 1 in 10 (13%) have been the victim of a financial scam which related to coronavirus. Two-thirds (66%) of those who have been the victim of a financial scam also saw their total debts increase over the last year. This shows a clear correlation between low financial resilience and being the victim of a scam or fraudster.

Two-thirds (66%) of those surveyed said saving money on household bills has increased in priority since the pandemic began. The Financial Conduct Authority (FCA) said the Covid-19 pandemic has left over a quarter of UK adults with low financial resilience[vi].

Fraudsters understand that those with low financial resilience are more likely to want to save money on household bills, like insurance.

Insurers believe that fraud is typically committed for one of two reasons: need or greed. Supporting this, the Insurance Fraud Bureau found that insurance fraud grew by 17% in 2008, the year of the financial crash[vii].

Insurers are concerned that the 'need' rationale behind some insurance fraud is set to grow again. The recessionary factors caused by the pandemic have arguably created the biggest fraud threat to customers in a generation. Currently, government intervention is mitigating many of these financial impacts, but as government withdraws financial support for businesses and individuals and some consumers feel increased financial pressure, we expect to see more fraud in the coming year.

Application fraud

Against the backdrop of the pandemic and the interwoven economic challenges, Aviva's fraud data shows that car insurance application fraud grew by 34% in 2020, with fraud identified on more than 29,000 motor policy applications.

Although motor insurance premiums are currently the lowest in five years[viii], our research found that one-in-six people (17%) changed their age, address or claims history to get a cheaper quote on their insurance. For young drivers, this more than doubled to 37% who altered their details in search of a cheaper quote. This increase may in part be explained by the fact that 75% of young people (aged 16–24) said saving money on their bills had increased in priority during lockdown.

It's worth noting, as four-out-of-five people (81%) know, that not being honest on an insurance application puts the customer at risk of having worthless insurance, as in the event of an accident, a claim could be denied.

Chapter 3:
Financial resilience and fraud

Ghost broking

‘Ghost broking’ is at the sharp end of application fraud and is when an unauthorised insurance intermediary (ghost broker) fraudulently takes out motor insurance policies on behalf of people looking for cheap car insurance. The ghost broker usually charges a sizeable fee on top of the premium.

Ghost broking is increasingly common, especially within some vulnerable customer groups. Just over one-in-five people (21%) said they had been approached by someone who they suspected was not an insurance broker but who was claiming to offer access to cheap insurance. Young people (aged 16-24) are the age group most targeted by ghost brokers, with 43% saying they have received this type of approach.

Ghost brokers commonly use social media and their own websites to promote their ‘services’. A search for ‘cheap insurance’ on popular social media platforms typically reveals several suspicious posts promoting cheap insurance.

While only 18% of people said they would contact a suspect post on social media offering cheap insurance, this doubled to 36% for young people. Purchasing insurance through unauthorised channels puts the policyholder at risk of driving without insurance, and exposed to the risk of fines, conviction and the confiscation of their vehicle. In the event of an accident, they risk being left to cover the cost themselves.

Those who access a ghost broker’s services are usually left out of pocket, having paid fees and “premiums” to the broker for often worthless products. Ghost broking is a crime and is linked to identity and payment card fraud, which further impacts a wider group of victims. It also pushes the premiums up for genuine customers.

Chapter 4:
Reporting fraud

Why don't more people report fraud? Is it embarrassing to be the victim of fraud?

More than two in five (43%) of those who received a communication that they suspected to be a financial scam didn't report it.

Aviva Fraud Report 2020: This is a slight improvement on last year (46%) but there is clearly still more work to do in encouraging people to report fraud.

Fraud shame

Almost one in three (30%) said they would be embarrassed to admit to being the victim of a financial scam, whether to friends or family or the authorities.

People in Newcastle (35%) are most likely to be embarrassed to admit being the victim of a financial scam, followed by those in Leeds (33%) and then Cardiff (33%). People in Plymouth were the least likely to be embarrassed (18%).

One in eight (13%) have been the victim of a financial scam which related to coronavirus. Of those, 46% said being the victim of a scam negatively affected their mental health, their trust in others (45%) and their confidence in the financial services system (37%).

> "People often feel **embarrassed** to admit they have **fallen for a scam** but there is no shame in it - these fraudsters are surprisingly professional and convincing. Imitation websites which **copy-cat well-known financial services brands**, and misleading adverts are now commonplace. The impact on victims is not just financial either, it has a detrimental effect on people's mental wellbeing too. With fraud also undermining consumer trust in financial services, it's vital that the industry continues to work together with the authorities to **protect the public and our customers**."

Paul Pisano
Financial Crime Risk Director at Aviva

The most common reasons for not reporting fraud were:

1. **45%** didn't know who to report it to
2. **29%** didn't know they should report it
3. **29%** didn't think it would be investigated
4. **21%** couldn't be bothered

Chapter 4:
Reporting fraud

Aviva in Action:
Aviva works closely with law enforcement agencies to report fraudulent activity and appropriately share intelligence, to help combat fraud.

How to report suspected fraud

You should report misleading websites, emails, phone numbers, phone calls or text messages you think may be suspicious. Do not give out private information (such as bank details or passwords), reply to text messages, download attachments or click on any links in emails if you're not sure they're genuine.

Suspicious emails should be forwarded to report@phishing.gov.uk so the **National Cyber Security Centre** (NCSC) can investigate it.

Text messages should be forwarded to **7726** – it spells out SPAM. It's free – and this will share the suspected rogue text with your mobile phone provider.

Adverts: Consumers can report suspected online scams or misleading adverts to the **Advertising Standards Authority**, including those found in search engines, websites or on social media. You can also report scam or misleading adverts to Google if you found them in Google search results, or report to Bing if you found them in Bing search results.

If you think you've been the victim of an online scam or fraud, contact **Action Fraud**, either online or by calling **0300 123 2040**.

ICO: you can report spam texts or cold calls to the Information Commissioner's Office (ICO) at www.ico.org.uk.

Why is it important to report fraud?

It's more important than ever that people report any suspicious communication to Action Fraud, their financial services provider, or the authorities. We launched our online Fraud Hub at the height of the pandemic to help protect the public and our customers from financial scams. It includes practical advice for consumers on how to spot fraud.

As lockdown measures in the UK are eased, it's inevitable the fraudsters' tactics will develop beyond coronavirus. The financial services industry needs to work together with the authorities to support each other in protecting the public and our customers. The more people report fraud, the more pieces of the puzzle we have, and the better chance we have of tackling it.

Insurers are dedicated to fighting fraud

The insurance industry is determined to do everything it can to protect honest customers from being the victims of fraud. Fraudsters are entrepreneurial, and scams can range from non-existent motor insurance cover, being involved in a staged crash to being offered bogus investment opportunities which could put someone's life savings at risk. If something seems wrong, report it – to your insurer, the Insurance Fraud Bureau's confidential cheatline, **Action Fraud**, or the police.

Chapter 5:
Spot fraud - the most common scams

Misleading car accident claim adverts

Accident management companies advertise on search engines to try to 'capture' customers who are looking to make a claim following a road traffic accident. Many customers don't have their insurer's telephone number stored on their phone, and so use their mobile phone to search for the telephone number. Motor insurance customers would be wise to safely store their car insurer's claims number in their phone so they can safely, and quickly, contact them if they need to make a claim.

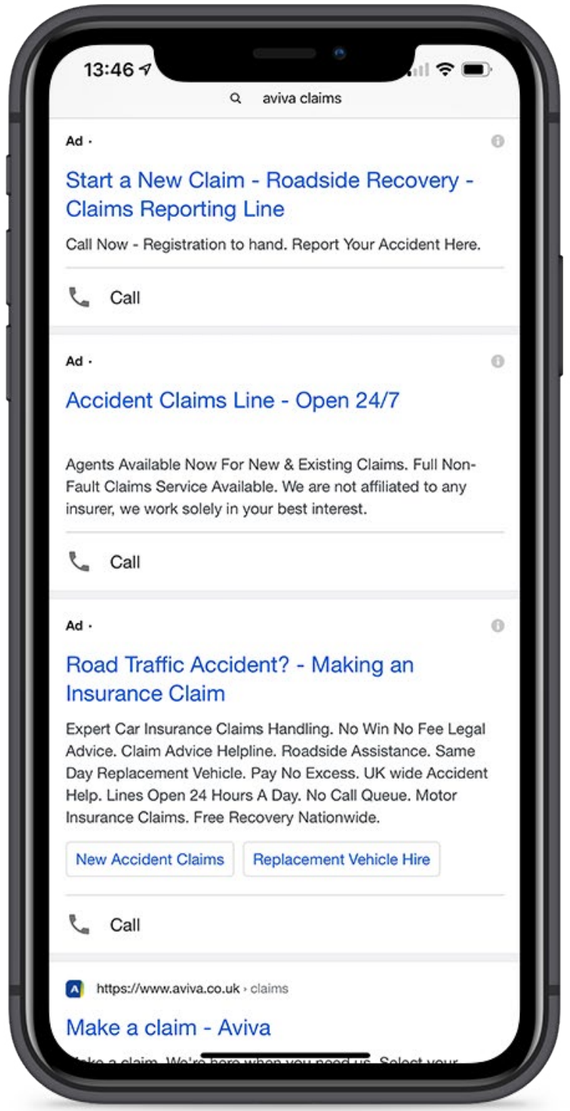
In the event of having to make a claim after a road traffic accident, 27% of people said they would look up their insurer's telephone number on their phone. While it is not illegal to target these individuals, some companies go too far using generic terms or language in order to deceive the customer that they are dealing directly with their insurer. The reason for this is so that the accident management company can handle the claim, and inflate the cost of the repair, replacement vehicle and other costs - all to line their own pockets.

Why is this a problem?

It is the at-fault insurance company that is responsible for paying the costs of a claim. Inflating the cost for vehicle repairs, the replacement vehicle, and other charges such as storage, all serve to push up the cost of insurance. Where customers are not clear who is handling their claim, it also leads to confusion, and worry over the safety and reliability of the repairs that have been made to their vehicle.

More than half (52%) of people said that they would be angry that they had been misled if they found that their car had been repaired by an unknown party instead of their insurer. And 39% said they would be worried that their car repair claim was not handled by professionals.

Perhaps the biggest risk to consumers, however, is that when they don't make a claim through their insurer, they place themselves at risk of being liable for the costs of the claim. When making a claim through a claims management company, consumers will be asked to sign credit agreements for the repair and replacement vehicle. These agreements state that the customer will be responsible for the costs of the claim, if the costs cannot be recovered from the at-fault party. If the at-fault insurer challenged the costs, or if it later transpired that the customer was at fault, they could face the bill for the replacement vehicle and in some cases, the repair. These costs can run to the tens of thousands of pounds.



Chapter 5:
Spot fraud - the most common scams

When a **customer clicks** on a **search engine ad** from a claims management company to report their claim, it launches a money-spinning operation for **inflated storage fees, repair costs** and **replacement vehicle hire** – all of which are borne by the at-fault insurer. However, if it later transpires that the customer who signed the agreements is at fault for the accident, then the **customer could be responsible for paying for these costs**. Likewise, if the at-fault insurer successfully challenged these costs, then the customer who signed the agreements could be responsible for paying them. These practices not only put consumers at risk of serious financial harm, but they also put upward pressure on motor insurance premiums for all customers.

Customer stood at the scene of the **incident**

Customer goes onto **search engine** and types **'Aviva claims line/number'** number on their mobile phone

Customer speaks to an accident management company – only interested in a non-fault claim, which they take control of

Storage/recovery

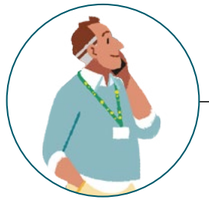
Garage/repairs

Replacement vehicle

The **customer's vehicle** may be recovered into **storage** whilst liability is negotiated with the 'at fault insurer'. A replacement 'credit hire' vehicle is often supplied at the same time instead of the courtesy car the customer has already paid for as part of their policy. Both services add extra cost which the **customer is ultimately liable** for. Repairs may not even begin until liability is admitted, which can take weeks or longer, adding additional cost.

The customer continues with the accident management company, unaware they are **not dealing directly with Aviva**. The claim is managed for the imposter's profit. When the repairs are made and the final bill is presented to the 'at fault' insurer, concerns about liability or cost could mean that the insurer refuses to pay.

OR



AVIVA

Customer calls **Aviva claims line** for an update on their claim, only to find that the claim has not been notified to them. Aviva will try to take over the claim and manage costs effectively whilst ensuring the **customer's claim is handled promptly**, however due to the existing contracts which bind the customer to the companies involved, this is often impossible and the customer has little choice but to continue with the imposter's claims service.

Customer potentially left with **liability** for **garage / storage / replacement car costs**.

AVIVA

Customer claim is handled by Aviva after delay caused by imposter.

AVIVA

Customer puts Aviva's official claim line into their phone contacts

Chapter 5:
Spot fraud - the most common scams

Action Fraud data, published by the Financial Conduct Authority (FCA), reported **£78 million** stolen in 'clone firm' investment scams between January-December 2020[ix].

Clone-firm investment fraud

The fraudsters set-up imitation websites which look like well-known financial services brands - often using the legitimate company name within the domain name - through which to sell bogus products to unsuspecting consumers. Fake comparison-style websites have also been set-up, which encourage consumers to provide information about themselves and the product they are interested in buying, under the guise of getting the best deal.

Victims of clone-firm investment scams tend to be people approaching retirement age who have access to their pension pot and are browsing the internet, in the hope of finding higher returns. They often have large amounts of cash at their disposal and which is currently making low returns in a low-interest environment.

The policy review

A typical Health and Life insurance scam involves a cold call telling consumers, "It's time to review your policy". The fraudsters will claim they're from a reputable insurance company or that they've been asked to do this by the regulators – all in a bid to gain trust. They may offer lower premiums but what they don't mention is that the lower premium also means reduced cover – often leaving the consumer with a worthless policy.

Pensions, Investment & Savings

As stock markets have fallen in value and the Bank of England base rate is at 0.1%*, people with investments are much more vulnerable to falling victim to scammers offering unrealistically high rates of return. People are usually offered a 'unique' investment opportunity or the chance to unlock cash in a pension.

Ghost broking

Ghost broking continues to present a significant threat to customers, both in terms of exploiting some innocent customer groups, potentially leaving them with worthless policies – essentially uninsured – but also by increasing the cost of motor premiums for honest customers.

Consumers should be wary of insurance offers from unusual sources such as advertisements on social media platforms or communications via messaging apps or services. Consumers can check the legitimacy of an insurance offer through the broker's status on the Financial Conduct Authority (FCA) or British Insurance Brokers Association (BIBA) websites, or alternatively contact the insurer directly. Ultimately, if an insurance premium seems "too good to be true", then it probably is.

How victims are targeted

Copy-cat websites

These often look professional, but there are some warning signs:

- Images on the website which appear blurry or low-quality.
- Text on the website which is poorly written and includes spelling or grammatical errors.
- Missing contact details.
- Broken links that, when clicked on, take you to a blank page.
- Advertising offers which appear too good to be true.

Phishing emails

These messages are designed to make you react emotionally to whatever you're receiving. With anything Covid-19-related, you're likely to have a greater emotional reaction and click any virus-infected links or open the malicious attachments. Fraudsters are preying on our vulnerabilities around the whole situation – offering financial support during this difficult period.

Chapter 6:

Don’t be a victim – top tips on how to avoid falling for a scam

Spot

- Scams usually begin with unsolicited contact – be extremely wary of anyone contacting you that you don’t recognise.
- Criminals actively use emails, texts, phone calls, messenger apps (e.g. WhatsApp) and social media to trick people. Look out for suspicious contact across all these channels, especially when you’re asked to:
  - Make a payment.
  - Amend or confirm bank details.
  - Click through to a website for ‘important’ information.
- Often, fraudsters will try to rush you or add time pressure.
- If it sounds too good to be true, it probably is. If you’re approached by anyone offering a great deal – be it lower life insurance or income protection premiums, the chance to unlock cash in your pension or a fantastic investment opportunity with guaranteed returns – be very cautious.

Pause and verify

- Don’t click on or attachments in emails and texts you don’t trust.
- Search for official guidance by visiting an organisation’s website.
- If you suspect a caller isn’t who they say they are, hang up the phone and call them back later on a number you trust (e.g. on previous correspondence).

Report and protect

Help protect others by reporting all suspicious emails, calls and texts you receive to Action Fraud: www.actionfraud.police.uk or 0300 123 2040.

How to protect yourself online

- Installing software and system updates when prompted – outdated software and apps could leave a device open to security flaws.
- Setting strong passwords – a weak password could make it easier for the wrong people to gain access to your accounts and devices.
- Installing antivirus software - these viruses could take over a device to steal information.
- Reducing digital footprint – limiting information shared on social media platforms.

Methodology:

All figures, unless stated otherwise, are from Aviva's research, conducted by Censuswide with a sample of 2,005 nationally representative respondents, between 30 June and 05 July 2021.

Categorising the pandemic time frame between 1 March 2020 and 05 July 2021, and the pre-pandemic time frame as 01 January 2019 and 28 February 2020.

Censuswide abide by and employ members of the Market Research Society which is based on the ESOMAR principles.

About Aviva

We are focused on the UK, Ireland and Canada where we have market-leading positions. We aim to be the UK's leading insurer; and we are the only insurer in the UK able to meet the needs of customers at every stage of their lives.

We offer a wide range of insurance and savings products which help people to protect what's important and save for a more comfortable future.

We've been looking after customers for more than 320 years. We are deeply invested in our people, our customers, our society and the planet. We're here to be with people today, as well as working for a better tomorrow.

The Aviva newsroom at www.aviva.com/newsroom includes links to our image library, research reports and our news release archive. Sign up to get the latest news from Aviva by email.

For further information, please contact the Aviva Press Office -

Katy Hurren
katy.hurren@aviva.com
07800 692 548

Erik Nelson
erik.nelson@aviva.com
07989 427 086

References

[i] Financial Conduct Authority (FCA) | 27 Jan 2021 | FCA issues warning over 'clone firm' investment scams

[ii] Office for National Statistics (ONS) | 07 Aug 2020 | Internet access - households and individuals

[iii] Office for National Statistics (ONS) | 02 Apr 2021 | Internet users

[iv] Action Fraud | 26 May 2021 | New figures reveal victims lost over £63m to investment fraud scams on social media

[v] Gov.uk | 12 May 2021 | Draft Online Safety Bill

[vi] Financial Conduct Authority (FCA) | 11 Feb 2021 | Covid-19 pandemic leaves over a quarter of UK adults with low financial resilience

[vii] Insurance Fraud Bureau (IFB) | 30 Sep 2020 | Insurance Fraud Bureau | Industry calls on the public to help 'stop the scams' amid predicted rise in insurance fraud

[viii] Association of British Insurers (ABI) | 05 Aug 2021 |
In reverse – the cost of motor insurance falls to a five-year low according to the ABI

[ix] Financial Conduct Authority (FCA) | 27 Jan 2021 | FCA issues warning over 'clone firm' investment scams

*accurate at the time of the report