



# COMMUNICATION NETWORKS & FRAUDULENT ACTIVITY RESEARCH

#### **REPORT OF FINDINGS**

#### **Prepared for:**

The Communications Consumer Panel Riverside House 2A Southwark Bridge Road London SE1 9HA

### Contents

1.	PRO.	JECT OVERVIEW	
	1.1	Background	2
	1.2	Research objectives	2
	1.3	Research method and sample: Overview	3
	1.4	Research report: scope and assumptions	4
2.	EXEC	CUTIVE SUMMARY	6
3.	QUA	NTITATIVE: KEY NUMBERS	10
4.	QUA	LITATIVE INSIGHT: EXPERIENCING FRAUD	
	4.1	Overview	13
	4.2	Contributing Factors	13
	4.3	Case Studies	14
<b>5</b> .	EXPE	RIENCING FRAUD: CHANNEL SPECIFICS	
	5.1	Overview	19
	5.2	Online	19
	5.3	Email	23
	5.4	Telephone	25
	5.5	Text	28
	5.6	Post	30
6.	REPO	ORTING FRAUD	
	6.1	Overview	31
	6.2	Awareness and Reporting Intent	31
	6.3	Actual Reporting Rates	32
	6.4	Experience of reporting	33
	6.5	Motivations to report	36
<b>7.</b>	THE	IMPACT OF FRAUD	
	7.1	Overview	38
	7.2	Financial impact	38
	7.3	Impact of financial loss	40
	7.4	Emotional and psychological impact	41
	7.5	Secondary Impacts	44
8	Δррі	FNDIX	47

### 1. Project Overview

#### 1.1 Background

The Communications Consumer Panel (CCP) is an independent panel of experts set up under the Communications Act 2003<sup>1</sup>. The CCP's role is to provide well-evidenced, independent advice to Ofcom, Government and the communications sector about issues faced by consumers, citizens and micro businesses across the UK. In particular, the panel is concerned with the needs of older people, people with disabilities, those living in rural areas and people on low incomes.

One of the key issues facing consumers today is exposure to fraudulent activity. The National Crime Agency puts the annual cost of fraud at £190 billion per year and cites fraud as the most commonly experienced crime in the UK<sup>2</sup>. There are clear indications that exposure to fraud and scam activity is on the rise<sup>3</sup> and that the majority of this happens via communications networks and services<sup>4</sup>. The consequences of being a victim of fraud can be very serious. The financial impacts can push consumers into debt and threaten the livelihoods of people in business. The emotional and psychological impacts can also be very damaging and long-term.

Against this background, the Communications Consumer Panel wished to investigate the scale of the problem and understand all aspects of fraudulent activity conducted over communications channels, including telephone, text, online, email and post. In particular, the CCP wished to understand the impact on consumers who have experienced fraud.

### 1.2 Research Objectives

The overarching objectives of the research were to:

- Understand the types of fraud 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.
- Assess the impact that frauds and scams have, particularly on people in a vulnerable or potentially vulnerable situation, including any 'chilling effect' on use of communication services.
- Determine what actions people take as a result of being exposed to fraud.

### 1.3 Method and Sample: Overview

<sup>&</sup>lt;sup>1</sup> https://www.communicationsconsumerpanel.org.uk/

<sup>&</sup>lt;sup>2</sup> https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

<sup>&</sup>lt;sup>3</sup> UK Finance 2019

<sup>&</sup>lt;sup>4</sup> Out of all the types of fraud reported to Action Fraud, 76% are via communications networks, of which 41% are via online and email, 20% are via telephony, and 15% are via post.

The research was conducted in two stages:

- Quantitative: to quantify people's awareness, knowledge and experience of fraud.
- Qualitative: to explore the experiences of people who have been victims of fraud.

#### Stage 1: Quantitative

We surveyed a nationally representative sample of 4,492 adults using three approaches:

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

The two booster samples were used to include people aged 55+ who may not be online or who make limited use of the Internet.

#### Stage 2: Qualitative

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

40 interviews were conducted with consumers and 6 interviews with owners of microbusinesses from across the regions and nations of the UK.

#### Achieving a balanced sample

Recruitment criteria were put in place to ensure the findings were based on a balanced mix of consumers and scams experienced. In addition to the standard variables, such as age, gender, lifestage, ethnicity and location, we also included specific sub-samples of people who were in a vulnerable or potentially vulnerable situation (e.g. limited digital skills, low income, socially isolated or something circumstantial, such as illness).

Participants also needed to have experienced fraudulent activity. This required a team of specialist individual recruiters, who had very well-established, trusted networks within their communities. Many of the participants had been left humiliated and embarrassed by their experience and these recruiters were able to provide the reassurances needed to encourage participation. Several consumers were still too traumatised by their experience and declined to take part.

Initially, participants were free found, but as recruitment progressed, quotas were set to ensure a range of scams across all the different channels were represented. The final sample included a well-balanced mix of consumers who had been exposed to different scams and had suffered in varying degrees. Many of those that did participate were talking about their experiences for the first time.

#### 1.4 Research Report: Scope and Assumptions

This report is primarily a qualitative analysis of fraudulent activity that takes place via communication channels. Our focus has been to identify the factors that can contribute to people being scammed, as well as the tactics used by fraudsters to turn these factors into weaknesses they can exploit. We have also explored the impacts of being scammed, both financially and emotionally, to show the extent of the potential harm suffered and the effect this has on their engagement with communications services.

In Section three, we have provided a summary of the key quantitative highlights. Throughout the report, we have combined quantitative and qualitative findings as appropriate. It should be noted that the report contains some discussion of results which are based on low sample sizes. In these instances, we have highlighted the low sample base<sup>5</sup> (as footnotes) and suggest these findings should be treated as indicative.

#### A note on language / definitions

Our definition of being scammed is anyone who had suffered any of the following impacts: losing money, personal details stolen or taking part in an activity unwillingly.

We have used the terms scam and fraud interchangeably throughout this report. In the past, scam has been used to denote something that is more fleeting and of less value than fraud. In this report, we have not made this distinction and apply the same meaning to both, i.e. wrongful or criminal deception intended to result in financial or personal gain.

We have used different terms for someone who has experienced fraudulent activity. We have avoided using the term 'victim', except where it has been used in other documentation. We have used the term 'target' when describing the tactics used by fraudsters, 'consumer' to refer to any member of the UK public and 'participant' when referring to anyone taking part in the research.

Finally, it should be noted that the data collection for this study took place prior to the social restrictions put in place due to Covid-19 virus. As a result, this report makes no reference to the fraudulent activity that might have taken place during the lockdown in the UK.

<sup>&</sup>lt;sup>5</sup> The total base for people who were targeted and scammed on any channel was n=404. Where the sample size falls below n=40 (i.e. 10% of the total base), we have highlighted this as a small sample size and provided details in a footnote.

### 2. Executive Summary

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 on any channel 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%) thought 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 an estimated 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<sup>6</sup>. 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%)<sup>7</sup> lost more than £500.

Older people, particularly, those aged 65+, were predominantly scammed by telephone 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 were targeted and scammed, nearly 1 in 2 (48%)<sup>8</sup> were scammed via telephone. Of those aged 65+ who lost money, seven out of ten (70%)<sup>9</sup> lost more than £100, with several in the qualitative sample losing thousands and suffering serious emotional damage.

<sup>&</sup>lt;sup>6</sup> Small sample size. Out of a total n=54 who were targeted and scammed via text, n=22 were 16-24 year olds.

<sup>&</sup>lt;sup>7</sup> Small sample size. Out of a total n=88 25-34 year olds who lost money, n=26 lost more than £500.

<sup>&</sup>lt;sup>8</sup> Small sample size. Out of a total of n=21 aged 65+ who were targeted and scammed, n=10 were scammed via telephone.

<sup>&</sup>lt;sup>9</sup> Small sample size. Out of a total of n=11 aged 65+ who lost money, n=8 lost £100+.

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.

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 (52%) 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 women were particularly susceptible to these types of scams.

• Telephone accounted for just 12% of people who lost money<sup>10</sup>, but 64% lost more than £100, of whom 28% lost more than £500<sup>11</sup>.

## 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.
- Women 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%)<sup>12</sup> 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 who were targeted and scammed – 6% via post that was addressed personally, 4% via post not addressed personally. Post also accounted for 10% of those people who lost money – 5% via post that was addressed personally, 5% via post not addressed personally<sup>13</sup>.

## 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,

<sup>&</sup>lt;sup>10</sup> Small sample size. Out of a total of n=285 who lost money, n=36 lost money via telephone.

<sup>&</sup>lt;sup>11</sup> Small sample size. Out of n=36 who lost money via telephone, n=23 lost £100+, n=10 lost £500+.

<sup>&</sup>lt;sup>12</sup> Small sample size. Out of a total of n=42 who lost money via text, n=26 lost up to £100.

<sup>&</sup>lt;sup>13</sup> Small sample size. Out of a total of n=285 who lost money, n=29 lost money via post (n=16 addressed personally, n=13 not addressed personally.

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, 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.

### 3. Quantitative Results: Summary

For benchmarking purposes, the questionnaire used was based on a similar survey conducted by Citizens Advice in 2017<sup>14</sup>. We have included the results from the Citizens Advice survey alongside the results from this project, where possible.

The vast majority of UK adults had confidence in identifying a scam on any channel.

**% Consumers who are confident in identifying a scam** (Q2. To what extent are you confident or not that you would be able to identify a scam if you came across one?

Net Confident (i.e. all those	Channel	ССР	Citizens Advice
who	Online	86%	81%
responded fairly and very	Email	93%	85%
confident	Text	92%	87%
Bases:	Telephone	92%	88%
CCP (n=4,478) CA (n=3,062)	Post (addressed personally)	90%	88%
Cr (ii 3/662)	Post (not addressed personally)	93%	87%
	Someone coming to your door	89%	86%

Nearly 8 out of 10 UK adults (79%) have been targeted by a scam on any channel in the past 2 years. Of those who have been targeted in the past two years, over 1 in 10 (11%) were scammed.

	ССР		Total Population	Citizens Advice	
	Targeted Scammed		Scammed	Targeted	Scammed
	Base: all (n=4,478)	Base: all targeted (n=3,525)	(% targeted x % scammed)	Base: all (n=3,062)	Base: all targeted (n=2,205)
All 79% 11% Channels		11%	9%	72%	14%

**% Consumers Targeted and Scammed** (Q5. In the last two years, have you received anything or been contacted by anyone that was trying to scam you? This could include any form of contact, including by telephone, text, email, letter, mailshot or someone coming to your door? Q8. On this last occasion, which of the following occurred (I lost money, my personal details were taken, I ended up taking part in an activity I did not want to do/later regretted?

\_

<sup>&</sup>lt;sup>14</sup> Changing the story on Scams - Citizens Advice - 2017

Of those people who had been targeted on any channel . . .

- Just under half thought they had been targeted online (47%), yet online accounted for the largest proportion of UK adults being scammed (27%)
- 9 out of 10 people thought they had been targeted by email, with just over a quarter (26%) being scammed.

	C	<b>Total Population</b>	
Channel	Targeted Base: all targeted (n=3,525)	Scammed  Base: all targeted and scammed (n=404)	Scammed (% targeted x % scammed)
Online	47%	27%	13%
Email	90%	26%	23%
Text	64%	13%	8%
Telephone	82%	16%	13%
Post (personal)	36%	6%	2%
Post (not personal)	28%	4%	1%
Coming to your door	27%	7%	2%

**% Consumers Targeted and Scammed** (Q5. In the last two years, have you received anything or been contacted by anyone that was trying to scam you? This could include any form of contact, including by telephone, text, email, letter, mailshot or someone coming to your door? Q8. On this last occasion, which of the following occurred (I lost money, my personal details were taken, I ended up taking part in an activity I did not want to do/later regretted? Q9: And on that last occasion, in which of the following ways was this aimed at you? (online, email, text, phone, post)

#### **Financial Impact:**

[Base: all scammed who lost money n=285]

### 7 out of 10 (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
  - o 62% of 16-24 year olds lost up to £100
  - 67% of those aged 55+ lost more than £100<sup>15</sup>
- Overall, two thirds (68%) recouped some money, of whom three in ten (30%) recouped all of it.

 $<sup>^{15}</sup>$  Small sample size. Out of a total of n=24 aged 55+, n=16 lost more than £100.

Online accounted for nearly a third (31%) of people losing money, however, people were scammed for higher amounts via telephone – more than a quarter (28%) lost more than £500<sup>16</sup>.

Channel	££ lost (median)	% Proportion of people losing money	+/- £100 lost (%)
Online (n=89)	£76	31%	60% lost up to £100
Email (n=65)	£76	23%	50% lost more than £100 <sup>17</sup>
Telephone (n=36)	£301	13%	64% lost more than £100 <sup>18</sup>
Text (n=42)	£76	15%	63% lost up to £100 <sup>19</sup>
Post (n=29)	£301	10%	51% lost up to £100 <sup>20</sup>
Someone coming to your door	£301	7%	52% lost more than £100 <sup>21</sup>

 $<sup>^{16}</sup>$  Small sample size. Out of a total of n=36 who lost money via telephone, n=10 lost £500+.  $^{17}$  Small sample size. Out of a total of n=65 who lost money via email, n=32 lost £100+.

<sup>&</sup>lt;sup>18</sup> Small sample size. Out of a total of n=36 who lost money via telephone, n=23 lost £100+.

Small sample size. Out of a total of n=42 who lost money via text, n=26 lost up to £100.
 Small sample size. Out of a total of n=29 who lost money via post, n=15 lost up to £100.
 Small sample size. Out of a total of n=21 who lost money via someone coming to their door, n=11 lost £100+.

### 4. Qualitative Insight: Experiencing Fraud

#### 4.1 Overview

In almost all the qualitative interviews, participants had to co-operate with the fraudster for the scam to succeed. In some cases, the co-operation was very minimal, but in most cases, participants co-operated willingly, with some going to extreme lengths to comply with the fraudster's wishes.

Participants engaged with the fraudster for a variety of reasons. Some were motivated by the offer, others believed they were helping to solve a problem and a few did what they were told because they lacked the confidence or knowledge to question.

Fraudsters, on the other hand, would seek to exploit these vulnerabilities and win over the participant by employing various tools and techniques.

It was the combination of these motivating factors and techniques that encouraged rational participants to engage in activities that would lead to harm.

#### 4.2 Experiencing Fraud: Contributing Factors

Throughout many of the interviews, participants expressed a deep sense of shame and embarrassment at being caught out. In their mind, it was their fault that they had got scammed. However, it was clear from the experiences described that it was a combination of factors – on the part of the participant and the fraudster - that had led to them to being scammed.

In almost all the interviews, participants needed to co-operate with the fraudster and the fraudster needed to persuade the participant to buy into the scam.

When describing their experiences, participants appeared to co-operate because of various triggers that encouraged them to believe the scam was genuine. These included, variously:

- A trusting nature and respect for authority, in particular public service institutions
- Scarcity and uniqueness of the offer (i.e. the drive not to miss out)
- Confidence in their judgement and a belief that they were in control
- Responding positively to those who reflected their own attitudes and beliefs
- The stimulus of a big prize and the reassurance of recommendations
- Identifying coincidences and seeing these as supporting evidence for the communication

In addition, vulnerabilities, such as digital literacy, cognitive impairment and social isolation, as well as circumstantial factors, such as illness, appeared to contribute in some cases.

On the fraudster's side, a variety of tools and techniques were employed to exploit the above triggers. Adopting a professional and legitimate appearance, clever use of technology and good sales techniques were common to many scams. In addition, fraudsters would adopt other approaches, depending on the channel and scam, such as taking small amounts of money or engaging in identity fraud. In a minority of cases, they would use pressure and coercion.

The following case studies illustrate some of the different combinations of these factors – on the side of the participant and the fraudster – that led to an individual getting scammed. Additional examples of other combinations, relating to individual channels, can be found in Chapter 5.

#### 4.3 Experiencing Fraud: Case Studies

## Leveraging trust and the appearance of legitimacy on consumers with limited digital skills and low confidence

A common scam was when a fraudster took advantage of a participant's trust in public institutions, limited digital skills and low confidence in technology or administrative functions. The fraudster would set up the legitimate appearance carefully and then use their interpersonal skills to coerce the participant into complying. Often, the participant would comply because they thought they were helping solve a problem.

#### Case study #1: Female, 43, Rural, Micro-business owner, Northern Ireland

Harriet runs a farm, has a basic mobile phone, a landline and describes herself as not technical and lacking confidence. She received a call on the landline from HSBC saying they had noticed someone had tried to access her business account. She was a bit surprised but thought it was perhaps a cheque she had used the week before. The man said she should call another number to stop any further action, which she did. A different person took her through various steps, including handing over her bank details, password, PIN and the code from the HSBC key fob. Throughout the call, Harriet thought this man was trying to help her resolve a problem. A few days later, she saw that two payments had gone out of her account — one for £5,000 and one for £12,000. She called the police, who gave her a crime number, and then her bank, who said they could not help as she had authorised the payments. Harriet was deeply traumatised once she realised the extent of the scam. She suffered personal financial difficulties, but the farm was able to support the loss.

Often the fraudsters would go to extensive lengths to reassure the participant of the legitimacy of the scam, which, in turn, would help to hide the actual objectives. In one case, involving a team of fraudsters pretending to be from different reputable organisations (Scotland Yard, Visa Fraud, the Bank), the extent of the illusion created was so powerful that the participant, a lady aged 74, was persuaded, against the advice of her husband, to get in her car, go to the bank, take out £5,000 and hand the money to a courier at eight o'clock in the evening.

#### Taking advantage of low confidence in technology and exploiting personal traits

Many of the more intricate deceptions took place over the telephone as this channel allowed the fraudster to develop rapport and adapt their approach to exploit each participant's specific vulnerabilities. These could include low confidence in technology and a trusting nature, but also personal characteristics, such as anxiety and a protective personality, which the fraudster exploited by pretending to support and help.

#### Case study #2: Female, 53, Urban, Wales

Jo is married and has three children in their late teens and 20s. She is a department head at a university. She is not very digitally confident and can get anxious about finances. She received a call on the landline at 8am on Saturday morning. The rest of the family were asleep and the man said he was calling from BT and the internet in the area had been compromised. He was calm, friendly and very reassuring as Jo had started to get panicked that their details had been stolen. He said he would take her through various steps to work out what details had been taken and then fix everything. Forty minutes later she was still on the phone and very stressed, seeing lines of code on her laptop. Her son came down and she told him what had been going on. He said it was a scam and put the phone down for her. Jo could not believe what had happened. She had been in the comfort of her home and her world had been turned upside down. She felt violated and angry at the terrible irony that, whilst she was trying to protect the family, all she had done was invite harm. She also was upset that she had believed the caller and had to be rescued by her son. She felt like a child when she was meant to be the responsible adult. She reported the incident to her provider, but they said there was nothing they could do. Two years on and she is still deeply traumatised by the event.

### Leveraging legitimate appearance and clever use of technology with consumers who consider themselves to be in control.

Other examples of professional appearance scams simply made clever use of technology. Masking telephone numbers – either via telephone or text - to appear to come from a legitimate business supported the deception, particularly with participants who felt confident in their ability to spot a scam. This sense of being in control appeared to be a contributing factor in several scams, particularly amongst younger, more technically savvy participants. They would engage without applying the necessary checks, thinking a scam would never happen to them.

Fraudsters also made clever use of technology via email, tricking people into making payments that were bogus and had not been authorised. Two highly organised and responsible participants, working in administrative roles within organisations, were tricked by this technique, both with devastating consequences.

#### Case study #3: Nicky, Female, 52, Semi-Rural, Micro-business, England

Nicky works as a sole trader in her role as the treasurer for a sports club. She describes herself as diligent, organised, efficient and responsive. Her boss is the Chairman of the club and she has worked for him for many years. Nicky got an email from her boss asking her to pay £1,717 to a bank account. The email came from her boss' email account and it was written in the same tone that her boss used. Nicky, being efficient and responsive, made the payment immediately and confirmed she had done this. The Chairman questioned what she had done and she realised she had been tricked. She immediately called the bank to stop the payment but they made it clear that it was not their responsibility and it was her fault. Nicky was devastated. She felt stupid and thought she had let everyone down. She lost her confidence and believed her boss no longer trusted her. She didn't report it to the Police for fear that she would be treated as an idiot. She found it difficult to talk about the experience.

## Leveraging scarcity and uniqueness of a product; offering prices that are too good to be true.

Amongst the interviews, there were several examples of scams where fraudsters had offered products on established sites at prices that were set well below expectations. Participants were drawn to the price and, in many cases, the bargain overshadowed their judgement. Once the fraudster had drawn them into the scam, participants appeared to justify their commitment and went along with the scam, even though they had their suspicions.

#### Case study #4: Female, 48, Rural, England

Denise is a vet and wanted to buy a pedigree ewe. She saw an ad for a very good quality ewe on an online marketplace she had used before. The ewe would normally cost £3,000 but this one was being advertised for £900. It sounded too good to be true but she made enquiries. Denise started to become a little

Other participants had been lured into a scam by a good price and then persuaded to make payment outside established payment systems in return for a further price reduction. This scam was particularly common for lower value items, such as electronics, mobile devices and concert tickets. In the example below, the fraudster enhanced the credibility of the scam by pretending to be someone like the participant.

#### Case study #6: Tyrell, Male, 19, Urban, England

Tyrell needed a new phone fast and went on eBay. He saw a phone that was easily the best value (condition and price). He messaged the seller, who offered him a deal - a reduction from £180 to £150 if he deposited £50 via BACS, rather than full payment via PayPal. The seller gave the story that he was a student and couldn't afford to send the phone by recorded delivery (c.£20). This seemed plausible to Tyrell, as lots of his friends are students and have no money. Tyrell sent the money. Later that day, he checked eBay and saw that the seller had taken down his page. When he realised his money was gone, he reported it to PayPal and went through the process of reclaiming the £100, which he got back.

#### Leveraging consumer impulses to realise their dream

For some participants, the dream of something life-changing overshadowed their judgement and they made an impulsive decision, which backfired, often with very damaging consequences. In some cases, the participants had gone to great lengths to confirm the legitimacy of the offer and this was the prompt which led to the error of judgement.

#### Case study #7: David, 58, Male, Semi-Rural, Micro-business, England

David owns a micro-business operating a mechanical digger. He saw an advert for a digger in Auto Trader which he thought would really move his business forward. He made enquiries via email. The fraudster replied and set out the price and payment terms. After checking the supplier on Companies House, David agreed to pay £10,000 in return for delivery of the excavator to his home. He went ahead and

In other cases, participants had a strong suspicion that something was not quite right, but the lure of something life changing was too strong to resist. In the case below, the fraudster used pressure and coercion to extract more money.

#### Case study #7: Jim, 50, Urban, Scotland

Jim is living with HIV and financially vulnerable. Jim and his partner had been to the US and bought some lottery tickets. When they returned, they received an email saying they had won. Excited, they gave their address and phone number on the email. They got a call saying they had to wire £350 – to pay for the tax on the winnings. Jim thought this was sensible and wired the money. They then started receiving phone calls saying they need to wire another £1,500. The phone calls were at different times of the day and night. Jim was getting stressed. In the end, they agreed to wire the money. Just as he wired the money, he thought it was a scam and tried to stop the transfer. The cashier said there was nothing she could do. Jim reported it to the police in Glasgow but they couldn't help. Jim was devastated, describing the experience as 'horrendous and harrowing'. He felt stupid and angry. He had to change bank accounts, cards, telephone number and his social benefit details. He no longer trusts anyone – he doesn't open emails and doesn't answer his phone to anyone he doesn't know.

### 5. Experience of Fraud: Channel Specifics

#### 5.1 Overview

The types of scams experienced varied across the different channels. Some approaches, such as legitimate appearance, were applied across all channels, albeit in slightly different ways. A legitimate appearance scam over the telephone was likely to be more intricate and complex, compared with a similar type of scam applied via text or email. Scarcity and uniqueness of an offer was often applied online as this channel offered lots of opportunities for this approach via bogus websites and auction sites. Some scams, such as premium rate texts, were particular to a channel. Overall, participants engaged with channels in different ways and the fraudster adapted their approaches to reflect these differences in order to maximise the opportunities for exploitation.

#### **5.2** Online (e.g. when using a dating website, social media or shopping online)

Incidence Rates	Of those targeted, 47% thought they had been targeted online in the past 2 years. Of those scammed, 27% were scammed online on the last occasion.
Demographic Differences	<ul> <li>Younger age groups (aged 16-34).</li> <li>60% of 16-34 year olds thought they had been targeted</li> <li>Of all those scammed online, 52% were aged 16-34 years old (compared to 12% aged 55+)<sup>22</sup>.</li> </ul>
Money Lost	Median £76  Online accounted for 31% of people who were scammed and lost money  Of those scammed and losing money online, 60% lost up to £100.

## A wide variety of scams were experienced online, including bogus websites, auction scams, investment fraud and romance scams

In this study, the most common scams experienced online involved bogus websites that were designed to replicate well-known organisations and capture a participant's

<sup>&</sup>lt;sup>22</sup> Small sample size. Out of a total of n=109 who were scammed online, n=13 were aged 55+

personal details. Fraudsters also used websites to sell products that either did not exist or acted as proxies for capturing personal details (e.g. health scams offering samples). Scams via auction sites were also common where fraudsters tempted participants with out of stock or rare products at bargain prices. These were relatively low-cost strategies that could reach a very wide audience.

At the other extreme, fraudsters invested in high quality websites in order to promote trust and the illusion of an established and legitimate business. Investment scams, where participants were encouraged to buy shares in companies that did not exist, made use of this approach. Social media platforms were also exploited by fraudsters for romance scams. Fraudsters would identify their target and then develop a relationship in order to extract money.

## More people end up being scammed online than any other channel. Younger people were more likely to get scammed online than older age groups.

Over half (52%) of people scammed online were aged 16-34. One contributing factor to younger people being scammed appears to be the high levels of confidence they have in spotting a scam online – 40% of those aged 16-34 were very confident in spotting a scam. This sense of confidence, and care-free attitude to giving out personal details online, contributed to the participant getting scammed in the example below.

#### Case study #8: Lorna, 24, Female, Northern Ireland

Lorna is single and works as a community support officer. She likes testing out health products and has signed up for samples before, giving out her bank details. She saw an ad for some vitamins whilst browsing, clicked on the link, inputted her details and also signed up some of her friends. The samples never arrived. She got a call from her bank a few months later asking her about some irregular payments that had been coming out of her account. She realised that small payments had been taken out of her account over the past 5 months. Lorna was in shock and concerned that more money would be taken out, which she couldn't afford. She spoke to the bank's fraud department. They asked her a lot of questions and she felt that the bank was accusing her of trying to defraud them. They told her that she could go to court if that was the case. She was very stressed and upset that she was treated like a criminal. They did not refund any of the money and she didn't think of reporting it elsewhere in case she got the same treatment. She has since completely changed her behaviour and will only purchase online from reputable sites using PayPal. She became very concerned about having any personal details online and has taken herself off social media completely. This has had a big impact on her social life but the experience 'hit her hard'.

#### Auction platforms are attractive to scammers because they can take advantage of the features that are in place to support consumers.

Fraudsters can set up fake accounts with fake reviews to reassure people of their legitimacy. They can also promote products that they know are in short supply and offer cut down prices to attract people. The price is then further reduced in exchange for payment outside of the standard payment platforms.

#### Case study #9: Pauline, 47, Female, Urban, Scotland

Pauline is single, works as a legal secretary and considers herself to be confident with technology and highly organised. Pauline found a car she wanted on eBay and made contact with the seller. She did all the background checks with the DVLA and was really excited that she had found the car she wanted. She was then asked to send the payment via BACS as they didn't use PayPal. She was advised against doing this by her uncle but, convinced everything was fine, she sent £4,500 via BACS. The ad and eBay account were taken down immediately and the money disappeared. She reported it to the Police and Action Fraud, but heard nothing back. Pauline was devastated and very stressed about her finances. She had taken out a loan to pay for the car and now she was liable for the repayments and still needed a car. She was angry with herself for not using PayPal and has since lost a

Social media platforms contain a lot of personal information, which the fraudster can mine and use to develop relationships in order to defraud them, as illustrated in the example below.

#### Case study #10: Christina, 40, Female, Rural, England

Christina lives on her own and describes herself as socially isolated. She wanted to find a partner and has spent a lot of time on various social media platforms to find someone suitable. She received a message from a solider in Nigeria, who shared his profile and they started chatting. She was enamoured by his looks, charm and wit and become more involved. He said he had been injured and needed money for supplies. She found the situation very believable and initially sent £50, which escalated to a total of £700. Requests for money persisted over several months which she didn't like, and then he disappeared. Christina realised she had been manipulated and felt scared, lost and foolish. The experience affected her very deeply and she felt she couldn't trust men in the same way again. She declined to do the interview face to face and was audibly upset over the telephone. Christina

## The Internet also offers opportunities for fraudsters to promote themselves as professional and legitimate, and play on people's vulnerability to trust too easily.

In some cases, particularly high-end investment fraud, a lot of time, money and resources can be invested into creating the illusion, with high end websites, glossy brochures and slick sales teams. In these cases, online is often a supporting tool to attract people in before the hard sell is made over the phone.

#### Case study #11: Eva, 59, Female, Urban, Scotland

Eva is single and works for a charity. She describes herself as considered and careful. She received an endowment and wanted invest the money for her retirement. She looked around on the internet and found a company that looked very established with property investments all over the world. They had a very smart website and she received very professional looking brochures in the post. They were also offering sensible returns, nothing over the top. She had lots of conversations with someone who sounded very professional and genuine and invested £10,000. For the first 6 months, everything seemed fine, then she received notice that the firm was going into insolvency. A year later, she received a call from another investment business and she was convinced to make another investment of £10,000. A few months later, she received letters that this company had also gone into liquidation. Eva didn't know where to go. She started with the financial ombudsman, then the FCA, and was passed from pillar to post. She found none of them very helpful and resigned herself to losing all the money. She was devastated that she could have been so gullible. The experience damaged her health so she had to take time off work. She also lost confidence, as she had done a lot of research and trusted her own instincts. She felt very isolated and victimised, particularly when she realised she had been scammed for a second time. She has since received notice from the Police that an investigation has started, but she does not hold out any hope of retrieving any money.

#### 5.3 Email

Incidence Rates	Of those targeted, 90% thought they had been targeted once or more in the past two years via email. 52% were targeted 5 times or more in the last 2 years. Of those scammed, 26% were scammed via email on the last occasion.		
Demographic Differences	No particular segment affected.		
Money Lost	Median £76  Email accounted for 23% of people who lose money.  50% lost more than £100; 29% lost £101-£500 <sup>23</sup>		

Email has become the default service for business type communications and fraudsters exploit this by pushing fraudulent messages that appear to be from well-known organisations.

The effectiveness of email as a channel for scams would appear to be related to how this service is used. These might include communications from utilities, banks, HMRC, as well as from private companies, confirming purchases and offering tracking details. Fraudsters look to take advantage of people's trusting nature and set traps for those with limited digital skills and awareness.

Confidence levels in spotting a scam on email were high – more than nine out ten people (93%) were confident, with just under half (46%) saying they were very confident. It seems that people get a lot of unsolicited emails and awareness of this channel for potential scams was fairly widespread. However, confidence levels in spotting a scam would be to be somewhat illusory for some, with over a quarter of those targeted on email ending up being scammed (26%).

Emails pretending to be from public services or businesses asking for personal details were the most common examples of email scams. These communications were often well designed and personally addressed to the individual.

#### Case study #12: Dawn, 75, Female, Urban, England

Dawn is married and a pensioner. She is not very technically literate but she has sample size. Out of a total n=65 who lost money via email, n=32 lost £100+, n=19 lost £101-£500. email on her phone and likes to have a go on the competitions at Tesco sometimes. She gives her email address in case she wins. She received an email one day, which said she had won £500 and she needed to provide her bank details to receive the money. She clicked on the link of the email, inputted her bank details and, about a week later looked in her account to see if the money had arrived. She saw that

Email was also used for push payment fraud, where the fraudster sends a message pretending to be from a legitimate company and asking for payment to be made.

In our business sample, two participants had been scammed in this way. Both had responded to what they thought were messages from their boss to make payments. In both cases, the fraudster had carefully created the message to replicate the style and tone of the participant's boss. The impact of the scam was particularly damaging in both cases.

#### Case study #13: Mary, 54, Urban, Micro-business, England

Mary worked as a financial director in a communications agency. She had been there several years and was on the board. She received an email from the Chief Executive asking her to pay £17,000 to a company. The email was identical to the emails she usually received from him – in language, look and tone. She made the transfer and confirmed with the CEO, who knew nothing about it. She contacted the bank but they were unable to help as she had authorised the payment. She was devastated. She felt she had let herself and the company down. She didn't know where to turn to and felt very isolated. She was so traumatised by the experience that she took a year out of work and went to counselling for help.

Email was also be used to exploit consumers through pressure & coercion. Several participants mentioned that they had received emails, accusing them of accessing illegal or inappropriate content, and to avoid this information being shared with their contacts or the police, the fraudster wanted payment.

### 5.4 Telephone

Incidence Rates	Of those targeted, 82% thought they had been targeted via telephone once or more over the past two years. Of those scammed, 16% were scammed via telephone on the last occasion.
Demographic	Women and older age groups (65+)
Differences	Of those scammed, more than two thirds (69%) were women, compared with less than a third of males (31%) <sup>24</sup> . Amongst all those aged 65+ who were targeted and scammed, nearly 1 in 2 (48%) <sup>25</sup> were scammed via telephone.
Money Lost	Median amount lost was £301. Telephone accounted for 13% of people who lost money. Of those who were scammed and lost money, nearly two thirds (64%) lost more than £100, 28% lost more than £500 <sup>26</sup> .

#### Telephone, through its high quality one to one interaction, offers the fraudster the opportunity to develop rapport and create trust quickly.

The majority of scams via telephone in this study involved fraudsters creating the appearance of legitimacy. They often went to great lengths to enhance this illusion. Many of the scams experienced involved complex set ups, often with several fraudsters working together.

More than twice as many women (69%) compared to men (31%) were scammed via telephone. It is not clear from the survey results why this is. Telephone accounts for just under half of the scams (48%)<sup>27</sup> experienced by those aged 65+.

Across all age groups, of those targeted, 82% thought they had been targeted via telephone, with 16% ending up being scammed. In the booster surveys, the incidence rates of being targeted and scammed were higher.

• In the telephone survey, over half (54%)<sup>28</sup> of those aged 55+ who had been targeted were scammed via telephone.

<sup>&</sup>lt;sup>24</sup> Small sample size. Out of a total of n=63 who were scammed via telephone, n=20 were male.

<sup>&</sup>lt;sup>25</sup> Small sample size. Out of a total of n=21 aged 65+ who were scammed, n=10 were scammed via telephone.

<sup>&</sup>lt;sup>26</sup> Small sample size. Out of a total of n=36 who lost money via telephone, n=23 lost £100+, n=10 lost £500+.

<sup>&</sup>lt;sup>28</sup> Small sample size. Out of a total of n=50 who scammed, n=27 were scammed via telephone.

• In the face to face survey, just under half (45%)<sup>29</sup> of those aged 75+ who had been targeted ended up being scammed via telephone.

It is not clear whether this was because these age groups were more susceptible to these scams, or whether fraudsters were deliberately targeting the older age groups.

## In this study, the majority of scams via telephone involved some sort of legitimate appearance techniques.

This approach tended to involve fraudsters pretending to call from reputable businesses or public institutions and attempting to extract personal details or to gain access to these remotely.

Fraudsters posing as legitimate businesses seek to exploit several factors that might predispose consumers to taking the bait. First and foremost is trust and authority. In nine out of the ten qualitative interviews where telephone was the scam channel, fraudsters exploited consumers' trust and respect for authority and public institutions.

#### Case study #14: Ray, 74, Rural, England

Ray is retired, but continues to administer the family business. His acuity has become slightly impaired according to his son. Ray is predisposed to being honest, trusting, and respectful of authority. Ray received a call from someone impersonating an HMRC official. He was about the same age as Ray, well-spoken, authoritative and very persuasive. The fraudster said Ray had a VAT payment owing and should pay to avoid a fine. The caller said if he paid now then no further action would be taken. Ray transferred £4,500. His son investigated and HMRC confirmed no payment was due. The bank took no responsibility and could not help. Ray reported the incident to the Police and Action Fraud, but heard

25

<sup>&</sup>lt;sup>29</sup> Small sample size. In the telephone booster survey, out of a total of n=50 who scammed, n=27 were scammed via telephone.

Consumers also appeared to have a strong sense of confidence in spotting a scam on the telephone. Over nine out of ten (92%) were confident, with nearly half (46%) of these saying they were very confident. This confidence appeared to contribute to the participant being scammed in the example below.

#### Case study #15: Neil, 24, Urban, England

Neil is married and a father of two small children. He works in debt finance, hears about scams all the time and considers himself pretty savvy. He was just getting into his car, rushing to get to the shops and get home for a football game, when he received a text from his bank, asking him if he had noticed unusual activity on his account and to respond 'Yes' or 'No'. He responded 'No'. He immediately got a follow up call asking him to confirm details, which he did – all of them. He thought nothing of it and then noticed small amounts going out of his account followed by one payment for £400. He spoke to the fraud department who implied that it was his fault and questioned why he had handed over his details. They then froze his bank account for three weeks whilst they investigated. Neil was annoyed and disappointed with himself for being caught out. He couldn't believe it had happened. His attitude has now changed. He doesn't like talking to the bank on the phone and will go into the branch instead. He has also put his money into different

Fraudsters can use the telephone / their voice to pressure and coerce the participant into doing something they would otherwise not want to do. In the example below, the fraudster used aggressive tactics that caused a vulnerable woman to get stressed and engage unwillingly.

#### Case study #16: Wendy, 65, Urban, Wales

Wendy is financially and physically disabled, with low digital literacy. She just has a mobile. She got a call asking if she wanted to take part in a survey in return for vouchers for various products. She went through all her hobbies, likes and dislikes, and then the caller started to try and sell her things, which she didn't want. The caller became very pushy and aggressive. Wendy just wanted to get rid of her so decided to get a subscription for £1. She handed over her bank details. A week later she went to the ATM and discovered that £96 had been removed. She panicked as this was money that she could not afford to lose. She went straight to the bank and, after looking into her account, they refunded the money.

#### 5.5 Text

Incidence Rates Overall	Of those targeted, 64% thought they had been targeted in the past two years via text. Of those scammed, 13% were scammed via text.
Demographic Differences	Women and younger age groups (16-34).
	Of those scammed via text, two thirds were women (67%) and just over two fifths (41%) were aged 16-24 <sup>30</sup> .
Money Lost	Median £76  Text accounted for 15% of people who lost money.
	Of those who were scammed and lost money, just under two thirds (63%) lost up to £ $100^{31}$ .

## In this study, text was used by fraudsters in two ways – premium rate texts and texts pretending to come from legitimate organisations.

Bogus legitimate appearance texts take advantage of this channel being used predominantly for notifications from public services, such as banks, dentists, HMRC, doctors, etc. These text scams appear to succeed with people who are pre-disposed to trusting in these public services and those lacking awareness of these types of scams.

#### Case study #17: Roy, 48, Male, Urban, Northern Ireland

Roy is a taxi driver, married with 3 children. He lacks digital confidence and never comes into contact with HMRC. He received an email from HMRC one day and ignored it. A few days later, he got a text message also from HMRC saying he needed to update his details. He was a bit surprised by this and put it down to his daughter just turning eighteen. He was also a bit concerned and thought he should do something. He clicked the link, put in his bank details. Next day his bank called to ask whether he was aware that £100 was taken out of his account. He was annoyed that the bank could not help recover the money.

27

<sup>30</sup> Small sample size. Out of a total of n=54 who were scammed via text, n=36 were female, n=22 were aged 16-24.

<sup>&</sup>lt;sup>31</sup> Small sample size. Out of a total of n=42 who lost money via text, n=26 lost up to £100.

## Confidence levels in spotting a scam via text were high – overall 92% were confident, with 45% saying they were very confident.

This feeling of confidence, combined with clever use of technology and a coincidence being seen as evidence, were the factors that led to this participant being scammed in the example below.

#### Case study #17: Tracy, 39, Female, Urban, England

Tracy is married with 2 children and considers herself to be technically savvy. She has a credit card with Argos and was thinking she was due a refund. She received a text from Argos saying she was due a refund. The text used the same number Argos always used for confirmation and authentication. She clicked the link and inputted her bank details and tried to log into her account, with different usernames and passwords. She realised something was wrong and called Argos. The fraudster had taken £800 from her account, which was refunded by Argos. Tracy was upset with herself for being scammed, but she was convinced by the number being masked and that the message said she was due a refund. It has left her feeling very anxious, and she checks her accounts daily.

Young adults and women<sup>32</sup> appeared to be more susceptible to premium rate scams. These might involve a spoof text saying you have subscribed to a service with payment being taken unless you type STOP. This 'micro-mugging' is intended to remove small amounts of money such that the target does not notice and report the incident.

#### Case study #18: John, 23, Male, Urban, Scotland

John is 23 and works as an engineer. He noticed that his bill was not a round number and downloaded his service provider app to see what payments were going out. He noticed that £4.99 was going out to company he had never heard of and he had been making these payments over the past eleven months. He called his service provider and, to his surprise, they gave him a number of the company to call. He had looked for this number online and hadn't been able to find it. He called the company and they reimbursed him his money, without question. He found it odd that his service provider was fully aware of this activity.

#### **5.6 Post**

32

<sup>&</sup>lt;sup>32</sup> Small sample size. Out of a total of n=12 scams via premium rate texts, women accounted for n=11 scams and 16-24 year olds accounted for n=6 scams.

Incidence Rates Overall	Of all those targeted, 36% thought they had been targeted in the past two years via post addressed to them personally; 28% thought they had been targeted via post not addressed to them personally.  Of those scammed, 10% were scammed via post overall, 6% via post addressed personally, 4% via post not addressed personally <sup>33</sup> .
Affected Segments	No difference between segments
Money Lost	Median £301  Post accounted for 10% of people who lost money <sup>34</sup> . Of those who lost money via post, 51% lost more than £100 via post addressed to the personally, and 54% lost up to £100 via post not addressed to them personally <sup>35</sup> .

Scams via post appear to cover a range of fraud, including fake official letters, fake invoices, advance fee scams, investment scams and inheritance fraud. In the case of one participant, a combination of factors - including coincidence as evidence, sophisticated legitimate appearance and illness – appeared to contribute to the scam.

#### Case study #19: Vicky, 34, Female, Semi-rural, Northern Ireland

Vicky was heavily pregnant and feeling very unwell. She received a letter from Netflix saying she needed to update her account. As her card had just expired, she thought this made sense. She also felt responsible for dealing with the matter quickly as several members of her family relied on the account. She typed in the link and was taken to a site, identical to Netflix's account page. She put in her details and forgot about it. A few weeks later, she went to pay for something with her credit card and it was declined. She thought it was odd as she had a £500 limit and never used her card. She contacted the bank and they confirmed it was a scam. She felt very stupid and emotional due to her condition. She recouped all of the money.

 <sup>34</sup> Small sample size. Out of a total of n=285 who lost money, n=29 lost money via post.
 <sup>35</sup> Small sample size. Out of a total of n=16 who lost money via post addressed to them personally, n=8 lost £100+. Out of a total of n=13 who lost money via post not addressed personally, n=7 lost up to £100.

<sup>&</sup>lt;sup>33</sup> Small sample size. Out of a total of n=44 scammed via post, n=26 were scammed via post addressed personally, n=18 via post not addressed personally.

### 6. Reporting

#### 6.1 Overview

Awareness of organisations involved in tackling crime, such as Action Fraud, appeared to be fairly widespread across amongst the online sample, including across the older age groups. Awareness of Action Fraud amongst the online sample was higher than amongst the booster samples and seems to have changed since the 2017 Citizens Advice report. The reasons for this are not clear. This may be due to differences in survey methodology (online vs telephone, for example) or that awareness has increased, particularly amongst those engaging online.

Reporting rates overall (after having been scammed) were largely consistent across the different samples – just over three in five people who were scammed (61%) say they reported the incident to someone. Reporting rates to specific supporting organisations were similarly consistent but much lower – roughly one in five reported the scam to Action Fraud.

Amongst the qualitative sample, awareness of, and engagement with, supporting organisations were similar to the booster samples. Only a minority had heard of Action Fraud, for example, and reporting to Action Fraud generally took place due to referrals from the Police. Most people only reported to their bank as this was the most likely route to recouping their money. A minority reported to the Police – almost all businesses and a few consumers who felt they should report the crime. Most did not think their case warranted involvement beyond the bank.

For most, there was little motivation, at least in the short term, for people to report the incident. Supporting organisations, even if people were aware of them, could not help with recouping their money. The exception was the Financial Ombudsman. However, some participants were motivated to share their experiences, once the initial shock had passed, in order to try and prevent it from happening to others. Several commented that sharing their experiences in a supportive environment could help them cope emotionally. Conversely, where the actual experience of reporting was negative or they received no feedback, feelings of isolation and self-blame were compounded.

#### 6.2 Awareness of Organisations and Reporting Intent

In the quantitative survey, prior to be asked about their exposure to scams, participants were asked how confident they were in knowing who to report to if they wanted to report what they thought was a scam. Just under two thirds (61%) reported they were confident and these levels were consistent across the different samples (online, telephone and face to face).

However, reported awareness of supporting organisations, such as Action Fraud, amongst the online sample was much higher than the booster samples and has changed since the 2017 Citizens Advice report, as illustrated below.

Figure 4. % organisations they would report to if they wanted to report a scam

	Online	Online	Phone (55-	F2F (75+)	Citizens
	(all)	(55+)	74)	F2f: n=151	Advice 2017 n=3,026
	Online all: n=4,038	Online 55+: n=1,472	Telephone: n=303		·
Police	50%	53%	51%	60%	48%
Action Fraud	40%	47%	9%	1%	5%

#### 6.3 Actual Reporting Rates

Actual reporting rates, (i.e. reporting to an organisation after being scammed) were largely consistent across the different data collection approaches. Overall, 61% said they reported the incident.

As illustrated below, the differences in reporting rates between the main survey and the booster samples were not considerable, and should be considered indicative due to the small samples sizes in the booster samples.

Figure 5. Actual Reporting: % Organisations reported to after being scammed<sup>36</sup>

Base: all targeted & scammed	Online (all ages) (base n=331)	Online (55+) (base n=44)	Telephone (55+) (base n=30)	Face to Face (75+) base n=22
Police	50%	53%	37%	25%
Action Fraud	24%	29%	13%	15%

Reporting rates amongst the qualitative interviews were in keeping with the booster samples. Out of forty-six interviews (all with people who had been scammed), a total of eleven people reported the fraud – ten to the police and five to Action Fraud. Of these eleven, five were businesses and six were consumers. Three out of the sample had heard of Action Fraud prior to the scam, and the five who reported to Action Fraud had been recommended to do so by the Police.

<sup>&</sup>lt;sup>36</sup> Small sample size amongst booster samples (telephone and face to face).

Overall, it appears that reporting rates to organisations involved in tackling fraud other than the Police (such as Action Fraud) remain low.

#### 6.4 Experience of Reporting

Participants in the qualitative stage had very different experiences from each other when reporting to organisations involved in tackling fraud.

#### 6.4.1 Reporting to Banks

Most participants in the qualitative sample had been affected in some way financially and most of these contacted their bank first.

All of those reporting a scam were put through to their respective bank's fraud department and had to answer some detailed questions.

For some, the experience was purely functional with the fraud team taking details and saying they would look into it. Most of these were not successful in recouping their money because they were told they had handed over their bank details on their own volition.

For several others, the experience was upsetting, reporting that the bank had not only implied that it was their fault, but they had been foolish to have allowed it to happen.

"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 as I've got my mortgage with them." (Male, 24, England)

One or two felt that the bank's response was more like an interrogation and they were the ones under suspicion.

"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)

For a minority, the experience was positive, primarily because they received their money back. In this respect, there did not appear to be any common factors that influenced successful recovery of money, just the bank's discretion at the time. Almost all had voluntarily handed their details over to a fraudster and had money removed

from their account. There was some indication that the banks looked more kindly on the very elderly and the most vulnerable

"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)

"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)

The majority of people who had used a credit card were refunded their money. Similarly, the majority of people who used PayPal also recovered their money. PayPal was praised for the processes it had in place to protect people who had not received the goods as expected. The majority of those who had been scammed on auction sites had lost money because they had made payments outside of PayPal (in return for a reduced price) or used the friends/ family method on PayPal (in return for a reduced fee).

"The answer is use PayPal and then you're protected. I transferred money via BACS because they said they didn't use PayPal and I lost £4,500. I would have been protected with PayPal." (47, Female, Scotland)

#### 6.4.2 Reporting to Other Organisations

A minority also reported to other organisations. These included the Police, Action Fraud and the Financial Ombudsman. Reporting to these organisations was made by most businesses and those consumers who felt the scam was sufficiently serious to take it further than just their bank. In most cases, this was because the amount of money lost was in the thousands, or there was an unresolved disagreement with the bank.

#### The Police:

By and large, reporting to the police was seen as the logical step as a victim of crime. It was also the only place to go for most as awareness of any other organisation for support was very low. Expectations of the police resolving the problem were generally low.

"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)

There were one or two cases where participants felt that better integration between the banks and the police would have made a difference

"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)

#### **Action Fraud:**

Of the five participants who reported to Action Fraud, four had submitted reports and heard nothing back. One had contacted them for advice and was pleased with the response

"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)

#### **Financial Ombudsman:**

Just two participants had reported to the ombudsman. In both cases, they received no notification when the submitted their reports, but they did hear back several months later that their cases were being reviewed. Both cases stayed with the Ombudsman for just under two years and were resolved successfully in the end. Overall, lack of communication appeared to be the issue.

#### **6.4.3 Reasons for Not Reporting:**

Participants in the quantitative phase, who had been scammed and not reported it, were asked why they had not reported. Of the 39% of those who had been scammed and did not report the incident, 27% said they did not know who to report it to, 24% thought it would make no difference if they had reported it and 21% felt it was not worth reporting.

These findings were consistent with outputs from the qualitative interviews. Many participants felt that that amount of money they had lost was not worth reporting to any organisation other than their bank. For most, the only other organisation they knew about was the Police and they felt their experience did not warrant contacting

the Police. Most just wanted to get their money back and it was the fraud department in the bank that was the best route for this

"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)

One or two felt that engaging any other organisations might interfere with the bank's efforts jeopardise their chances.

"I didn't want anyone else poking around. I was relying on the fraud department and I thought they might not appreciate the police getting involved, not that they probably would have done." (62, Female, Northern Ireland)

And there were a few that were too traumatised to go through the process of reporting to another organisation.

"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)

#### 6.5 Motivations to Report:

Survey participants who had been targeted and scammed were asked what might encourage them to report more in the future.

Figure 6: Elements that would motivate people to report

Q24. What, if anything, would make you more likely to report a potential scam in the future?



These results were consistent with the qualitative feedback, in which most participants felt there was little motivation in reporting as it was unlikely to help in the immediate aftermath of a scam. Their focus was on trying to recoup the lost money.

Beyond this, a small minority did not want to report the scam because they did not want to relive the experience, and risk being told that they were to blame.

Conversely, there was a strong sense that, after the initial shock of being scammed, some participants did not want to just let the matter rest. These were participants that were heavily impacted by their experience and they wanted some means of communicating their experience in order that others did not suffer in the same way.

One participant took to social media and asked friends to pass her story around. To her surprise, she received a lot of responses that people already knew about the scam. She was left wondering why she was the only one that had not known about it and wished that such information was more readily available.

The rest did not know where to go to and took no action in spite of their willingness to share their experiences.

# **6.5.1** Reparation & Reporting:

It was notable how many of the participants commented on the positive effect of being able to talk to someone about the scam and to know that their experience was being taken seriously. This was sometimes realised when giving a statement to the police as the police were generally felt to be attentive and sensitive. It was also evident when conducting these interviews as for many participants this was the first time that someone had taken an interest. This 'attentiveness' appeared to help reduce the burden of isolation and self-blame that seemed common with people who had been scammed.

Conversely, the lack of support at the time of reporting, or hearing nothing back after having made a report, seemed to compound people's sense of isolation and negative feelings.

"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)

# 7. Impact of Fraud

#### 7.1 Overview

More than two thirds (70%) of people scammed lost money and younger people were more likely to lose money than older age groups. For a minority, the financial loss had a very significant impact with people going into debt and losing savings.

More people lose money online than other channels but the majority (60%) lost up to £100 online. However, whilst telephone accounted for over one in 10 (13%) of those who lose money, participants appeared to lose more money via telephone than other channels<sup>37</sup>, often into the thousands (as evidenced from our qualitative interviews).

For many participants in the qualitative sample, the impact of being scammed was very damaging, affecting, variously, their emotional and psychological state, their reputation and standing, their personal and professional relationships, and their physical wellbeing and safety. In several of these cases, people's attitudes and behaviours changed significantly from what they were prior to the scam and there was a 'chilling effect' on their use of communication services.

# 7.2 Financial Impact: Key Figures

70% of consumers, who were scammed once or more than once in the past two years, lost money. Of those who lost money, half (51%) lost more than £100 (24% lost more than £500). Just under a third of those who lost money (32%) did not recoup any money. Amongst the majority who did recoup some money (68%), just under one third (30%) recouped all the money<sup>38</sup>.

Amongst those who were scammed and lost money, younger age groups were more likely to lose money than older age groups. Nearly 4 out of every 5 16-34 year olds (79%) lost money, compared with two out of every 5 aged 55+ (44%).

However, in terms of the amount of money lost, the majority (62%) of 16-24 year olds lost up to £100, compared with 25-34 year olds, where 61% lost more than £100.

Amongst those who lost money, the majority was seriously affected in some way, as illustrated in the chart below.

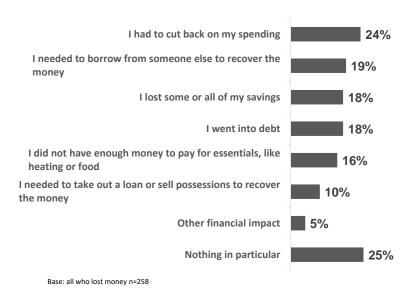
<sup>&</sup>lt;sup>37</sup> Small sample size: Out of a total of n=36 who lost money via telephone, 64% (n=23) lost more than £100 (28% lost more than £500 (n=10); compared with email, where out of a total of n=65 lost money, 45% lost more than £100 (n=29), 16% lost

more than £500 (n=10).

38 Base size: all who lost money once or more than once in the past 2 years n=285

Figure 7. % of people impacted in different ways by financial loss

Q27. What was the financial impact to you personally of losing this money as a result of the scam?



### **Financial Impact: Differences by Channel**

The proportion of people losing money through the different channels largely correlated with scam incidence rates. Online accounted for the highest number of people getting scammed (27%) and the highest proportion of people losing money (31%). Email accounted for 26% of people getting scammed, and accounted for 23% of those losing money.

However, in terms of the amount of money lost per channel proportionately, the results were different. Of those who lost money online, the majority (60%) lost up to £100. Similarly, of those who lost money via text, the majority (63% $^{39}$ ) lost up to £100. And via email, of those who lost money, half (50% $^{40}$ ) lost up to £100.

Telephone, however, accounted for just 13% of people who lost money. But, of those who lost money by telephone, only a third (35%) lost up to £100. Nearly two thirds (64%) lost more than £100, and, of these, more than a quarter (28%) losing more than £500. In short, those who did get scammed by telephone, mostly older age groups, were likely to lose more money than via any other channel. These figures correlate with median / modal calculations below and are also in keeping with the qualitative feedback.

<sup>&</sup>lt;sup>39</sup> Small sample size. Out of a total n=42 who lost money via text, n=26 lost up to £100.

<sup>&</sup>lt;sup>40</sup> Small sample size. Out of a total of n=65 who lost money via email, n=32 lost £100+.

The median and modal amount of money lost per person across all channels was £301.

Figure 2. Median and modal amount lost by channel

	TOTAL	Online	Email	Phone	Text	Post (personal)	Post (not personal)
Median	£301	£76	£76	£301	£76	£301	£76
Mode	£301	£76	£301	£301	£301	£76	£36

Base: All those targeted and scammed and lost money once or twice in the past 2 years (total n=285; online n=89; email n=65; telephone n=36; text n=42; post (personal) n=16; post (not personal) n=13. (note: small sample sizes).

## 7.3 Impact of Financial Loss

In the qualitative interviews, the amount of money lost varied from relatively small amounts to tens of thousands of pounds. However, the impact felt by the loss of money was related to the person's circumstances; for some, even losing a relatively small amount of money could lead to financial difficulties. In some cases, the amount of money lost was small and the impact was negligible. These small amounts resulted from scams on auction sites involving concert tickets, technical equipment, mobile phones, etc. In these cases, the impact of the short-term loss was often nothing more than a reminder that it was more advisable to protect themselves with payment platforms, such as PayPal.

The impact of other relatively small losses, for example 'micro-mugging' via premium text scams, stimulated the participants to be more vigilant, as well as provoking feelings of irritation that these activities went undetected.

However, for one or two of the most financially vulnerable, any loss was extremely distressing, raising the prospect of going into debt and putting pressure on their health.

"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 short-term loss was acutely felt in cases where bank accounts were frozen whilst the fraud was being investigated. This meant the individual had to find other means of finding money, usually by borrowing off friends or family. The sudden uncertainty of having no access to money, coupled with having to ask others for help, was invariably stressful.

"I'm a single dad with two children, and suddenly out of nowhere I couldn't pay for anything. I felt completely helpless and very stressed. Fortunately, the sports club where I work lent me some money but it was embarrassing to have to ask. I hadn't even done anything; my phone was hacked, and I didn't know anything about it." (Male, 43, England)

For a few consumers and businesses, the financial loss had serious long-term implications, which they were struggling to come to terms with.

"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)

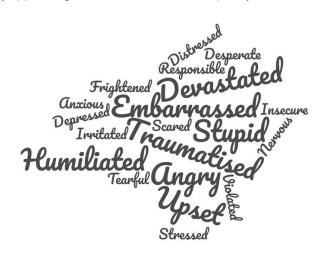
"I had big plans to expand the business with the new piece of machinery, now I'm £10,000 down and will have to take out a loan to cover the hole. I've gone backwards several years, it's so depressing." (58, Male, England)

# 7.4 Emotional / Psychological Impact

Whilst the financial loss had a significant impact on several participants, the emotional and psychological impact often extended long after the immediate financial lost. In some cases, the impact was purely emotional and psychological and not linked to any financial loss. It was clear, however, that the impact of being scammed had a profound and damaging impact, emotionally and psychologically, on many of the participants in our qualitative sample.

When asked to describe their experiences, and the impact of being scammed, the following words were mentioned.

**Figure 3. Words used to describe the emotional impact of being scammed.** (Words used most frequently appear larger than words used less frequently).



Often, participants expressed a combination of the above emotions to describe the impact of their experience. Common to almost everyone was the feeling of embarrassment and shame that they had fallen for the scam. All of these participants considered themselves competent, careful people prior to the scam. However, after their experience, many had begun to question their judgement and had lost their self-confidence.

Participants voiced a number of specific impacts and these are discussed in detail below:

- Embarrassment & Loss of Self-Belief
- Responsibility & Loss of Trust
- Anger & Frustration
- Personal Intrusion & Violation
- Impact on Relationships
- Time and Resources

#### **Embarrassment & Loss of Self-Belief**

Embarrassment and loss of self-belief was acutely felt by those participants who had co-operated with the fraudster's wishes to an extent that seemed unbelievable to them once the full extent of the scam was revealed. In many of these cases, there had been plenty of opportunity to stop complying with the fraudster (including being advised by others to do so), but such was the extent of their belief that they were doing the right thing or were close to the prize that they continued. Their conviction in the scam only served to compound their feelings of embarrassment.

"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)

#### **Responsibility & Loss of Trust**

Scams in the workplace appeared to have a particularly devastating impact. The sense of shame and embarrassment was felt both as an individual and as an employee. The sense of responsibility, of letting people down and perceived loss of trust by their boss were extremely damaging. In these cases, the person could be too upset to talk about it to anyone else, including their friends and family.

"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)

"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)

#### **Anger & Frustration**

Strong feelings of anger were another emotion widely felt. People were angry at being duped and stolen from. Most of all, people appeared to be angry because they felt they could do nothing about the scam, not even prevent it from happening to others. One or two were angry because they felt they had been scammed due to the failings of others and no action was being taken. Often, these feelings of anger were compounded by other people who appeared to pass judgement

"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)

#### **Personal Intrusion & Violation**

Several reported how they felt they had been personally violated and this was often felt by people who had been scammed over the telephone, particularly the landline. Added to this, many of these interactions with the fraudster took time and involved a degree of intimacy. The fraudster often goes to great lengths to develop rapport and promote feelings of trust. As a result, when the scam was revealed, these feelings of being intruded and violated were particularly strong

"I spent an hour on the phone with this man, who I had grown to like I suppose – he was helping me protect my family by fixing these problems with the Internet. It took me quite a while to realise what had happened and then I just felt sick, dirty and

violated by a man, who had just intruded into my family home on a weekend and turned it upside down. I still get upset when I think about it." (53, Female, Wales)

## 7.5 Secondary Impacts

A number of secondary impacts were reported, that came about as a result of the initial emotional trauma. These included the impact on relationships, as well as the time and resources needed to fix the damage. In addition, several participants commented on the longer-term implications of their experience.

#### **Impact on Relationships:**

Several talked about the impact on their relationships with close family. In one or two cases, the financial loss was acutely felt by everyone in the household, resulting in arguments, recrimination and blame

"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)

The impact on the victim of the romance scam was similarly damaging and extended over a long period. This consumer was socially isolated and vulnerable in the first place, and the impact of the scam made them feel wary and anxious about attempting to develop new relationships

"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)

#### **Time and Resources:**

The amount of time and resources needed to repair the damage as a result of persona details being compromise was noted by many participants. The majority of interviewees had to make changes to bank accounts as well as updating direct debits and other accounts with new details, usernames and passwords. For those receiving government support, updating these details were particularly time consuming, often involving face to face visits.

#### Long-term Implications: Changes in Behaviour

Almost without exception, people admitted to being more cautious and careful when engaging with any communications services. This new cautionary behaviour manifested itself in different ways. For a small minority, more caution generally was enough, seeing the experience as part of life and moving on

"I know there are people out there trying to pull a fast one. But I'm not going to spend the rest of my life not doing things I like and looking over my shoulder thinking everyone's a thief. I'll just be more careful." (75, Female, England)

For others, the changes in behaviour were a little more pronounced, such as spreading their finances between accounts, checking their accounts and subscriptions and ensuring the used payment mechanisms that offered some protection (e.g. PayPal or credit cards).

#### "Chilling Effect"

Many, however, had become increasingly anxious since being scammed and, to mitigate these feelings, had made quite dramatic changes to their behaviour. These changes tended to relate primarily to the channel via which they had been scammed, but, in some cases, also extended far beyond.

Those people scammed via telephone, landline in particular, were now very wary about picking up the phone and, in many cases, had simply stopped. One lady in her 80s, for whom the landline was her only communication device, had decided to protect herself by having a whistle next to the phone and blowing it loudly if the caller was unknown to her.

In cases where people had been scammed online, several had stopped purchasing from any websites, aside from mainstream e-commerce sites such as Amazon or Argos. For some of those who were vulnerable in terms of their digital literacy, there was a very significant regression and disengagement from the online world, almost entirely

"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)

One or two younger participants had become so anxious about their personal information being used against them that they had decided to remove themselves from socialising online.

"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)

For a small minority, often vulnerable due to illness, the effect has been very dramatic and they have all but stopped communicating on any device with strangers.

"I don't open emails from anyone I don't know. I don't answer the phone any more 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).

# 8. APPENDIX:

# 8.1 Method and Sample

# 8.1.1 Stage 1: Quantitative

We surveyed a nationally representative<sup>41</sup> sample of 4,492 adults using three different approaches.

The main sample (n=4,038) was conducted using an online panel with quotas set to ensure the results were nationally representative of UK adults aged 16+. An online panel approach was agreed as it offered the right combination of a trusted environment for participants (the panel had been established for over 10 years and was well managed) as well as anonymity.

We supplemented this main sample with two smaller surveys, one via telephone, the other using a combination face to face and telephone. The aim with these 'booster' surveys was to ensure representation of those who may not be online or who make limited or no use of the Internet.

We conducted a telephone survey with n=303 adults aged 55-74 (n=100 55-64 year olds; n=203 54-74 year olds). Telephone was agreed as an acceptable approach, given their confidence in answering the phone and willingness to participate in a bona fide survey.

The face to face survey comprised n=151 adults aged 75+ (n=100 75-84 year olds; n=51 aged 85+). These consumers were contacted and interviewed by individual recruiters who had trusted networks in their communities. A face to face approach was agreed as it could provide suitable support and reassurance.

All those who identified as being scammed were asked if they were willing to take part in further research. These re-contacts were important to ensure we represented the full range of experiences in Stage 2.

We combined the three datasets (online, telephone and face to face) and then applied a weighting to ensure the merged dataset was nationally representative.

<sup>&</sup>lt;sup>41</sup> This means representation of the UK population in terms of age, gender, nation (England, Scotland, Wales and Northern Ireland), location (urban and rural); SEG (AB, C1, C2 and DE); income, working status, ethnicity, disability and digital skills

# 8.1.2 Stage 2: Qualitative

We conducted 40 in-depth, face to face interviews with a good cross-section of 16-85+ adults, using the standard variables of age, gender, SEG and location (urban, suburban, semi-rural, rural). We also conducted 6 interviews with micro-businesses.

Within the consumer sample, we included specific sub-samples of people who were in a vulnerable or potentially vulnerable situation. About half of the sample identified themselves as being with limited digital skills, low income, socially isolated or with circumstantial vulnerabilities (e.g. physical sickness).

Twenty-eight participants out of forty, and all the business interviews, were free found via individual recruiters with established, trusted networks. These close ties with their community were important to encourage participation amongst scam victims, many of whom had been left feeling humiliated and embarrassed by their experiences.

The remaining twelve participants were recruited via the re-contacts from the quantitative survey. These allowed us to represent the full range of scams identified in Stage 1, some of which we were unable to find via recruiter networks. The final sample also corresponded with number of scams identified via the different channels. Of the 40 interviews, 24 interviews involved scams via online / email; 15 via phone / text; 1 via post.

# 8.1.3 A note on interpretation, analysis and reporting of qualitative data

It is important to note that the findings of this report are not statistically representative of the views of the general public. Qualitative research is designed to be illustrative, detailed and exploratory and provides insight into the perceptions, feelings and behaviours of people rather than conclusions drawn from a robust, quantifiably valid sample.

# **8.1.4 Final Qualitative Sample Frame:**

			England	Wales	Scotland	N Ireland
	Total	Total Achieved	Achieved	Achieved	Achieved	Achieved
	40	40	15	8	9	8
Male	18	17	6	2	6	3
Female	22	23	9	6	3	5
16-18	4	2		1	1	
19-21	5	5	2		2	1
22-29	4	4	3			1
30-40	4	4	1		1	2
41-54	5	7	3	2	1	1
55-64	5	7		3	2	2
65-74	6	6	2	1	2	1
75+	7	6	4	1	1	
Single	8	8	3	1	2	2
Partnered / no children	5	6	2		3	1
Younger family	5	5	4			1
Older family	5	5		3	1	1
Empty nester	5	6	3	1		2
Retiree	12	10	3	3	3	1
ABC1	15	15	8	2	2	3
C2	11	11	4	4	1	3 2 3
DE	14	15	3	2	7	
Low / limited digital skills	6	7	2	2	1	2
Circumstantial	6	2		1		1
Socially isolated	3	2	1	1		
Very low income /	6	9	2	1	4	2
Financially vulnerable						
Sight impairment	2	1	1			
Hearing impairment	2	3	2		1	
Dexterity / mobility impairment	2	1			1	
Urban	14	16	9	2	3	2
Suburban	11	12	4	4	3	1
Semi-rural	8	7		1	3	3
Deep rural	7	5	2	1		2
Via telephone call	11	11	7	2	1	1
Via email	11	8	1	1	3	3
Via online (websites)	8	16	5	3	5	3
Via text (mobile app)	5	4	2	2		
Via post (personal / non-	5	1				1
personal)						