The Aviva Fraud Report

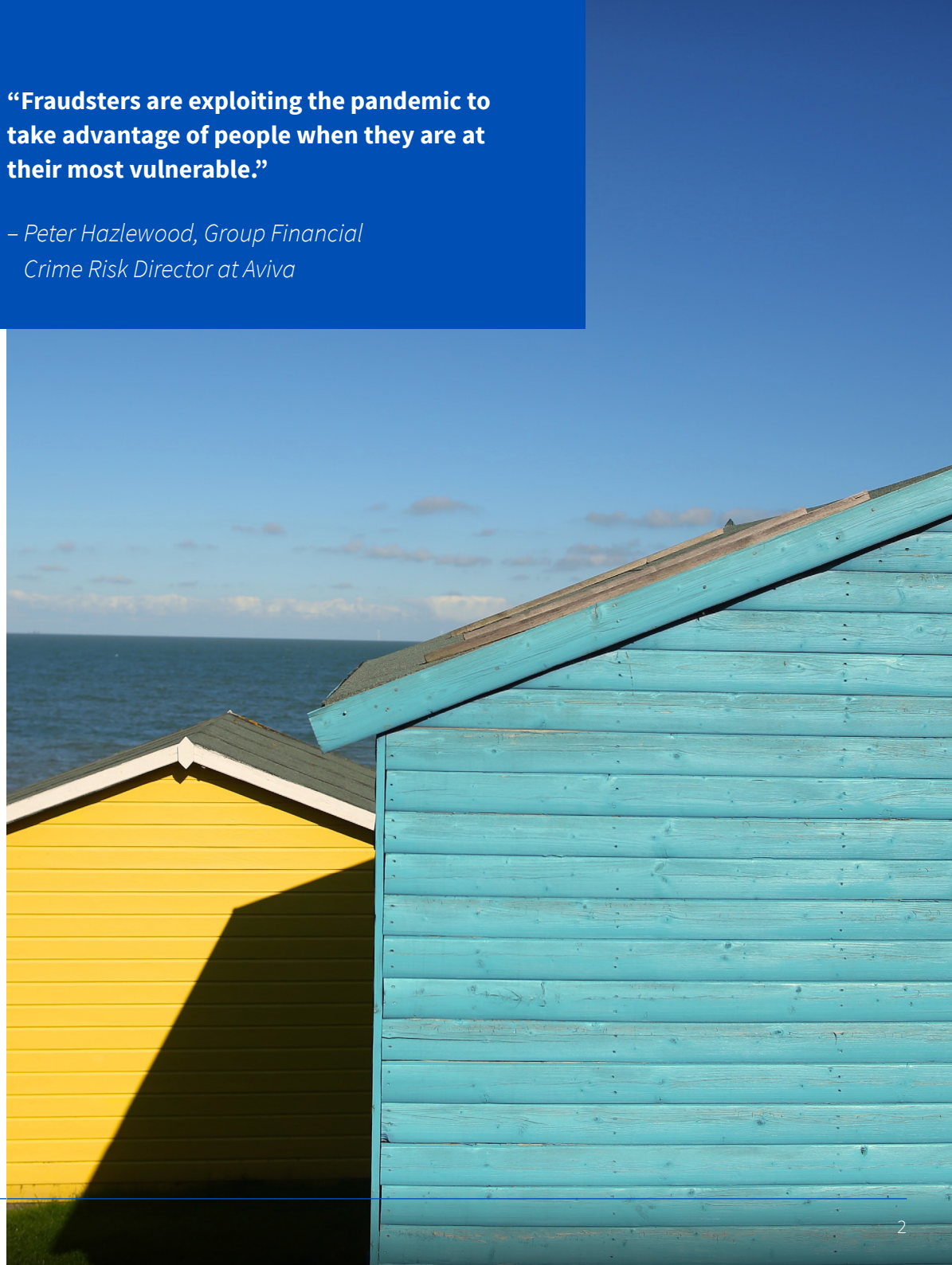
The Aviva Fraud Report uses consumer research to investigate fraud and scams which relate to pensions, savings, investments and insurance.

July 2020

Contents

"Fraudsters are exploiting the pandemic to take advantage of people when they are at their most vulnerable."

– Peter Hazlewood, Group Financial Crime Risk Director at Aviva



Welcome to the Aviva Fraud Report

Peter Hazlewood, Group Financial Crime Risk Director at Aviva

The coronavirus pandemic has raised the threat level of fraud and scams.

Action Fraud, the UK's national reporting centre for fraud and cybercrime, reported a 400% increase in coronavirus-related fraud reports from February to March[1].

While the types of financial scams are generally the same as those before the pandemic, fraudsters are exploiting the pandemic to take advantage of people when they are at their most vulnerable. They are using coronavirus as a pretext to lure potential victims. The scams range from attempts to sell people unsuitable insurance to, at worst, stealing their entire retirement savings. The impact on victims is not just financial either, it has a detrimental effect on people's mental wellbeing too.

In this, the first Aviva Fraud Report, our research has found 1 in 5 (22%) report having been targeted by suspicious communications (e.g. emails, texts and phone calls) which mentioned coronavirus – which equates to 11.7 million people in the UK[2]. Almost half (46%) of those who received a communication that they suspected to be a financial scam didn't report it. The most common (41%) reason being that they didn't know who to report it to.

The tactics deployed by fraudsters constantly evolve. As lockdown measures in the UK are eased, it's inevitable the fraudsters' tactics will again develop beyond coronavirus. Within this report we look at the most common scams at this moment in time and the criminals behind them.

It's more important than ever that people report any suspicious communication to Action Fraud, their financial services provider or the Police. When surveyed, 4 in 5 (78%) victims of a scam told us the fraudsters pretended to be from a company they already deal with. The best chance we have of catching these criminals is through better information sharing.

We launched our online fraud information and reporting service at the height of the pandemic to help protect the public and our customers from financial scams.

We firmly believe that it's more important than ever that the financial services industry works together with the authorities to support each other in protecting the public and our customers.

The victims of fraud

These are based on real case studies of people who have been affected by financial crime which have been anonymised to protect the individual's identity. Just over a quarter (26%) of all people said they would be would be embarrassed to admit being the victim of scam, whether to friends and family or the authorities.

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 wasn't able to 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.

4 in 5 (78%) victims of a coronavirus-related fraud said the fraudster pretended to be from a company they already deal with

As a result of reports into our online fraud reporting service, we have been able to identify a trend in fake savings bond websites purporting to be Aviva. We acted quickly, identifying the fraudulent domain names and publishing these to the fraud hub on our website as a warning to people.

I was diagnosed with cancer and then realised I'd been misled

Out of the blue, I had a call from a person who wanted to talk about my life insurance. I assumed that he was from my existing insurer, or calling on their behalf. He talked about reviewing my current policy, and its cost to me. We discussed the life and critical illness insurance I currently had. He said he was able to offer exactly the same cover for a lot lower premium. I thought this sounded like a great deal, and agreed to go ahead. I gave my bank details for premium-collections at the lower-price to start there-and-then, and that afternoon received my new documents.

A few months later I had some devasting news from my doctor. I had cancer. The one reassurance I had at this time was knowing I had cancer cover. We called my insurer, Aviva, to tell them the news. However, I was completely taken aback to hear that when I had switched policies, I had lost the cover conditions that I could claim under.

I explained to Aviva about the call I'd received, and how I believed that it was them that had offered to simply reduce my premium for the same cover.

Aviva confirmed that they don't make any calls such as that, or allow anybody to do so, and I realised that I'd been misled by the caller. Thinking back to the call, I realise now that I'd had to provide a lot of information that the caller would already have known if he was really from Aviva. Fortunately me for, Aviva made a goodwill decision to pay my claim.

Spotlight on: Covid-19 fraud

Key findings

- 1 in 5 (22%) report having received emails, texts, phone calls and other communications that mentioned coronavirus and which they suspected to be a financial scam – which equates to around 11.7 million people in the UK.
- Almost half (46%) of those who received a communication that they suspected to be a financial scam didn't report it. The most common (41%) reason given was they didn't know who to report it to.
- 1 in 12 (8%) have been the victim of a financial scam which related to coronavirus. 4 in 5 (78%) victims said the fraudsters pretended to be from a company they already deal with and 41% said the experience negatively affected their mental health.

Fraudsters exploit covid-19 fears – increase in suspicious communications since pandemic

If further evidence were needed to expose the unscrupulous nature of these fraudsters and how they prey on people's fears, the research shows that suspicious communications, such as emails, texts and phone calls etc. which relate to health insurance increased by 15 percentage points since the pandemic. Suspicious investment-linked communications were the second most common since the pandemic. There were also increases in suspicious life insurance (10%) car insurance (7%), pension (3%) and annuity (2%) linked communications.

% of people who reported receiving suspicious communications

Financial services product	01 Jan 2019 – 29 Feb 2020 (before covid-19)	01 Mar – 15 Jun 2020 (during covid-19)
Health insurance	11%	27%
Investment	25%	25%
Life insurance	14%	24%
Car insurance	14%	20%
Pension	13%	16%
Annuity	6%	8%

Fraudsters bank on people not reporting suspicious coronavirus communications

During the pandemic, many more people are at home and, for some, with more time on their hands to spend using a laptop or mobile phone. **1 in 5 (22%) report having been targeted by suspicious communications (e.g. emails, texts and phone calls) which mentioned coronavirus – which equates to 11.7 million people in the UK.** The elderly and vulnerable, in particular, might not have family around to check these communications are legitimate.

While the types of financial scams are generally the same as those before the pandemic, fraudsters are exploiting the pandemic to take advantage of people when they are at their most vulnerable. They are using coronavirus as a pretext to lure potential victims. The scams range from attempts to sell people unsuitable insurance to, at worst, stealing their entire retirement savings.

Spotlight on: Covid-19 fraud

Almost half (46%) of those who received a communication that they suspected to be a financial scam didn't report it. The most common (41%) reason given was they didn't know who to report it to. It's more important than ever that people report any suspicious communication to Action Fraud, their financial services provider or the Police. The best chance of catching these criminals is through better information sharing.

1 in 12 (8%) have been the victim of a financial scam which related to coronavirus and of those, 4 in 5 (78%) said the fraudsters pretended to be from a company they already deal with. In June this year, Action Fraud reported £5million having been lost to fraud since February[3]. However, if only half of people report suspicious communications this could be the tip of the iceberg.

Becoming a victim of a fraud does not just have the potential for financial impact. Of those people who reported losing money to covid-related a fraud, **41% said being the victim of a scam negatively affected their mental health.**

Top 5 professions most likely to have fallen victim to a scam during coronavirus pandemic:

1. Accountant **(22%)**
2. IT **(17%)**
3. Customer service **(11%)**
4. Administration **(8%)**
5. Teacher **(5%)**

Behavioural economics of fraud

Would you report an attempted burglary at your home?

Our research suggests people are putting themselves at risk of fraud by not treating it as a serious crime.

Only just over half (54%) of people who received a communication that they suspected to be a financial scam which mentioned coronavirus, reported it. This is low when you compare it to reporting other types of theft; for example, seven in ten (71%) would report an attempted burglary of their house. Arguably, people actually have more money at risk through a financial scam – for some people, it's their entire life savings.

Those people who received a communication that they suspected to be financial scam and which mentioned coronavirus, didn't report it because:

41%
they didn't know who to report it to

36%
they didn't think it would be investigated

25%
they couldn't be bothered

21%
they didn't know they should report it

9%
they thought it was legitimate at the time

Behavioural economics of fraud

Young people more embarrassed to be a victim

More than a third (35%) of young people aged 25-34 said they would be embarrassed to admit falling for a scam, which compares to only 20% of those aged 55 and over.

However, young people are more likely to report a communication which they suspected to be a financial scam and which mentioned coronavirus. Almost two-thirds (65%) of those aged 25-34 said they did report it, whereas only 43% aged 55 and over said the same.

"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. They set-up fake websites and use the names of real people working for legitimate companies."

– Peter Hazlewood, Aviva

Fraud shame

Over a quarter of all people (26%) said they would be embarrassed to admit being the victim of a financial scam, whether to friends and family or the authorities.

People in London are twice as likely as those in the East of England to be embarrassed to admit being the victim of a financial scam, whether to friends and family or the authorities.

Embarrassed to admit being the victim of a financial scam, whether to family and friends or the authorities

Most likely	
1	Greater London (37%)
2	NorthEast (35%)
3	Yorkshire and the Humber (28%)
4	Northern Ireland (27%)
5	West Midlands (26%)
6	Wales (26%)
7	North West (25%)
8	East Midlands (25%)
9	Scotland (24%)
10	South East (22%)
11	South West (22%)
12	East of England (18%)
Least likely	

The criminals behind the scams

The unscrupulous individuals and firms attempting to defraud people come in various different guises, from the individual at home on their laptop to the organised crime gangs who have contact centres set-up all over the over world.

The Gangster

- Individuals working from home who are using the hit-and-hope approach. They might make hundreds of cold-calls, emails or texts a day just to get one victim.
- They aim for small-scale financial scams, for example, making small amounts of commission from worthless insurance policies. This also provides them with the opportunity to build a relationship with a victim, and a way-in to asking for more small amounts of money.
- They are not particularly professional and they are not in it for the big pay out. They need a high number of individual victims to be able to make a regular income.

The Godfather

- A large crime syndicate running fraud networks like businesses, with the same level of professionalism and business acumen.
- They have a range of skills and expertise at hand. Whether employing website designers to build legitimate-looking fake websites to having access to stolen data.
- These gangs are in it for the big individual pay-outs. Setting up a fake website takes time and money but it's worth it to snag victims who are convinced to part with hundreds of thousands of pounds worth of life savings.
- They are not put off by taking on the big brands.
- They focus on using stolen data to build strong relationships with their victim. They also do their homework; getting the names of real people who work in legitimate organisations so if the victim checks with the firm they will say 'yes, we have an employee with that name'.
- They are skilled at manipulation. Coaching their victims as to what the a legitimate firm might say if they were to check with them. Often, victims of these scams are so taken in that they will refuse to believe they have been defrauded even when contacted by the Police.

The criminals behind the scams

To carry on successfully defrauding people, The Gangsters and The Godfathers are reliant upon:

- People posting sensitive personal data online.
- People not reporting concerns about them or their suspicious communications to the authorities or financial services providers.
- People not checking the legitimacy of a firm before going ahead and giving them money.
- Victims believing that fraudsters are unprofessional and a scam would be easy to spot.
- Behavioural psychology – the manipulation techniques are extremely sophisticated.
- Financial worries.
- Poor understanding of how scams work.

What are financial services providers doing to protect people?

Aviva launched its online fraud information and reporting service on its website at the height of the pandemic to help protect the public and our customers from financial scams. Our Financial Crime Intelligence Unit has over 170 years' combined experience in Financial Crime Intelligence. Working across several sectors and organisations including; National Crime Agency (NCA), Financial Services Authority, HMRC, Global Banking and Insurance, and the Commercial Crime Bureau of the Hong Kong Police.

The most common scams

Some legitimate companies use cold calling or social media to promote their products and services to potential customers but the problem is that criminals do this too. A genuine business may contact customers using contact details they have obtained legally. Criminals often use data which has either been stolen or simply wasn't meant to be used in this way. A common tactic used by fraudsters is to pretend to be from a well-known company or a firm which the potential victim has dealt with before. 1 in 5 (22%) report having been targeted by suspicious communications (e.g. emails, texts and phone calls) which mentioned coronavirus – which equates to 11.7 million people in the UK, and 4 in 5 (78%) of these said the fraudsters pretended to be from a company they already deal with. A simple way to verify a firm is to call them using a number displayed on their website, first checking that the website is legitimate. Aviva launched its online fraud information and reporting service on its website at the height of the pandemic to help protect the public and its customers from financial scams.

Types of scam

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 haven fallen in value and the Bank of England interest 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

Known as ghost policies, these make-believe car insurance policies are set up by fraudsters to entice consumers into buying them at an 'ultra-low price'. In 2019, we found over 4,000 instances of policy fraud that were linked to ghost policies[4]. Criminals can make these bogus products look like the real thing, even providing seemingly genuine policy documents – but they're far from it. They don't cover the customer or a third party.

How victims are targeted

Fake websites

While these often look professional, 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 more 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.

How to avoid a scam

It's more important than ever that people take steps to protect themselves against fraud; particularly online and through digital communications channels. Our research has found 1 in 5 (22%) report having received emails, texts, phone calls and other communications that mentioned coronavirus and which they suspected to be a financial scam – which equates to around 11.7 million people in the UK.

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 & 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 via Google.
- 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 & 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 and locking down privacy settings on these accounts.

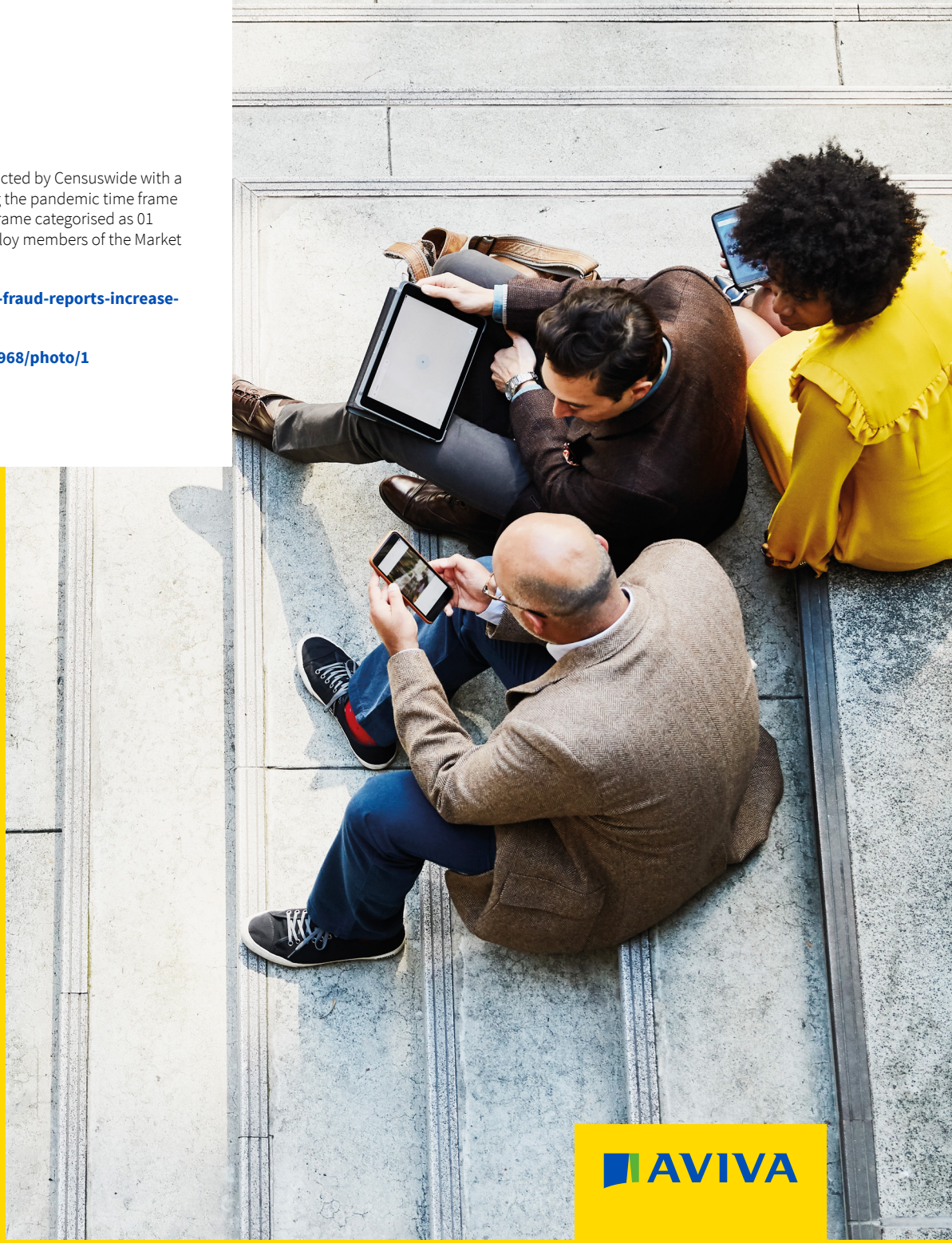
Methodology

1 All figures, unless stated otherwise, are from Aviva's research, conducted by Censuswide with a sample of 2,009 nationally representative respondents, categorising the pandemic time frame between 1 March 2020 -15 June 2020, with the pre-pandemic time frame categorised 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

2 **https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march**

3 **https://twitter.com/actionfrauduk/status/1268839575734099968/photo/1**

4 Data from Aviva's Policy Investigation Unit (PIU), 2019



About Aviva

Aviva is a leading international savings, retirement and insurance business. We exist to be with people when it really matters, throughout their lives – to help them make the most of life. We have been taking care of people for more than 320 years, in line with our purpose of being 'with you today, for a better tomorrow'.

For more details on what we do, our business and how we help our customers, visit **www.aviva.com/about-us**.

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 Katy Hurren at the Aviva Press Office:
07800 692 548 | **katy.Hurren@aviva.com**.

| Retirement | Investments | Insurance | Health |

AVIVA