COMMUNICATIONS
CONSUMER
PANEL

Scammed!
Exploited and afraid
What more can be done to protect communications consumers from the harm caused by scams?

December 2020

Contents

“I thought I was getting pretty up to speed with browsing the Internet and then I click on a link to buy some visas for a trip and the top search result turns out to be a scam and I lose £200. It’s really set me back.”

(78, Male, England)

“It’s difficult as a lot of my life was on social media – that’s how I communicated with my friends. Now I miss out on quite a lot. But I’ve become so anxious since the scam that it’s just better for me not to use social media anymore.”

(24, Female, Northern Ireland)

As the financial director, I was meant to be the responsible one and I lost £17,000 because I believed the instruction had come from my boss. I let everyone down. I was so traumatised that I couldn t talk about it and had to get counselling to cope. I didn t work again for two years.”

(54, Female, Micro-business, England)

It was a really tough time. We couldn t afford to lose the money and I was responsible for managing the household finances. It affected my family - my husband had to continue working really hard which annoyed my son because he wanted his father to stop. My husband tried not to be upset but sometimes it would spill over and we would argue. We became close to separating, it was awful.”

(62, Female, Northern Ireland)

I don t open emails from anyone I don t know. I don t answer the phone anymore unless I know the number. I ve changed all my accounts, cards, telephone number, all my personal details. It s been a long process but I feel more protected in this way.”

(50, Male, Scotland)

1. Executive summary

Fraud or 'scams' cost the UK £190 billion a year and are closely connected with other aspects of organised criminal activity[1]. In addition, a third of victims of fraud have suffered a significant emotional or psychological impact as a result. In this time of COVID-19, people around the world have become ever more reliant on communications services. The key role that these services play in people's lives has never been more evident as we hurtled into new ways of living, working and existing. Yet, at this critical time for UK consumers and micro businesses, it appears that fraudsters have taken the opportunity to increase their scamming activities and prey on vulnerable people[2],[3].

We use the terms 'fraud' and 'scam' interchangeably to describe fraudulent activity designed to harm and exploit consumers or citizens.

Anecdotal evidence has suggested that there has been an increase in scams during the last year. Our aim in commissioning this research was to:

- Understand the **types of scams** that happen via communication networks and the extent to which people are targeted and end up being scammed.
- Investigate the **circumstances** in which people are exposed to fraud and explore the reasons why people become involved.
- Determine what **actions** people take as a result of being exposed to fraud.
- Assess the **impact** that frauds and scams have, particularly on people in a vulnerable or potentially vulnerable situation, including any 'chilling effect' altering consumers' attitudes to the use of the communications services they were scammed through.

We are grateful to Citizens Advice for sharing the questionnaire used in their 2017 study[4] for benchmarking purposes.

In our research, more than 4 out of 5 of those surveyed across the UK felt confident spotting a scam - although numbers were lower when it came to spotting a scam on the internet compared to identifying one sent via email, post, text etc. A high proportion - 79% of respondents - said that they had been targeted by a scammer - with 11% of those people actually being scammed as a result. This would equate to an estimated 9% of the total population* suffering detriment from a scam across all communications channels (online, email, telephone, text and post).

[1] The Police Foundation December 2018

[2] BBC article on romance scams: https://www.bbc.co.uk/news/business-52664539

[3] Action Fraud article 'UK Finance reveals ten Covid-19 scams to be on high alert for: https://www.actionfraud.police.uk/news/uk-finance-reveals-ten-covid-19-scams-the-public-should-be-on-high-alert-for

[4] Changing the story on Scams - Citizens Advice - 2017

*Please treat this as indicative, due to small sample sizes

Online (e.g. when using a dating website, social media or shopping online) was more likely to be a source for scams targeting young people and of those scammed online, 52% were aged 16-34 years old, compared to 12% aged 55+.

70% of people scammed once or more in the past two years lost money:

- Half (51%) lost more than £100; nearly a quarter (24%) lost more than £500.
  Younger people tended to lose less money than older age groups: 62% of 16-24 year olds lost up to £100 while 67% of those aged 55+ lost more than £100.

- Overall, two thirds (68%) recouped some money, of whom three in ten (30%) recouped all of it.

- Online scams accounted for nearly a third (31%) of people losing money, however, people were scammed for higher amounts via telephone – more than a quarter (28%) scammed in this way lost more than £500.
  Both post and telephone scams saw median amounts lost of just over £300.

Amongst all online respondents who'd been scammed, 50% had reported to the Police and 24% to Action Fraud[5]. However, amongst our scammed respondents aged 55-74 interviewed by phone, only 50% of respondents had reported the offence - with 37% approaching the police and only 13% contacting Action Fraud.

Similarly, amongst those aged 75+ who were interviewed face to face, 25% had contacted the police, 15% Action Fraud and 60% had not reported it at all.

Participants who had been scammed told of the way they had been scammed and what effect the crime had had on them. Scammers had taken advantage of them using the following levers:

➢ Trust and the appearance of legitimacy on consumers with limited digital skills (mimicking the kind of communication style that they might expect, without knowing how to spot something wasn't right)

➢ Taking advantage of low confidence in technology and exploiting personal traits e.g. trusting that the scammer is genuinely there to help Clever use of technology and design with consumers who consider themselves to be in control (giving the recipient no reason to suspect a scam)

➢ Scarcity and uniqueness of a product (offering prices that are too good to be true, or a time-limited offer)

➢ Consumer impulses to realise a life-changing dream (winning the lottery)

The devastating impacts that the scams had on some of the participants' lives and businesses are told in their own words in the main research report. For some, the impact of the scam was compounded by unsympathetic treatment by their communications provider, bank, the police or another agency. Some people reported more compassionate handling of their experience but sympathetic handling needs to be backed up by proper resource and

[5] Action Fraud is the UK's national reporting centre for fraud and cyber crime

processes to build public trust. A number of participants described the ‘chilling effect’ on their future use of communications services (a hesitance to use the services that were used to scam them) and other impacts on their lives going forward.

In December 2018, the UK’s policing think tank – The Police Foundation – published a study on improving the police response to victims of fraud, acknowledging the imbalance between the scale and impact of fraud and the response it receives from policing.

The Police Foundation study asserted that most fraud cases do not result in a conviction and on average it takes 54 days between a fraud being reported to Action Fraud and a case being allocated for investigation, leading to consumer disappointment and disengagement. In addition, the report stated that there is a lack of clarity surrounding ownership of fraud investigations. The Police Foundation suggested that those responsible for fraud investigations should be required to monitor and record the outcomes of investigations in a consistent manner and seek to improve the quality of information provided by victims to Action Fraud. Furthermore, it suggested that the government should produce a national, cross-departmental strategy for tackling fraud alongside a specific national fraud policing strategy to provide greater accountability and clarity across the system. In terms of preventing fraud, the Police Foundation recommended that messaging on fraud awareness be coordinated and targeted to prevent confusion; and the government should consolidate fraud intelligence data across the public and private sectors to enable an intelligence-based prevention approach.

Our evidence strengthens the case for action - particularly in the current climate - there is no time to further delay action on scams until the UK economy has recovered from the current crisis – consumers who are already under financial pressure are being made more vulnerable by the crisis and more susceptible to scammers.

Scams are a dynamic issue, requiring collaborative, ongoing work across the communications sector and with other sectors, in order to keep a step ahead of organised criminals and opportunists.

It has become clear from our research that the fight against scams requires multi-agency collaboration. We’ve grouped our recommendations into a ‘SCAM’ model with the following aims to benefit and reassure consumers, citizens and micro businesses:

- **Security:** consumers feel that they can use communications services without being afraid of scams;
- **Clarity:** consumers can find information on scams easily; if targeted, consumers have a clear way of reporting the scam - they know who to report it to and can do so in a way that suits them;
- **Action:** consumers have a right to expect that their report of fraudulent activity will be handled compassionately, and action will be taken;

- **Monitoring:** agencies work together to measure and fix the problem and governments provide necessary regulatory and enforcement resources[6] to support this.

In our 2016 report 'Digital Footprints: a question of trust'[7], we highlighted the role that communications providers can play in helping to protect their customers from digital crime. One of our recommendations was that communications providers should provide their internet customers with a basic level of anti-virus software to all of their customers and we have been pleased to see that some providers have been providing this. But we need to do more - people have a right to be able to easily access better information if they have been scammed, find clear guidance on who to contact and receive swift support and advice to get the help they need. So we now want to build on our previous undertaking and work with other consumer bodies, regulators, enforcement agencies, scams-focused cross-sector groups and governments, to make it harder for fraudsters to attack consumers and citizens through communications services and, if they do, ensure that people can access the support they need, when they need it.

[6] The Money and Mental Health Policy Institute has come to the same conclusion following its own research - www.bbc.co.uk/news/business-55230784

[7] https://www.communicationsconsumerpanel.org.uk/downloads/communications_consumer_panel_digital_footprints-cover_report.pdf

2. Methodology

We commissioned Futuresight and also sought input from Ofcom to develop a quantitative and qualitative methodology, reflecting also on previous scams research conducted by Citizens Advice to see whether we could measure changes in the scale of the problem.

Quantitive study: a nationally representative sample of 4,492 adults was recruited, then boosted to make the sample more inclusive of people who are less likely to be online[8]:

- Main sample: n=4,038 adults aged 16+ using an online panel
- Booster sample #1: n=303 adults aged 55-74 years olds via telephone
- Booster sample #2: n=151 adults aged 75+ years old conducted face to face

Qualitative study: 46 face to face interviews were conducted, with adults who had been the victims of different types of fraud via telephone, online, email, text and post.

40 of the interviews featured consumers and 6 interviews were with owners of micro-businesses - all from across the regions and nations of the UK.

Many of the participants in the qualitative study were talking about their experiences for the first time.

3. Insights from our National and Consumer Stakeholder Hubs

The Panel holds Hub meetings across the UK, bringing together a range of stakeholders to gain insights on issues affecting consumers. While the meetings are held under 'Chatham House rules', the themes discussed in the Hubs provide useful insights which we share here with the permission of the participants:

Consumer insights:

- **Covid-19** – the pandemic has proved that anyone can suddenly find themselves in circumstances that could cause them to become vulnerable. During these vulnerable periods, we are arguably more susceptible to being targeted by a fraudster and subsequently scammed. We have heard anecdotally across our National Hubs that scams have increased during the crisis period, preying on consumers, citizens and micro-businesses at their most vulnerable.

  – initiatives developed off the back of Covid-19 are likely to be targeted by scammers. Ofcom recently published on its website advice for consumers around track and trace and the types of questions contact tracers will never ask

[8] Ofcom: "Our media literacy research suggests that the number of people who use the internet remained stable in 2019. Some 13% of adults (aged 16 or over) said they never went online, a figure that has remained broadly consistent since 2014. Older adults and DE adults were more likely to not use the internet (27% of DE adults, 30% of adults aged 65-74, and 51% of adults aged 75+). More than half (52%) of people who did not go online said that they were just not interested in doing so: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/196408/online-nation-2020-summary.pdf)

(https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/nhs-test-and-trace-scams).

- Information on tackling scams is currently fragmented and it is unclear for consumers where to find relevant information. This is likely to be particularly stressful for consumers who have recently been scammed. A cross-sectoral coordinated approach to tackling scams would help to provide clarity and consistency long-term.
- Though younger people are more susceptible to being scammed, the greatest level of harm is arguably among older people and consumers with access requirements. They are more likely to be socially isolated and, according to our research, more likely to lose significant amounts of money.
- Scams are increasing the digital divide by dissuading citizens from moving online.
- Communications Providers rely on customers to proactively find online information on fraud and scams. This is particularly difficult for consumers with low digital literacy and customers who face barriers to online access e.g. inaccessible platforms.

Research and initiatives that are currently taking place to tackle scams

- **Which?** has introduced an online scams alert that consumers can sign-up to: https://action.which.co.uk/page/s/which-scam-alerts;
- **The Payment Systems Regulator** is helping to tackle authorised push payment (APP) scams; a number of banks have signed-up to a voluntary Contingent Reimbursement Model (CRM) Code to help consumers recover money lost to scammers: https://www.psr.org.uk/psr-focus/app-scams;
- **Scottish Government** are developing a scams prevention strategy: https://www.gov.scot/
- **The Take Five Campaign** urges consumers to pause before acting, to protect themselves from scams: https://takefive-stopfraud.org.uk/
- **CMA** opened an investigation into misleading online reviews and ‘price gouging’: https://www.gov.uk/government/publications/cma-and-trade-bodies-joint-statement-against-price-gouging
- **National Trading Standards** has undertaken a call blocking project funded by DCMS and demand was high https://www.nationaltradingstandards.uk/news/free-call-blockers-for-victims-of-scam-and-nuisance-phone-calls/
- **Alzheimer’s UK** have posted a blog and postcard: https://www.alzheimers.org.uk/blog/coronavirus-covid-19-scams-people-affected-dementia
- **Niccy Youth Panel** has anecdotally seen an increase in scams targeting younger people https://www.niccy.org/about-us/youth-panel/

5. Key findings of this research

Consumers in the UK are regularly exposed to scams via the services they use to communicate and transact every day. In this study, nearly eight out of ten people (79%) had been exposed to a scam in the past two years. Exposure was highest on email (90%) and telephone (82%), with 64% of consumers exposed to scams via text and 32% via post. Just under half (47%) think they have been exposed to a scam online.

Across all channels, 11% of those people who had been exposed to a scam ended up being scammed. This equates to 4.1 - 5.3 million UK adults aged 16+ being scammed in the past two years. Amongst those who had been targeted and scammed, online accounted for the highest proportion (27%), followed by email (26%), telephone (16%), text (13%) and post (10%).

Younger age groups (16-34 year olds) were the most susceptible to being scammed and accounted for over half of all the scams experienced (52%).

- One in five (20%) of those aged 16-34 had been scammed in the past two years, compared with one in twenty-five (4%) of those aged 55+.
- 16-24 year olds were susceptible to text scams, accounting for 41% of these scams. Of those 16-24 year olds who lost money, just under two thirds (62%) lost up to £100.
- 25-34 year olds were the most likely of any age group to get scammed via telephone or online. Of those 25-34 year olds who lost money, nearly two thirds (61%) lost more than £100, and just under a third (30%) lost more than £500.

Older people, particularly, those aged 65+, were scammed by telephone predominantly and appeared to have lost considerable sums of money.

- Over half (53%) of those aged 65+ had been exposed to telephone scams more than five times in the past two years (more than twice the rate of 16-24 year olds).
- Of those aged 65+ who targeted and scammed, nearly 1 in 2 (48%) were scammed via telephone. Of those aged 65+ who lost money, seven out of ten (70%) lost more than £100, with several in the qualitative sample losing thousands and suffering serious emotional damage.

The feeling of embarrassment and shame at having fallen for a scam was a common theme throughout the qualitative interviews. Almost everyone felt it was their fault and blamed themselves. When listening to the experiences however, it was clear that that people had been drawn into co-operating with the fraudster, not because they were reckless or gullible, but because of a number of strongly influencing factors. It should also be noted that scammers' techniques are becoming increasingly sophisticated.

Respect for authority and scarcity and uniqueness of an offer were the two main factors that appeared to have the most influence. People's trusting nature, alongside respect for authority and public institutions, were common traits. These combined with low confidence in technology offered the fraudster lots of opportunity for exploitation, and they often went to great lengths to appear legitimate in order to conceal their true objective. Scarcity and uniqueness of an offer was another common factor, which fraudsters exploited using a range of tactics, the majority of which were implemented online.

Participant's confidence in their ability to spot a scam also appeared to have an influence. Across all channels, 91% of consumers were confident in spotting a scam and this feeling of being in control (i.e. a scam would never happen to them) meant their guard was often down. Levels of confidence in spotting a scam were particularly high amongst young people. These factors, in combination with the tools and techniques employed by the fraudster, were played out in various ways across the different channels.

More people (27%) were scammed online than any other channel.

- Fraudsters created bogus websites to capture people's personal details, used established auction sites to lure people with low prices and targeted individuals via social media.
- Fraudsters also created high-end websites to promote credibility and trust with people looking to invest large sums of money.
- Online accounted for the highest proportion of people losing money (31%) and over half (51%) of people scammed online were aged 16-34.

In contrast, telephone – through its high-quality one-to-one interaction – was often used for more intricate scams.

- Fraudsters would go to great lengths to pretend to be from well-known organisations.
- Older people and females were particularly susceptible to these types of scams.
- Telephone accounted for just 12% of people who lost money, but 64% lost more than £100, of whom 28% lost more than £500.

Email and text were often used by fraudsters to push messages pretending to be from well-known organisations asking participants to provide personal details.

- Younger age groups were most susceptible to scams on both these channels, although there were several cases of older people with low digital skills getting caught out too.
- 1 in 2 (50%) of those scammed on email were aged 16-34 years old and email accounted for 23% of people who lose money.
- Females and those aged 16-24 were most susceptible to text scams (often premium rate scams). Text accounted for 15% of people who lost money, with the majority (63%) losing up to £100.

Post was used for a wide range of scams, including advance fee scams, investment and inheritance fraud.

Post accounted for 10% of UK adults – 6% via post that was addressed personally, 4% via post not addressed personally.

The majority of people who had been scammed suffered financial hardship and/or had been deeply traumatised by the experience.

- The majority (70%) of people scammed lost money, but many (68%) recouped some of their money
- The financial loss had a very significant impact on the majority. This included, variously, losing some or all of their savings, having to borrow money, going into debt and not having enough money for essentials.

It was clear from the qualitative interviews that the experience of being scammed had a profound and damaging impact, emotionally and psychologically, on many participants. Participants spoke of their embarrassment at being caught out and their subsequent loss of self-belief. This was acutely felt by those who had gone to considerable lengths to comply with the fraudster's wishes. Most, however, felt angry that they had been duped and frustrated that they felt they could not do anything about it. Several were too embarrassed to talk to friends or family, leaving them feeling alone, isolated and helpless. Those who had been tricked due to the likeable, friendly nature of the fraudster talked about feeling violated and having their personal lives intruded.

The impact on participants' long-term behaviour varied from simply taking greater care to implementing major changes in their behaviour. Everyone vouched to be more careful, and some changed the way they paid for things, ensuring they had protection. However, a few had become so anxious that they took steps to reduce their exposure. This involved, variously, not picking up the phone, not answering any communications from people they did not know, no longer purchasing from websites, and, in one case, removing herself entirely from social media.

The experience of reporting the scam also appeared to have an influence on the participant's well-being. When participants felt they were being listened to and taken seriously, this appeared to help. Conversely, when the participant was made to feel that they were to blame, this compounded their sense of shame and, in some cases, put them off reporting the issue further.

Awareness of, and engagement with, supporting organisations, such as Action Fraud, would appear to be limited. There seems little evidence that people would report the incident, even if Action Fraud was known. There does not seem to be much motivation to report the scam, at least in the immediate aftermath of the scam when most people are trying to recoup their money. However, some participants, once the initial shocked had passed, were interested in sharing their experiences to try and prevent it happening to others.

Qualitative study: the emotional and financial impact of scams and what happens next

Participants who had been scammed told of the way they had been scammed and what effect the crime had had on them. Scammers had taken advantage of them using the following levers:

- Trust and the appearance of legitimacy on consumers with limited digital skills (mimicking the kind of communication style that they might expect, without knowing how to spot something wasn't right)
- Taking advantage of low confidence in technology and exploiting personal traits (trusting that the scammer is genuinely there to help 'fix the internet', as seen in our opening quote)
- Increasingly sophisticated use of technology and social media,designed to make consumers consider themselves to be in control (giving the recipient no reason to suspect a scam)
- Scarcity and uniqueness of a product (offering prices that are too good to be true, or a time-limited offer)
- Consumer impulses to realise a life-changing dream (winning the lottery)

The devastating impacts that the scams had on some of the participants' lives and businesses are told in their own words, below:

"Looking back on it, I was really annoyed that I'd fallen for it, but more so because they'd taken food off my family's table and I was effectively being reminded of what an idiot I was by the person in the bank." (24, Male, England)

"As the financial director, I was meant to be the responsible one and I lost £17,000 because I believed the instruction had come from my boss. I let everyone down. I was so traumatised that I couldn't talk about it and had to get counselling to cope. I didn't work again for two years." (54, Female, Micro-business, England)

"It was a really tough time. We couldn't afford to lose the money and I was responsible for managing the household finances. It affected my family - my husband had to continue working really hard which annoyed my son because he wanted his father to stop. My husband tried not to be upset but sometimes it would spill over and we would argue. We became close to separating, it was awful." (62, Female, Northern Ireland)

"My husband advised me to get out of it, but I was so convinced that I was helping them solve criminal activity in my local branch, that I went down to the bank and took out £5,000 and handed the money in person to a young courier at 9pm in the evening. I felt so stupid and embarrassed." (Female, 74, England)

"I had already wired them £500 to release the winnings and then they demanded another £1,000. As I went to Western Union, it didn't feel right but I thought we were nearly at a

life changing moment. It's really rocked my confidence that I fell for something so obvious." (50, Male, Scotland)

"I was devastated. I did what I thought was right and I lost the club £1,717, which was a lot of money to them. I was so ashamed and embarrassed and had no-one to turn to. It was a terrible time." (52, Female, Micro-business, England)

"I had taken out a loan to pay for the car and now I've lost the money for the car. So now I have to make monthly payments for three years to pay back the loan for a car which I don't have. It's devastating." (47, Female, Scotland)

"I had big plans to expand the business with the new piece of machinery, now I'm £10,000 down and will have to take out a loan to cover the hole. I've gone backwards several years, it's so depressing." (58, Male, micro business, England)

For some, the impact of the scam was compounded by unsympathetic treatment by their communications provider, bank, the police or another agency:

"They went about the questioning in a way that implied that I had paid this person willingly and I was now trying to defraud the bank to get the money bank. I was made to feel like a criminal. They even said that if this was the case I would be taken to court. It wasn't my fault I couldn't answer some of their questions – I was in shock that I'd been scammed." (Female, 24, Northern Ireland)

"I was made to feel very stupid. They asked me why I had handed over my details and basically said that it was my fault and there was nothing they could do. I came away feeling even worse than I already did. I thought they could have been a bit more sympathetic; I've got my mortgage with them." (Male, 24, England)

"I rang my service provider a while after it happened, thinking I have to do something. It took me an age to get through to anyone who would listen, and all I was told that it would be put on file." (53, Female, Wales)

However, some reported compassionate handling of their report:

"My mother lost £5,000 by giving her details to someone pretending to be the bank and they were very kind and gave it back to her. I couldn't believe it." (Proxy for 82 year-old, Female, Scotland)

"Losing £96 was a lot of money to me and I was very anxious and began to have panic attacks. I have diabetes and recently had a fall so I wasn't at my best anyway. Fortunately, the bank helped me out otherwise I wouldn't have been able to pay some bills." (65, Female, Wales)

"The bank was so kind – they were really supportive and after checking on what had happened, they refunded me the £96. It meant a lot as that I couldn't afford to lose that money." (65, Female, Wales)

"I was very stressed as they had my driving licence, usernames, passwords, you name it. I wanted some advice and Action Fraud was really helpful – they calmed me down and told

me what to do. It seemed like they were offering a counselling service, which was just what I needed." (42, Female, England)

Sympathetic handling needs to be backed up by proper resource and processes to build public trust:

"I reported it to the police and they were very nice and supportive, said they'd look into it. I chased them for an answer but they said they done their best and there was nothing they could do; they just didn't have the resource for these sorts of things." (74, Female, England)

"The bank knew that the criminals would be picking up the goods that day from the big electrical warehouse because they could see the stolen money had been used to make payments. So why couldn't the bank call the police and get them arrested?"   (62, Female, Northern Ireland)

"I just wanted to get my money back. I can't see what the other organisations you've mentioned are going to do to help – it just sounds like a lot of forms to fill out and nothing will get done." (47, Male, Northern Ireland)

"I didn't want to tell the police because I thought they'd just laugh at me for being   so stupid, and just tell me it was my fault and I was responsible." (54, Female,   England)

Participants described the 'chilling effect' on their future use of communications services and other impacts on their lives going forward:

"I thought I was getting pretty up to speed with browsing the Internet and then I click on a link to buy some visas a for a trip and the top search result turns out to be a scam and I lose £200. It's really set me back." (78, Male, England)

"I've tried to develop relationships in the past, but since being bullied like I was, I've changed and I'm now wary of getting involved with men. It really affected me that someone could be so manipulative and unpleasant. I get really nervous talking to men on the phone now." (Female, 40, England – romance scam)

"It's difficult as a lot of my life was on social media – that's how I communicated with my friends. Now I miss out on quite a lot. But I've become so anxious since the scam that it's just better for me not to use social media anymore." (24, Female, Northern Ireland)

I don't open emails from anyone I don't know. I don't answer the phone anymore unless I know the number. I've changed all my accounts, cards, telephone number, all my personal details. It's been a long process but I feel more protected in this way." (50, Male, Scotland).

6. Recommendations

Scams are a dynamic issue, requiring collaborative, ongoing work across the communications sector and with other sectors, in order to keep a step ahead of organised criminals and opportunists.

We've grouped our recommendations into a 'SCAM' model with the following aims to benefit and reassure consumers, citizens and micro businesses:

- **Security: consumers can to feel safe that in using communications services they will not be subject to scams;**

  Key stakeholder: Industry:

  - provide a basic level of anti-virus software for all users of their services;

  - ensure protection of personal data in line with GDPR and data protection legislation;

  - work with a wide network of organisations to identify scammers and block them from communications networks;

- **Clarity: consumers are able to find information on scams easily; if targeted, consumers have a clear way of reporting the scam - they know who to report it to and can do so in a way that suits their needs;**

  Key stakeholder: Governments:
  - consumers and citizens should receive clearer messaging on reporting of scams, who to report to and what to expect. Publishing anonymised case studies would also help to bring the issue to life, making it clear that many consumers have suffered similar experiences. This could help to combat any embarrassment or shame felt and encourage consumers to report.

  - work with regulators and industry to develop a cross-sectoral 'scams toolkit' helping consumers to locate relevant information all in one place, ensuring the information is consistent, impactful and far-reaching.

  - consider developing training for school children, using real examples of scams that have affected 16-24 year olds, so that young people recognise that this is an issue that is not confined to older or less digitally skilled people. This could be delivered alongside financial capability training, which would help young people to understand how to look after their money and which payment methods are more secure than others.

Key stakeholder: Industry:

- provide consumer safety tips such as avoiding money and bank transfers to people they do not know and using methods of payment that offer built-in protection, as demonstrated by banks.

- clearly explain processes and what consumers can expect (a Customer Charter) e.g. what happens if a customer does not pay their bill? A customer will never receive a 'bill not paid' prompt from an unrecognised mobile number. As part of this, use infographics and distribute advice across a multitude of communication channels, being cognisant of consumers who are not online.

- promote educational tools across communications services such as 'scam' quizzes e.g. 'Friends Against Scams' and 'Take Five Campaign' quizzes.

- promote digital inclusion and encourage customers to acquire digital skills to increase confidence and understanding of scams and warning signs. This is particularly relevant to Communications Providers who are moving towards digital only services.

➢ **Action: consumers have a right to expect that their report of fraudulent activity will be handled compassionately, and action will be taken:**

Key stakeholder: Governments:

- as recommended by the Police Federation in its 2018 report, Action Fraud's processes and actions should be more transparent, so that consumers receive updates and know what action has been taken;

- Action Fraud should receive the resourcing it needs to fulfil this role effectively

- Ensure that Action Fraud's communication channels for reporting are effective and inclusive and do not pose any barriers to consumers with additional access requirements, low digital literacy or a lack of access to the internet

Key stakeholder: Industry:

- recognise that victims of scams are consumers in a temporarily vulnerable situation, who may have temporarily have different needs and need more support

- develop a customer charter

➢ **Monitoring: agencies continue to work together to measure and fix the problem and governments provide necessary regulatory and enforcement resources to support this.**

Key stakeholder: Governments, regulators and industry:

- work collaboratively with consumer groups and charities, to develop a scams toolkit, as recommended above. Use this to track fraudulent activity, monitor blocking activities and evaluate the experience of those reporting scams;

- regularly share intelligence among sectors on the types of scams affecting consumers and citizens