Technical Report - Online Scams & Fraud Research

Table of Contents

Preface

The online scams and fraud research was undertaken by Yonder Consulting on behalf of Ofcom. The main objectives of this study were to better understand people's experience with online fraud or scams, and the impact the experience has had on victims' mental wellbeing and behaviours.

The research has strengthened Ofcom's understanding of user experience of online fraud and the impact of this harm from a financial and emotional perspective. The insights drawn from this research may inform Ofcom's future work to prepare for its forthcoming duties under the Online Safety Bill.

The research used a mixed-method approach consisting of a quantitative online survey, followed by qualitative in-depth interviews. Further information about the study is summarised in the sections below.

Summary of Approach

- This research was a mixed-method quantitative and qualitative study, conducted with a sample of UK adults aged 18+, to understand the experiences of various types of online scams or fraud.
- The quantitative phase was carried out as an online survey, with respondents recruited from Yonder's proprietary online panel 'YonderLive', containing around 150,000 panellists from all over the UK. Respondents were recruited to be nationally representative of the UK internet user population, with quotas set on gender, age, socio-economic group (SEG) and region. Boosts were applied to those who last experienced a low-incidence scam or fraud on a best-effort basis to attempt to achieve a minimum base size of 100.
    - The data was weighted to be representative of the UK internet user population on age within gender, and overall to the region and SEG profiles. This approach counteracted any effect that boost oversampling would have had on the final data.
    - A total of 2,097 quantitative interviews were conducted between 5th May – 17th May 2022.
- The qualitative phase consisted of online depth interviews with 32 victims of online scams or fraud, to explore their experiences and the resultant impact on their lives in greater detail. In addition, 5 experts who have supported victims of online scams or fraud were recruited to obtain an independent view.
    - Interviews took place between 12th October – 11th November 2022.

Quantitative Research

Introduction

Yonder Consulting conducted an online survey with a sample of 2,097 UK adults between 5th May – 17th May 2022 in order to understand the prevalence of online fraud or scams, to understand the user journey including various communication channels that may be used when encountering instances of scams or fraud, to explore how victims responded to encounters and the outcome reached as a result, and to investigate the impact on victims' mental wellbeing and behaviours.

Details of the sample design, research methodology, and weighting procedures for this study are outlined on the following pages. A note on statistical reliability is also included.

Sample Design

A sample of UK internet users aged 18-84 was provided by Yonder's proprietary online panel, YonderLive, which is made up of 150,000 internet users across the UK. Boosts were also applied to low-incidence online scams or fraud to ensure that achieved base sizes were large enough to allow for detailed and statistically robust analysis. This was done on a best-effort basis due to the difficulty of targeting these respondents.

Quotas

Interview quotas were applied so that the final sample was representative of UK internet users by age, gender, region and socio-economic group (SEG).

Targets for quotas were derived from Yonder's bi-weekly online omnibus, and moderated by data obtained from the Ofcom Online Research Panel[1] recruitment and the Office of National Statistics (ONS).

Quotas were set on the following variables:

- Age (18-24, 25-34, 35-44, 45-54, 55-64, 64-74, 75-84)
- Gender
- Region
- SEG

The table below details the specific quotas that were used for this study:

Demographic group	Category	Quota
Gender	Male	49%

[1] Ofcom commissioned Yonder to create a ring-fenced online panel (the Online Research Panel) of 6,000 internet users as part of the contract for research into experiences, attitudes and behaviours online, of which this study forms part of. This panel was recruited from Yonder's wider panel (YLive). It is known that certain biases may exist on online panels given the nature of the methodology (e.g. panelists may be more active internet users). In order to mitigate bias, during the recruitment phase for the Online Research Panel, Yonder conducted an offline CATI calibration exercise to obtain the most up-to-date and accurate data for time spent online per day, device usage, and video-sharing platform usage. Weighting profiles for this study were then moderated using a combination of the data from the online and offline recruitment exercises, and benchmarked against data available on the known proportion of each age group that use the internet, provided by the ONS.

	Female	51%
Age	18-24	12%
	25-34	18%
	35-44	17%
	45-54	19%
	55-64	15%
	65-74	12%
	75-84	6%
Region	Scotland	8%
	North East	4%
	North West	11%
	Yorkshire & Humberside	8%
	West Midlands	9%
	East Midlands	7%
	Wales	5%
	Eastern	9%
	London	14%
	South East	14%
	South West	9%
	Northern Ireland	3%
SEG	AB	27%
	C1	30%
	C2	21%
	DE	22%

Fieldwork

All quantitative interviews were conducted between 5th May – 17th May 2022 using Yonder's online panel (YonderLive), closing fieldwork at 2,097 interviews. We included boosts for all low-incidence scams or fraud that were most recently experienced by the respondents, attempting to get a minimum sample of 100 on a best-effort basis.

Due to the highly sensitive nature of some of the research topics, respondents were forewarned of the sensitive nature of the research topic and asked to give their consent to participate, in line with MRS guidelines. They were also reminded of their right to withdraw before being shown a question related to the emotional impact of a scams or fraud experience. At the end of the survey, they were provided with web links to organisations that could provide guidance and support to those who have experience of scams or fraud.

Duplication checks took place to ensure that respondents could not complete the survey more than once. As well as duplication checks, Yonder carried out the following checks during and post fieldwork as standard:

- IP geo-locator checks to ensure the respondents are all based in the UK.
- Front and back end quality control questions within the survey to ensure respondents are answering logically and consistently.

- ‘Trap’ questions within the survey to ensure respondents are paying attention and reading each code i.e. at a random question we would ask them to select a certain code, those who do not select this will be remove from the data.
- Manual speeder check post fieldwork to remove anyone deemed to have proceeded through the questionnaire at an unreasonable pace.
- Manual flatlining checks post fieldwork to check grid questions and ensure respondents aren’t answering the same codes across an unreasonable range of grid/scale questions.
- Open end checks to ensure respondents are answering thoughtfully and not spamming answers.

Weighting

The data has been weighted to be representative of the UK internet user population on age within gender, and overall to the region and SEG profiles. This approach counteracted any effect that boost oversampling would have had on the final data.

Weighting profiles were created using a combination of Yonder online omnibus data and CATI omnibus data[2] to produce the most accurate profile of UK internet users.

Sample Representativeness

The following table shows the unweighted sample:

Demographic group	Unweighted counts	Unweighted %	Weighted counts	Weighted %
Male	1,122	54%	1,022	49%
Female	964	46%	1,064	51%
18-24	162	8%	257	12%
25-34	384	18%	389	19%
35-44	382	18%	366	17%
45-54	385	18%	395	19%
55-64	361	17%	312	15%
65-74	290	14%	247	12%
75+	133	6%	130	6%

[2] Certain biases may exist on online panels given the nature of the methodology (e.g. panelists may be higher internet users). In order to mitigate any bias, Yonder conducted an offline CATI calibration exercise to obtain the most up-to-date and accurate data for time spent online per day, device usage, and VSP usage. Weighting profiles were then moderated using a combination of this offline exercise and data on the known proportion of each age group that use the internet, taken from the ONS.

ABC1	1,195	57%	1,186	57%
C2DE	890	42%	899	43%
White	1,835	88%	1,813	86%
MEG	244	12%	266	13%

Significance Testing

Significance testing for the Online Scams and Fraud research has consistently been applied at 95%.

Guide to Statistical Reliability

The variation between the sample results and the “true” values (the findings that would have been obtained if everyone had been interviewed) can be predicted from the sample sizes on which the results are based, and on the number of times that a particular answer is given. The confidence with which we can make this prediction is calculated at the 95% that is, the chances are 95 in 100 that the “true” values will fall within a specified range. However, as the sample is weighted, we need to use the effective sample size (ESS) rather than actual sample size to judge the accuracy of results.

The following table compares ESS and actual samples for some of the main groups within the main sample.

TOTAL	ACTUAL	ESS
	2,097	1,999
GENDER: Male	1,122	1,070
GENDER: Female	964	934
AGE: 18-24	162	161
AGE: 25-34	384	382
AGE: 35-44	382	373
AGE: 45-54	385	381
AGE: 55-64	361	353
AGE: 65-74	290	286
AGE: 75+	133	128
SEG: AB	552	522
SEG: C1	643	615
SEG: C2	456	441
SEG: DE	434	416

The table below illustrates the required ranges for different sample sizes and percentage results at the "95% confidence interval".

Approximate sampling tolerances applicable to percentages at or near these levels

Effective sample size		10% or 90%	20% or 80%	30% or 70%	40% or 60%	50%
		±	±	±	±	±
TOTAL	1,999	1.3%	1.8%	2.0%	2.1%	2.2%
Male	1,070	1.8%	2.4%	2.7%	2.9%	3.0%
Female	934	1.9%	2.6%	2.9%	3.1%	3.2%
18-24	161	4.6%	6.2%	7.1%	7.6%	7.7%
25-34	382	3.0%	4.0%	4.6%	4.9%	5.0%
35-44	373	3.0%	4.1%	4.7%	5.0%	5.1%
45-54	381	3.0%	4.0%	4.6%	4.9%	5.0%
55-64	353	3.1%	4.2%	4.8%	5.1%	5.2%
65-74	286	3.5%	4.6%	5.3%	5.7%	5.8%
75+	128	5.2%	6.9%	7.9%	8.5%	8.7%
ABC1	1,135	1.7%	2.3%	2.7%	2.9%	2.9%
C2DE	853	2.0%	2.7%	3.1%	3.3%	3.4%
White	1,753	1.4%	1.9%	2.1%	2.3%	2.3%
MEG	232	3.9%	5.1%	5.9%	6.3%	6.4%

For example, if 30% or 70% of a sample of 1,999 gives a particular answer, the chances are 95 in 100 that the "true" value will fall within the range of +/- 2.0 percentage points from the sample results.

When results are compared between separate groups within a sample (e.g. male/female), there may be a difference between those groups. The difference may be a "real" difference between those groups, or it may occur by chance (because not everyone in the population has been interviewed). To test if the difference is a real one – i.e. if it is "statistically significant" – we again have to know the size of the samples, the percentages giving a certain answer and the degree of confidence chosen. If we assume "95% confidence interval", the difference between two sample results must be greater than the values given in the table below to be significant.[3]

Differences required for significant at or near these percentages

Effective sample sizes being compared	10% or 90%	20% or 80%	30% or 70%	40% or 60%	50%
	±	±	±	±	±

[3] It is important to note that these numbers are estimates. Further testing should be carried out on individual examples to understand whether differences are significant.

GENDER: Male v Female (1,070 v 934)	2.90%	3.60%	4.10%	4.40%	4.40%
AGE: Young (18-34) v Older (55+) (517 v 764)	3.60%	4.60%	5.20%	5.50%	5.60%
Children in Household v No children in household (555 v 1,443)	3.20%	4.10%	4.60%	4.90%	4.90%

Types of online scams and fraud

In the survey, we asked respondents which online scams or fraud they have ever experienced (Q6a) and which one was the most recently experienced (Q6b) in order to gain detailed insights into their last journey. Below we present the list of online scams or fraud and the descriptions that were presented to the respondents. We also list the number of those who last experienced each particular scam or fraud. We only reported on the scams or fraud with bases of 50 and upwards.

Type of scam or fraud last experienced	Description presented at Q6a	Unweighted sample size based on Q6b
Counterfeit goods scam	Counterfeit goods (e.g. fake designer brand clothes, accessories, perfumes, pirated copies of DVDs and computer games), often found at auctions and web marketplaces, where you can't check if the products are genuine until the item has been delivered	139
Investment, pension or 'get rich quick' scam	Fraudsters often present themselves as a trustworthy institution or advisor to pressurise you to invest money, or by luring with returns that are too good/quick to be true. They may present legitimate sounding investment opportunities such as energy firms, the foreign exchange market, or cryptocurrencies	131
Computer software service fraud or ransomware scam	Fraudsters use computer techniques to disable your	118

	computer's normal functioning, sometimes unknowingly to you, to steal your money or personal information	
Impersonation fraud	Fraudsters pretend to be from a legitimate organisation (e.g. a financial institution, the NHS, lottery institution, solicitors, government officials) and request a payment or information from you	112
Romance or dating scam	Fraudsters pretend to be someone else or lie to gain your affection and trust, and eventually ask for your money or financial information to purchase goods and services	103
Identity fraud	Fraudsters pretend to be you by accessing information about your identity (e.g. name, date of birth, current or previous addresses) and use it to obtain goods or services without your permission	75*
Health or medical scam	Health products or medication that are described as alternative forms of medical cures, or you believe are exactly the same as another legitimate brand of medication at a lower price. You may have seen advertisements promising miracle results, or you are allowed to make a purchase without a valid prescription	44**
Fake employment scam	Job advertisements that claim you can make a lot of money with little time and effort. You may be required to buy a starter kit, tools or goods that are worthless	41**

Holiday scam	Holidays advertised online (e.g. using social media) that are fake or misrepresented	33**
Psychic or clairvoyant scam	Fraudsters approach you to say they have seen something special in your future and ask for money in order to provide you with a full report about it. They may ask forcefully or may threaten to invoke bad luck if you refuse	32**
Money mule recruitment or money laundering	Fraudsters recruit people as money mules to transfer illegally obtained money between different bank accounts, sometimes internationally	28**

Source: Online Scams and Fraud Survey 2022

Q6a. Have you ever experienced the following type of online fraud or scam in your lifetime?

Base: All respondents who have engaged with online fraud or scams (958)

Q6b. Which of the following best describes your last experience?

Base: All respondents who have experienced online fraud or scams (893)

Caution for the bases flagged as small and very small***

NET definitions featured in the published tables

Certain subgroups within the sample were grouped together to aid analysis and are featured alongside this report in the published data tables. The definitions of these so-called NETs are as follows:

Category	Question	NET	Definition
Type of suspicious content	Q2. Thinking about the suspicious content you have encountered or seen online, what made you think it might have been a fraud or scam when you first saw it?	Lack of familiarity	Codes 1-2 at Q2
		Bad design/content	Codes 3-5 at Q2
		Lack of support from others	Codes 6-8 and 13 at Q2
		Suspicious communication	Codes 9-10 at Q2
		Suspicious information	Codes 11-12 at Q2
Frequency of encountering	Q3. In general, how often do you find yourself encountering	Frequently	Codes 1-2 at Q3

Category	Question	NET	Definition
suspicious content	or seeing content online that you suspect to be a fraud or scam?	Rarely	Codes 4-5 at Q3
Ever engaged with online fraud or scams	Q5. Have you ever personally been drawn into engaging with fraud or scams that began online? You may not have lost money in the end but you may have, for example, clicked on an advertisement, followed specific instructions, or replied to a message.	Yes	Codes 1-4 at Q5
		Total yes recalling the number of incidents	Codes1-3 at Q5
Type of online service or platform the online fraud or scam was first encountered on	Q9. Which of the following best describes the type of online service or platform you were using when you first encountered the fraud or scam you last experienced?	Social media	Codes 2-4 at Q9
		Websites and apps	Codes 9-11 or 14-16 at Q9
Type of content through which the online fraud or scam was first encountered through	Q11. Which of the following best describes the type of content through which you first encountered the fraud or scam you last experienced?	User-generated content	Codes 1-2 at Q11
		Influencer-generated content	Codes 3-4 at Q11
		Targeted message	Codes 5-6 at Q11
		Advertisements	Codes 7-9 at Q11
Type of communication channel used to interact with the fraudster	Q14. Which one of the following best describes the communication channel the fraudster used to interact with you first, if at all, after you had encountered/seen the fraud or scam?	Online	Codes 2-12 at Q14
		Offline	Codes 13-15 at Q14
Type of online communication used	Q15. You selected [show selected code at Q14], what method did the fraudster use to communicate with you first?	Messaging	Codes 1-3 at Q15
		Video calling	Codes 4-5 at Q15
Length of time before realising it	Q18. How long did it take from engaging with the content (e.g.	Short term (within a month)	Codes 1-6 at Q18

Category	Question	NET	Definition
was a fraud or scam	clicked on the advertisement, followed specific instructions, replied to a message) for you to realise it was a fraud or scam?	Medium term (1-3 months)	Codes 7-8 at Q18
		Long term	Code 9 at Q18
Money lost	Q19. Sometimes people end up losing money through fraud and scams, for example, thinking they are investing in a scheme that will make them money or sending money to someone they met on a dating app to pay for an operation or a debt which doesn't actually exist. How much money did you lose in this instance, if any?	Yes	Codes 2-6 at Q19
		£1-£99	Code 2 at Q19
		£100-£999	Code 3 at Q19
		£1,000-£9,999	Code 4 at Q19
		£10,000-£19,999	Code 5 at Q19
		£20,000 or above	Code 6 at Q19
		I didn’t lose any money	Code 1 at Q19
		Can’t remember/Prefer not to say	Codes 7-8 at Q19
Ways the payments were made	Q20. How did you make the payment(s)? Please select all that apply.	Cash transfer	Codes 1-4 or 9 at Q20
		Card payment	Codes 7-8 at Q20
Action taken	Q21. When you realised you had experienced a scam or fraud, which of the following action(s) did you take, if any?	Yes	Codes 1-15 at Q21
		No	Code 16 at Q21
		Reported	Codes 1-6 at Q21
		Shared my experience	Codes 8-10 at Q21
		Avoid future contact	Codes 12-14 at Q21
Reasons behind no action taken	Q22. You mentioned you did not take any action, why not? Please select all that apply.	Didn’t think it was that serious	Codes 1-2 at Q22
Results of reporting the incident	Q23. You mentioned you reported the incident. What happened as a result? Please select all that apply.	Received a response	Codes 3-4 at Q23
		Reimbursed	Codes 6-7 at Q23

Category	Question	NET	Definition
Types of measures to prevent others from engaging with online fraud or scams	Q26. Which of the following measure(s) do you think could stop people from engaging with the fraud or scam you last experienced? Please select all that apply	Online alerts	Codes 1-6 at Q26
		Offline promotion	Codes 7-12 and 16 at Q26
		Online promotion	Codes 13-15 at Q26
Levels of agreement with statements	Q27. On a scale of 1 to 10, where 1 means 'strongly disagree' and 10 means 'strongly agree', to what extent do you agree with each of the following statements describing you after the online fraud or scam you last experienced?	Agree	Codes 7-10 at Q27
		Neither	Codes 5-6 at Q27
		Disagree	Codes 1-4 at Q27

Qualitative Research

Introduction

Yonder conducted 32 interviews with victims to one of a number of types of scams or fraud[4], with 5 interviews each on money laundering scams[5], romance scams, investment scams, counterfeit goods scams, ransomware scams, and impersonation scams, and 2 interviews on cryptocurrency scams[6]. The qualitative research also involved speaking to 5 experts who have supported victims of online scams and fraud. Interviews were conducted online using Zoom and lasted around 60 minutes each and took place between 12th October – 11th November 2022.

Recruitment

All participants were recruited using Free Find techniques[7] as we were unable to book interviews by recontacting participants who had given their consent to be contacted again for follow-ups from the quantitative phase.

Final sample quota:

- 5 x victims of money laundering / money mules
- 5 x victims of romance/dating scams
- 5 x investment/pension/get rich scams
- 5 x counterfeit goods
- 5 x ransomware
- 5 x impersonation
- 2 x cryptocurrency

Additionally, the sample aimed to recruit:

- Victim impact and amount of money lost to fall out naturally
- Mix of platforms the scam was initiated from
- Mix of gender, age and region

5 x Experts of supporting victims / perpetrators of online scams

- 2 x psychologists who support victims of online scams and perpetrators
- 1 x psychologist who has experience with victims of romance scams
- 1 x bereavement counsellor
- 1 x psychologist who has experience of working with a victim of an online scam

[4] The definition of the scams and fraud can be found in the recruitment screener in Appendix A.
[5] Victims of money laundering scams were recruited based on self-reports of their past experiences and they would have qualified if they believed they may have been involved in this type of scam or fraud, even if there was no evidence of 'classic' money laundering (e.g. people were not asked to accept money into their account or move it).
[6] Cryptocurrency scams was added as a category of interest because a notable number of open text answers in the quantitative survey mentioned this.
[7] Free-find recruitment involves specialist qualitative recruiters using approaches such as online, telephone and in-person approaches to find participants for research projects from outside a specific panel.

Appendix

Appendix A – Quantitative questionnaire

Introduction

Today we would like to ask you some questions about your online experiences and your views on online fraud and scams, such as financial and dating scams. **This survey does not include fraud and scams that originate from texts or calls, we are only interested in instances when it began online, such as when you received an email, saw an online advertisement, or received a message on social media.** Some questions in this survey may potentially be upsetting, for example, recalling an experience of losing money. Your participation is voluntary and you have the right to withdraw at any point should you wish to. Your honest answers will help us to better understand adult experiences of online life in the UK.

Are you happy to take part?

1. Yes
2. No [SCREEN OUT]

Scale of fraud (general)

ASK ALL

Q1. Thinking about the time you spend online, for example, using social media and messaging, watching videos, playing games and searching for information online - this could be using a mobile phone, laptop, tablet (like an iPad), computer or games console:

Have you ever encountered or seen anything suspicious online which you thought might be a fraud or scam?

A fraud or a scam involves someone wrongfully deceiving you with the intention of taking your money or other valuable possessions. It may involve them lying to you with made-up, false information, or deliberately hiding certain facts from you. They may promise to provide you with certain rewards, goods or services which they don't actually deliver, or something might be delivered but it is not as described.

[SINGLE CODE]

1. Yes
2. No [SKIP TO Q4]
3. Don't know [SCREEN OUT]
4. Can't remember [SCREEN OUT]

ASK IF Q1 = CODE 1, YES

Q2. Thinking about the suspicious content you have encountered or seen online, what made you think it might have been a fraud or scam when you first saw it? Please select all that apply.

[MULTICODE, RANDOMISE STATEMENTS]

1. Didn't know the person who posted it/ contacted me
2. The company/ organisation was not familiar
3. No or poor-quality logo
4. Suspicious imagery (e.g. photos of a luxurious lifestyle, money)
5. Poorly written content (e.g. wrong spelling/ poor English)

6. Not endorsed by a credible person
7. Not endorsed by a credible organisation
8. No or few testimonials/ reviews
9. Contact with the fraudster was suspicious (e.g. how they spoke/ didn't use a call centre)
10. The fraudster expressed a strong personal/ emotional attachment too soon
11. Inconsistent profile information (e.g. photos/ bio of the supposedly same person didn't match)
12. Offered rewards which seemed 'too good to be true' (e.g. promise of free money, unrealistically high return on investment, extremely low price for a product/ service)
13. Comments from other users voicing suspicion
14. Other (please specify)
15. Don't know
16. Can't remember

ASK IF Q1 = CODE 1, YES

Q3. In general, how often do you find yourself encountering or seeing content online that you suspect to be a fraud or scam?

[SINGLE CODE]

1. Very frequently – almost every time when I go online
2. Frequently – more than half the time when I go online
3. Sometimes – about half the time when I go online
4. Rarely – less than half the time when I go online but more than a handful of occasions
5. Very rarely – only a handful of occasions
6. Don't know
7. Prefer not to say

ASK ALL

Q4. Do you know anyone personally who has fallen victim to a fraud or scam that began online?

[SINGLE CODE]

1. Yes
2. No
3. Don't know
4. Prefer not to say

ASK ALL

Q5. Have you ever personally been drawn into engaging with fraud or scams that began online? You may not have lost money in the end but you may have, for example, clicked on an advertisement, followed specific instructions, or replied to a message.

[SINGLE CODE]

1. Yes, just once
2. Yes, 2-3 times
3. Yes, 4 times or more
4. Yes, but I can't remember how many times

5. Never [TAKE TO Q25 AND Q26]
6. Can't remember [TAKE TO Q25 AND Q26]
7. Prefer not to say [TAKE TO Q25 AND Q26]

Type/ nature of fraud (actual experience)

ASK IF Q5 = CODE 1-4, YES

Q6.Intro. Thank you for your time so far, please note that the following section contains questions about your experiences of online scams or fraud.

ASK IF Q5 = CODE 1-4, YES

Q6a. Have you ever experienced the following type of online fraud or scam in your lifetime? ***You will be shown different types of scam or fraud individually, with options to select.*** [SINGLE RESPONSE PER SCAM/FRAUD, RANDOMISE ORDER]

1. **Romance or dating scam**
   Fraudsters pretend to be someone else or lie to gain your affection and trust, and eventually ask for your money or financial information to purchase goods and services.
2. **Investment, pension or 'get rich quick' scam**
   Fraudsters often present themselves as a trustworthy institution or advisor to pressurise you to invest money, or by luring with returns that are too good/ quick to be true. They may present legitimate sounding investment opportunities such as energy firms, the foreign exchange market, or cryptocurrencies.
3. **Money mule recruitment or money laundering**
   Fraudsters recruit people as money mules to transfer illegally obtained money between different bank accounts, sometimes internationally.
4. **Impersonation fraud**
   Fraudsters pretend to be from a legitimate organisation (e.g. a financial institution, the NHS, lottery institution, solicitors, government officials) and request a payment or information from you.
5. **Identity fraud**
   Fraudsters pretend to be you by accessing information about your identity (e.g. name, date of birth, current or previous addresses) and use it to obtain goods or services without your permission.
6. **Computer software service fraud or ransomware scam**
   Fraudsters use computer techniques to disable your computer's normal functioning, sometimes unknowingly to you, to steal your money or personal information.
7. **Psychic or clairvoyant scam**
   Fraudsters approach you to say they have seen something special in your future and ask for money in order to provide you with a full report about it. They may ask forcefully or may threaten to invoke bad luck if you refuse.
8. **Holiday scam**
   Holidays advertised online (e.g. using social media) that are fake or misrepresented.
9. **Health or medical scam**
   Health products or medication that are described as alternative forms of medical cures, or you believe are exactly the same as another legitimate brand of medication at a lower price. You may have seen advertisements promising miracle results, or you are allowed to make a purchase without a valid prescription.
10. **Counterfeit goods scam**
    Counterfeit goods (e.g. fake designer brand clothes, accessories, perfumes, pirated

copies of DVDs and computer games), often found at auctions and web marketplaces, where you can't check if the products are genuine until the item has been delivered.

11. **Fake employment scam**
    Job advertisements that claim you can make a lot of money with little time and effort. You may be required to buy a starter kit, tools or goods that are worthless.

OPTIONS:

1. Yes
2. No [IF SELECTED NO FOR ALL CODES, PLEASE ROUTE TO Q25 AND Q26]
3. Don't know [IF SELECTED DON'T KNOW FOR ALL CODES, PLEASE ROUTE TO Q25 AND Q26]
4. Can't remember [IF SELECTED CAN'T REMEMBER FOR ALL CODES, PLEASE ROUTE TO Q25 AND Q26]
   Prefer not to say [IF SELECTED CAN'T REMEMBER FOR ALL CODES, PLEASE ROUTE TO Q25 AND Q26]

ASK IF Q6A = YES TO ANY OPTIONS, 2 CODES OR MORE; IF ANSWERED ONLY ONE CODE AT Q6A, AUTOFILL

Q6b. Which of the following best describes your last experience?

[PIPE IN ANSWERS SELECTED AT Q6a without descriptions, title only – ANSWER SINGLE CODE ONLY]

- Other (please specify)

ASK IF Q6B IS CODE 2 - INVESTMENT, PENSION OR 'GET RICH QUICK' SCAM

Q7. You said you had experienced an investment scam. Do you know what kind of investment scam it was?

[SINGLE CODE]

1. **Pension scam**
   Fraudsters make false claims to gain your trust (e.g. claiming they are FCA-authorised or are not subject to FCA's approval because they are not providing the advice themselves) and typically design attractive offers to persuade you to transfer your pension to them, or to release funds from it. Once the funds are released and transferred, your money is stolen and no investment is made.
2. **Boiler room scam**
   Share and bond scams are often run from 'boiler rooms' where fraudsters cold-call investors offering you worthless, overpriced or even non-existent shares or bonds. Boiler rooms use increasingly sophisticated tactics to approach investors, offering to buy or sell shares in a way that will bring you a huge return.
3. **Pyramid or Ponzi scheme**
   Fraudsters offer great-sounding profits with little or no risk and asks you to pay a fee to join the scheme.
4. **Money flipping scam**
   Fraudsters reach out on social media offering a quick way to double or triple your money in a small investment. Once you have transferred the money, the scammer never responds. They often lure victims with images of money or adverts with language such as 'double or triple your £20 investment in minutes!"
5. **Other (please specify)**

6. **Don’t know**
7. **Can’t remember**
8. **Prefer not to say**

ASK IF ANSWERED Q6B
Q8. Sometimes, fraudsters or scammers may try to steal people’s money or valuable possessions in different ways. For example, a victim of a romance or dating scam was requested to transfer gift money to their lover as well as to share their personal details. The personal details were later used to obtain goods or services without the victim’s permission. This incident is best described as a romance or dating scam, but it also included elements of an identity fraud.

Did your last experience involve any other type(s) of fraud or scam apart from [CODE 6b]? Please select all that apply.
[MULTI CODE]

1. [Repeat all codes at Q6a except the one selected at Q6b]
2. No, it was only the one type of fraud/ scam I selected previously [EXCLUSIVE]
3. Don’t know [EXCLUSIVE]

ASK IF Q6a = CODE 1, YES
Q9. Which of the following best describes the type of online service or platform you were using when you first encountered the fraud or scam you last experienced?
[SINGLE CODE, RANDOMISE ROWS]

1. A video-sharing service (e.g. YouTube, TikTok, Vimeo)
2. My newsfeed on social media (e.g. Facebook, Twitter, Instagram, Snapchat)
3. A company page/ account on social media (e.g. a business profile on Facebook, Twitter, Instagram, Snapchat)
4. An individual’s page/ account on social media (e.g. a verified user or your friend’s profile on Facebook, Twitter, Instagram, Snapchat)
5. An online forum (e.g. Reddit, Mumsnet, The Student Room forum)
6. Livestreaming service (e.g. Twitch, Facebook Live, YouTube Gaming)
7. A search engine (e.g. Google, Yahoo, Bing)
8. An instant messenger (e.g. Facebook Messenger, WhatsApp, Skype, Discord)
9. A news website or app (e.g. BBC News, The Guardian, Daily Mail Online)
10. A gaming website or app (e.g. PlayStation Network, Nintendo Online, Xbox Live, Roblox)
11. A Q&A website or app (e.g. Quora, Yahoo! Answers)
12. Email
13. An online blog (e.g. WordPress, Bloglovin’)
14. A shopping website or app (e.g. Amazon, eBay, Gumtree)
15. A dating website or app (e.g. Match, Tinder, Bumble)
16. A standalone company website
17. Other (please specify)
18. Can’t remember
19. Prefer not to say

ASK IF Q6a = CODE 1, YES

Q10. What device were you using to access the internet at the time?

[SINGLE CODE, RANDOMISE ROWS]

1. Smartphone
2. Tablet
3. Computer (laptop or desktop)
4. Games console or handheld games player
5. Smart TV
6. Smart speaker
7. Other (please specify)
8. Can't remember
9. Prefer not to say

ASK IF Q6a = CODE 1, YES

Q11. Which of the following best describes the type of content through which you first encountered the fraud or scam you last experienced?

[SINGLE CODE, RANDOMISE ROWS, GROUP CODES 1+2, 3+4]

1. A user-generated post (e.g. an article written by ordinary internet users)
2. A user-generated video (filmed by ordinary internet users)
3. An influencer-generated post (e.g. an article written by an influencer, someone who built a reputation for their knowledge and expertise on a specific topic and generates followings of enthusiastic, engaged people)
4. An influencer-generated video (filmed by an influencer, someone who built a reputation for their knowledge and expertise on a specific topic and generates followings of enthusiastic, engaged people)
5. A direct message from an individual
6. A mass message posted to a group (e.g. on a social media page or in a messaging group)
7. An advertisement before a video played
8. An advertisement integrated in my social media (e.g. within or at the side of my newsfeed)
9. A pop-up advertisement on a webpage or app
10. A search result or listing
11. Other (please specify)
12. Can't remember
13. Prefer not to say

ASK IF Q11 IS CODE 1-4, 6 OR 10

Q12. You selected [show selected code at Q11: 1-4 or 10], were you aware if it was sponsored or promoted? By this we mean content that has been paid for to enhance visibility and may be labelled as 'Ad', 'promoted' or 'sponsored'.

[SINGLE CODE]

1. Yes – the content was promoted
2. No – the content was not promoted
3. Don't know
4. Can't remember
5. Prefer not to say

ASK IF Q11 IS CODE 1-2 OR 5-6

Q13. You selected [show selected code at Q11], was it shared or sent by someone you knew?

[SINGLE CODE]

1. Yes – it was from a friend or connection of mine
2. No – it was from a user I didn't know
3. Don't know
4. Can't remember
5. Prefer not to say

ASK IF Q6a = CODE 1, YES

Q14. Which one of the following best describes the communication channel the fraudster used to interact with you first, if at all, after you had encountered/ seen the fraud or scam?

[SINGLE CODE, RANDOMISE STATEMENTS]

1. I didn't interact with the fraudster at all [EXCLUSIVE]
2. A video-sharing service (e.g. YouTube, TikTok, Vimeo)
3. Social media (e.g. Facebook, Twitter, Instagram, Snapchat)
4. An online forum (e.g. Reddit, Mumsnet, The Student Room forum)
5. Livestreaming service (e.g. Twitch, Facebook Live, YouTube Gaming)
6. An instant messenger (e.g. Facebook Messenger, WhatsApp, Skype, Discord)
7. A gaming website or app (e.g. PlayStation Network, Nintendo Online, Xbox Live, Roblox)
8. A Q&A website or app (e.g. Quora, Yahoo! Answers)
9. Email
10. An online blog (e.g. WordPress, Bloglovin')
11. A shopping website or app (e.g. Amazon, eBay, Gumtree)
12. A dating website or app (e.g. Match, Tinder, Bumble)
13. Via SMS/ text
14. By Phone
15. By Post/ letter
16. Other (please specify)
17. Can't remember
18. Prefer not to say

ASK IF Q14 IS CODE 2-8 OR 10-12

Q15. You selected [show selected code at Q14], what method did the fraudster use to communicate with you first?

[SINGLE CODE]

1. One-to-one messaging in private
2. Group messaging in private
3. Messaging/ commenting in public
4. Video calling in private
5. Video calling in public e.g. webinars, conferences and livestreams
6. Other (please specify)
7. Can't remember [EXCLUSIVE]
8. Prefer not to say [EXCLUSIVE]

ASK ALL WHO AT Q14 CODES 2-16

Q16. Did the fraudster use any other communication channels to interact with you?

[SINGLE CODE]

1. No, we only communicated on one channel [SKIP TO Q18]
2. Yes, we communicated on multiple, different channels
3. Can't remember [EXCLUSIVE]
4. Prefer not to say [EXCLUSIVE]

ASK IF Q16 IS CODE 2 - YES

Q17. Which of the following additional communication channel(s) did the fraudster use to interact with you?
Please select all that apply.

[MULTICODE]

1. [Show codes 2-15 at Q14 except the one selected at Q14]
2. In-person meeting
3. Other (please specify)
4. Can't remember [EXCLUSIVE]
5. Prefer not to say [EXCLUSIVE]

ASK IF Q6a = CODE 1, YES

Q18. How long did it take from engaging with the content (e.g. clicked on the advertisement, followed specific instructions, replied to a message) for you to realise it was a fraud or scam?

[SINGLE CODE]

1. Straight away
2. Hours
3. A few days
4. Exactly a week
5. 1-2 weeks
6. 2-4 weeks
7. Exactly a month
8. 1-3 months
9. Longer than 3 months
10. Other (please specify)
11. Can't remember [EXCLUSIVE]
12. Prefer not to say [EXCLUSIVE]

ASK IF Q6a = CODE 1, YES

Q19. Sometimes people end up losing money through fraud and scams, for example, thinking they are investing in a scheme that will make them money or sending money to someone they met on a dating app to pay for an operation or a debt which doesn't actually exist. How much money did you lose in this instance, if any?

[SINGLE CODE]

1. I didn't lose any money [SKIP TO Q21]
2. £1 - £99
3. £100 - £999
4. £1,000 - £9,999

5. £10,000 - £19,999
6. £20,000 or above
7. Can't remember [SKIP TO Q21]
8. Prefer not to say [SKIP TO Q21]

ASK IF Q19 CODES 2-6
Q20. How did you make the payment(s)?
Please select all that apply.
[MULTICODE]

1. Single payment of a digital cash transfer (e.g. bank transfer, PayPal, Cash App, Western Union)
2. Single payment of a physical cash transfer
3. A series of payments over digital cash transfer (e.g. bank transfer, PayPal, Cash App, Western Union)
4. A series of physical cash transfers
5. Gift(s) to the fraudster (e.g. gift cards, digital stickers)
6. Transfer of cryptocurrencies
7. Debit card payment(s)
8. Credit card payment(s)
9. Set up a direct debit
10. Other (please specify)
11. Can't remember [EXCLUSIVE]
12. Prefer not to say [EXCLUSIVE]

Reporting of fraud/ mitigation

ASK IF Q6a = CODE 1, YES
Q21. When you realised you had experienced a scam or fraud, which of the following action(s) did you take, if any?
Please select all that apply.
[MULTICODE, RANDOMISE IN GROUPS 1-7; 8-11; 12-14; CODES 15-19 ANCHORED]

1. Reported it to the platform/ service where I encountered the scam (e.g. clicked the report/ flag button, marked as junk)
2. Reported it to Action Fraud
3. Reported it to the police
4. Reported it to Citizens' Advice
5. Reported it to my bank, credit card company, building society or pension provider
6. Reported it to a regulator (e.g. Ofcom, Financial Conduct Authority, Advertising Standards Authority)
7. Started to report it but failed to finish the process
8. Shared my experience with a friend or family member
9. Shared my experience on social media
10. Shared my experience on a ratings site (e.g. Trustpilot)
11. Searched for more information/ other people's similar experiences
12. I use the platform/ service less
13. Blocked the contact/ account
14. Closed my account/ left the service
15. Other (please specify)
16. I didn't take any action [EXCLUSIVE]

17. Can’t remember [EXCLUSIVE]
18. Prefer not to say [EXCLUSIVE]

ASK IF Q21 IS CODE 16 - I DIDN’T TAKE ANY ACTION
Q22. You mentioned you did not take any action, why not?
Please select all that apply.
[MULTI CODE, RANDOMISE ROWS]

1. I didn’t consider it to be harmful to others
2. I didn’t consider it bad enough to do something about
3. I didn’t see the need to do anything
4. I didn’t know what to do/ who to inform
5. I didn’t want to get into trouble for reporting it
6. I didn’t want to visit the platform/ service again after experiencing it
7. I thought somebody else would report it
8. I asked somebody else to report it
9. I didn’t think it would help/ make a difference/ be acted on
10. I wasn’t directly impacted
11. I couldn’t be bothered
12. I thought the platform/ service would remove the content themselves/ resolve the problem
13. I thought it might make it worse
14. I didn’t have time
15. I was embarrassed
16. Other (please specify)
17. Can’t remember [EXCLUSIVE]
18. Prefer not to say [EXCLUSIVE]

ASK IF Q21 IS CODE 1-15
Q23. You mentioned you reported the incident. What happened as a result?
Please select all that apply.
[MULTICODE]

1. Nothing [EXCLUSIVE]
2. The content was removed
3. I got a response to confirm my case is being investigated
4. I got a response to confirm my case won’t be investigated
5. I was asked to provide further information
6. I got all my money back
7. I got some of my money back
8. Something else (please specify)
9. Can’t remember [EXCLUSIVE]
10. Prefer not to say [EXCLUSIVE]

ASK IF Q6a = CODE 1, YES
Q24a. Since your last experience of a scam or fraud, have you noticed a higher than usual amount of suspicious content on the sites you visit and services you use?
[SINGLE CODE]

1. Yes, I have noticed more suspicious content
2. No
3. Don’t know
4. Prefer not to say

ASK IF Q6a = CODE 1, YES

Q24b. Since your last experience of a scam or fraud, have you been contacted more often by strangers online or offline?

[SINGLE CODE]

1. Yes, I have been contacted more often by strangers
2. No
3. Don’t know
4. Prefer not to say

ASK ALL, ROUTING BACK IN THOSE WHO SAY CODES 5-7 AT Q5

Q25. Whose responsibility do you think it is to take action against fraud and scams online? Please select all that apply.

[MULTI CODE, RANDOMISE]

1. The platform/ service itself
2. Action Fraud
3. The police
4. Ofcom
5. Financial Conduct Authority
6. Advertising Standards Authority
7. Users themselves, when they see fraudulent content or activity
8. My bank, credit card company, building society or pension provider
9. Other (please specify)
10. Don’t know
11. Prefer not to say

ASK ALL, ROUTING BACK IN THOSE WHO SAY CODES 5-7 AT Q5

Q26. Which of the following measure(s) do you think could stop people from engaging with the fraud or scam you last experienced?
Please select all that apply

[MULTICODE, RANDOMISE]

1. A warning from an authority that the content may be suspicious
2. A warning/ pop-up message from the platform to notify me when a link will take me to another site or service
3. An occasional pop-up warning on the platform to remain alert for fraudulent content
4. A warning from the platform that the same direct message has been forwarded many times
5. A warning from the platform that the content or message came from an unverified user
6. Make the content more obvious that it was promoted/ sponsored
7. Printed leaflets on advice about keeping safe online
8. Posters in bus shelters and on billboards etc. on advice about keeping safe online
9. Advertisements in magazines on advice about keeping safe online

10. Advertisements in newspapers on advice about keeping safe online
11. Articles in magazines on advice about keeping safe online
12. Articles in newspapers on advice about keeping safe online
13. Online advice about keeping safe online, specifically when I search for such information
14. Social media posts on advice about keeping safe online
15. Online video advice about keeping safe online
16. Advice about keeping safe online on television documentaries/ factual programmes (e.g. Rip-off Britain)
17. Texts from my bank, credit card company, building society or pension provider
18. Emails from my bank, credit card company, building society or pension provider
19. Other (please specify)
20. Don't know
21. Prefer not to say

Consumer Impact

You are almost at the end of the survey. The following section contains questions about how your last experience of online fraud or scam affected you personally, so please remember you do not need to answer and have the option to exit the survey now should you wish to.

ASK IF Q6a = CODE 1, YES

Q27. On a scale of 1 to 10, where 1 means 'strongly disagree' and 10 means 'strongly agree', to what extent do you agree with each of the following statements describing you after the online fraud or scam you last experienced?

[SINGLE CODE PER ROW]

[TOP BREAK]

1. 1 – Strongly disagree
2. 2
3. 3
4. 4
5. 5
6. 6
7. 7
8. 8
9. 9
10. 10 – Strongly agree
11. Don't know
12. Prefer not to say

[DOWN BREAK, RANDOMISE ROWS]

a) It had an immediate negative impact on my mental wellbeing
b) It had a long-term negative impact on my mental wellbeing
c) I now spend less time online overall
d) I have become more aware of suspicious content/ communications online
e) I have become more confident in identifying potential fraud or scams online
f) I feel better equipped to protect myself from future fraud or scams online

[SHOW TO ALL]
This is the end of the survey. Thank you so much for your time and comments, we greatly appreciate it.

We understand some of the questions asked today may have raised concerns for some people, if you would like to speak to anyone about what you might be feeling or have experienced, below are some organisations that can offer help and advice:

Keeping yourself safe online

UK Council for Internet Safety, https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Stop Online Abuse, https://www.stoponlineabuse.org.uk/
Action Fraud, https://www.actionfraud.police.uk/contact-us
Financial Conduct Authority, https://www.fca.org.uk/consumers/report-scam-us
Which? https://www.which.co.uk/consumer-rights/scams
Support and advice
Samaritans, https://www.samaritans.org/
Citizens Advice, https://www.citizensadvice.org.uk/
Mind, https://www.mind.org.uk/information-support/helplines/
Thanks again, your contribution today will help to promote safer, more positive online experiences.

Appendix B – Recruitment screener for victims of scams and fraud

Recruitment Screener
Reference: Scams and Frauds
Yonder Consulting - Ofcom

Qualitative recruitment spec and screener

- Recruiting 32 respondents to take part in an hour IDI (either online/telephone or f2f); this screener is for consumers.
- Our preference is to do them in home, in person, but we will be responsive to whatever participants prefer.
- £80 incentive paid either through cash, bank transfer or voucher (however participants prefer).

Key criteria

- We want this research to be inclusive, and we're especially keen to understand the views of vulnerable people. However, if potential participants are unable to take part effectively or would potentially be distressed or upset by doing so, we should exclude these individuals from the study.
- All participants to have experienced online fraud or scams

Sample Frame

• 5 x IDIs with victims of romance/dating scams • 5 x investment/pension/get rich scams (recruit at least one who lost £1k-9.9k and at least one £10k+) • 5 x counterfeit goods • 5 x ransomware • 5 x money laundering/money mule • 5 x impersonation • 2 x cryptocurrency
• Mix of victim impact to fall out naturally • Mix of amount of money lost • Mix of platforms the scam was initiated from • Mix of gender, age and region

Introduction for fresh sample: Good morning/afternoon, I am calling on behalf of Yonder, an independent market research agency, and Ofcom, the communications regulator for the UK, about a research study we are conducting on online scams and fraud and the impact it may have on people. If you go on to be part of the research you will be incentivised for £80 paid by cash, voucher or bank transfer. If you qualify, you will be asked to participate in either a 1:1 Zoom or face-to-face interview. I would like to ask you some questions and, if you are eligible, invite you to participate. The call will take around 5 minutes. Is this a good time to talk?

Introduction for recontact sample: Good morning/afternoon, I am calling on behalf of Yonder, an independent market research agency, and Ofcom, the communications regulator for the UK, about a research study we are conducting on online scams and fraud and the impact it may have on people. I understand that you recently participated in an online survey conducted by Yonder on online scams and fraud.

According to our records, you agreed to be recontacted about participating in a follow-up depth interview to understand the reasons for your responses in more detail and to help us to understand further any concerns about online scamming and fraud. If you go on to be part of the research you will be incentivised for £80 paid by cash, voucher or bank transfer. If you qualify, you will be asked to participate in either a 1:1 Zoom or face-to-face interview. I would like to ask you some questions which you answered in the survey again and, if you are eligible, invite you to participate. The call will take around 5 minutes. Is this a good time to talk?

1. Yes
2. No

1 = Continue and read out text below
2 = Thank and close

For all if agreed to continue with call: Ok, during this call, I will need to ask you for some personal information which will be used to establish if you qualify for this market research. The answers will be shared with Yonder and Ofcom.

We would first like to emphasise that within the research there is no obligation to answer any questions that you don't wish to and that your answers will be kept strictly confidential at all times. If any information about you is used in reporting, it will be anonymised.

You have the right to withdraw your consent to process the information you provide at any time during or after this conversation.

If you qualify, the research project will involve an interview that will focus on your experience on a suspected scam or fraud online and there will be no repercussions as a result of taking part. I will provide you with further information about how the interview will be conducted in an information sheet after this call.

Do you consent to take part in this phone call and the research project on this basis?

1 Yes
2 No

1 = Continue and read out text below
2 = Thank and close

Q1. Have you ever taken part in market research?

1 Yes
2 No

If code 1 continue to Q2, otherwise continue to Q3

Q2. What was the date of your most recent market research?
If less than 6 months ago then please terminate interview

Q3. Do any of your close friends/ family work in any of the following industries?

1. Journalism / Publishing
2. Market Research
3. Government
4. Regulatory body
5. Advertising / PR / Marketing
6. Comms providers (e.g. phone companies, satellite companies and internet service providers)
7. Comms technology providers (e.g. IBM, Microsoft, SAP, Oracle, Cisco)
8. Broadcasters / streaming platforms
9. Social media platforms
10. Online safety technology
11. Other (please specify)

Continue if code 11, all others please thank and close)

Q4. Please record gender
Please recruit a mix

Q5. How old are you?
Please recruit a mix of ages
Screen out if under 18

Q6. Please can you tell us where you live (i.e. your primary residence)?
Recruit a mix of regions

Q7. I am now going to ask you some questions about experiencing a scam or fraud – are you comfortable for us to continue?

1. Yes
2. No

Thank and close on participants who code 2

Q8. Have you ever personally been drawn into engaging with fraud or a scam that began **online**? You may not have lost money in the end but you may have, for example, clicked on an advertisement, followed specific instructions, or replied to a message.

1. Yes, just once
2. Yes, 2-3 times
3. Yes, 4 times or more
4. No, I haven't

Code 1, 2 or 3 = Continue to Q9
Code 4 = Thank and close

Q9. Have you ever experienced a scam or fraud as a result of interacting with content online e.g. dating site / influencer on social media / another user on an online forum?

20. Yes
21. No
22. Not sure

1 = Record type of fraud and continue

2 = Thank and close
3 = Record circumstances of scam and contact research team

Q10. I will now read out a list of different types of scams or fraud, please pick one that you think best describes your most recent experience. If you are not sure what it means, just let me know and I can give you a brief description.

Recruiter to read out and record all that apply. If participant has been scammed more than once, please record which scam they most recently experienced.

12. **Romance or dating scam**
Fraudsters pretend to be someone else or lie to gain your affection and trust, and eventually ask for your money or financial information to purchase goods and services.
13. **Investment, pension or 'get rich quick' scam**
Fraudsters often present themselves as a trustworthy institution or advisor to pressurise you to invest money, or by luring with returns that are too good/ quick to be true. They may present legitimate sounding investment opportunities such as energy firms, the foreign exchange market, or cryptocurrencies.
14. **Money mule recruitment or money laundering**
Fraudsters recruit people as money mules to transfer illegally obtained money between different bank accounts, sometimes internationally.
15. **Cryptocurrency investment scam**
Fraudsters invite or encourage you to invest in fake investments in cryptocurrency that don't really exist.
16. **Impersonation fraud**
Fraudsters pretend to be from a legitimate organisation (e.g. a financial institution, the NHS, lottery institution, solicitors, government officials) and request a payment or information from you.
17. **Identity fraud**
Fraudsters pretend to be you by accessing information about your identity (e.g. name, date of birth, current or previous addresses) and use it to obtain goods or services without your permission.
18. **Computer software service fraud or ransomware scam**
Fraudsters use computer techniques to disable your computer's normal functioning, sometimes unknowingly to you, to steal your money or personal information.
19. **Psychic or clairvoyant scam**
Fraudsters approach you to say they have seen something special in your future and ask for money in order to provide you with a full report about it. They may ask forcefully or may threaten to invoke bad luck if you refuse.
20. **Holiday scam**
Holidays advertised online (e.g. using social media) that are fake or misrepresented.
21. **Health or medical scam**
Health products or medication that are described as alternative forms of medical cures, or you believe are exactly the same as another legitimate brand of medication at a lower price. You may have seen advertisements promising miracle results, or you are allowed to make a purchase without a valid prescription.
22. **Counterfeit goods scam**
Counterfeit goods (e.g. fake designer brand clothes, accessories, perfumes, pirated copies of DVDs and computer games), often found at auctions and web marketplaces, where you can't check if the products are genuine until the item has been delivered.

23. **Fake employment scam**
    Job advertisements that claim you can make a lot of money with little time and effort. You may be required to buy a starter kit, tools or goods that are worthless.

*Close on participants who **only** code 6, 8, 9, 10,or 12*
Recruit to quota

Q11. Sometimes people end up losing money through fraud and scams, for example, thinking they are investing in a scheme that will make them money or sending money to someone they met on a dating app to pay for an operation or a debt which doesn't actually exist. How much money did you lose, if any?

1. I didn't lose any money
2. £1 - £99
3. £100 - £999
4. £1,000 - £9,999
5. £10,000 - £19,999
6. £20,000 or above
7. Can't remember
8. Prefer not to say

Recruit a good mix; we should recruit at least one in the 1k-9.9k bracket and at least one in the 10k+ brackets.
Close on participants who code 1, 7, 8

Q12. When did you realise you had experienced a scam or fraud, what if any action did you take?
Record

Q13. On a scale of 1 to 10, where 1 means 'strongly disagree' and 5 means 'strongly agree', to what extent do you agree with each of the following statements describing you **after** the online fraud or scam you last experienced?

13. 1 – Strongly disagree
14. 2
15. 3
16. 4
17. 5 – Strongly agree
18. Don't know
19. Prefer not to say

Recruiter read out:

1. It had a negative impact on my mental wellbeing
2. I now spend less time online overall
3. I have become more aware of suspicious content/ communications online
4. I have become more confident in identifying potential fraud or scams online

Record and recruit a mix

Q14. If you are selected, how would you like to participate in the research?

1. By phone

2. By zoom call
3. In – house

Code 1 = Continue to Q19
Code 2 = Continue to Q16
Code 3 = Continue to Q15

Q15. If your location is out of our reachable area, would you be happy to take part via Zoom / phone, instead?

1. Yes via phone
2. Yes via Zoom
3. No

If code 1, continue to Q19
If code 2, continue to Q16
If code 3, thank and record reason for refusal.

Q16. Do you have daily access to a personal computer with reliable broadband internet access? When we say personal computer we mean a desktop or laptop. We do NOT mean a tablet.

1. Yes daily access to a desktop
2. Yes, daily access to a laptop
3. No

Close on participants who code NO

Q17. The virtual interview will take place over Zoom and you must join in a quiet area in your home/office. Your personal computer must have a working video camera and a built-in microphone (or you must agree to use a headset with a built-in microphone). Do you have the necessary equipment in order to join a Zoom session?

1. Yes
2. No

Close on participants who code NO

Q18. Are you happy to take part in the virtual interview and for the interview to be observed and audio/video recorded?

1. Yes
2. No

If code 1 = Continue
If code 2 = Offer phone as an alternative or thank, record reason for refusal and close

Q19. As a thank you for your time and participation we would like to incentivise you £80. How would you like to receive your incentive?

1. By bank transfer
2. By voucher
3. By cash

Record

Q20. The research is being run by Yonder on behalf of their client, Ofcom, who may view your Zoom interview. By taking part in this, you agree to yourself and your comments being captured and viewed on video so it can be used in the research. Are you willing to participate on this basis?

1. Yes
2. No

Record
If code 2 please continue to recruit and record

Q21. Thank you for answering these questions. We would like to invite you to take part in a 60 minute interview. As a thank you for your time you will receive £80 incentive paid via BACS/Voucher/Cash.

We would like to re-emphasise that within the research there is no obligation to answer any questions that you don’t wish to and that your answers will be kept strictly confidential at all times. If you qualify, the interview will focus on your experience on a suspected scam or fraud online and there will be no repercussions as a result of taking part. You also have the right to withdraw your consent to process the information you provide at any time by contacting a member of staff. We will share the researcher’s contact details with you before the interview.

Do you consent to take part on this basis?

1. Yes
2. No

If code 2, thank and record reason for refusal

Recruiter Declaration

I confirm that this interview has been carried out with the respondent named, and that it was done in accordance with the instructions of [recruiter] and the Code of Conduct of the Market Research Society.

Recruiter Name:
Recruiter Signature:
Date:

Appendix C – Recruitment screener for experts who have supported victims of scams and fraud

Recruitment Screener
Reference: Scams and Frauds
Yonder Consulting - Ofcom

Qualitative recruitment spec and screener

- Recruiting 5 experts to take part in an hour IDI (either online/telephone); this screener is for experts.
- £70 incentive paid either through cash, bank transfer or voucher (however experts prefer).

Key criteria

- 5 x experts to work/have worked with online fraud or scams victims

Introduction: Good morning/afternoon, I am calling on behalf of Yonder, an independent market research agency, and Ofcom, the communications regulator for the UK, about a research study we are conducting on online scams and fraud and the impact it may have on people. If you go on to be part of the research you will be incentivised for £70 paid by cash, voucher or bank transfer. If you qualify, you will be asked to participate in either a 1:1 Zoom session or telephone interview. I would like to ask you some questions and, if you are eligible, invite you to participate. The call will take around 5 minutes. Is this a good time to talk?

3. Yes
4. No

1 = Continue and read out text below
2 = Thank and close

For all if agreed to continue with call: Ok, during this call, I will need to ask you for some personal information which will be used to establish if you qualify for this market research. The answers will be shared with Yonder if you are eligible to take part in an interview. We would first like to emphasise that within the research there is no obligation to answer any questions that you don't wish to and that your answers will be kept strictly confidential at all times. If any information about you is used in reporting, it will be anonymised.

You have the right to withdraw your consent to process the information you provide at any time during or after this conversation by letting me or a member of staff know.

Do you consent to take part in this phone call and the research project on this basis?

3 Yes
4 No

1 = Continue and read out text below
2 = Thank and close

Q1. Have you ever taken part in market research?

1. Yes
2. No

If code 1 continue to Q2, otherwise continue to Q3

Q2. What was the date of your most recent market research?
If less than 6 months ago then please terminate interview

Q3. Do any of your close friends/ family work in any of the following industries?

1. Journalism / Publishing
2. Market Research
3. Government
4. Regulatory body
5. Advertising / PR / Marketing
6. Comms providers (e.g. phone companies, satellite companies and internet service providers)
7. Comms technology providers (e.g. IBM, Microsoft, SAP, Oracle, Cisco)
8. Broadcasters / streaming platforms
9. Social media platforms
10. Online safety technology
11. Other (please specify)

Continue if code 11, all others please thank and close

Q4. Please record gender
Please recruit a mix

Q5. How old are you?
Please recruit a mix of ages
Screen out if under 18

Q6. Please can you tell us where you live (i.e. your primary residence)?
Recruit a mix of regions

Q7. Which of these best describes your current work status?

1. Working full time (30+ hours per week)
2. Working part time (up to 29 hours per week)
3. Unemployed – seeking work
4. Unemployed – not seeking work
5. Long term disabled
6. Stay at home to look after house/ family
7. In full time education
8. Retired
9. Refused

Please recruit a mix
Code 5 and 9 = Thanks and close

Q8. Do you work or volunteer in the healthcare sector?

1. Yes – I work

2. Yes – I volunteer
3. No

Please recruit a mix

Q9. Do you work or volunteer in a role / sector which supports people who may be struggling with their mental health?

1. Yes
2. No

Please recruit a mix

Q11. What is your work / volunteering role?

Record

Q12. Do you or have you ever worked with individuals who have been involved (either as perpetrators or as victims) with scams/fraud?

1. Yes – occasionally
2. Yes – regularly
3. No

All to code 1 or 2
Code 2 = Thank and close

Thank you for answering these questions. We would like to invite you to take part in a 60 minute interview. As a thank you for your time you will receive £70 incentive paid via BACS/Voucher/Cash.

We would like to re-emphasise that within the research there is no obligation to answer any questions that you don't wish to and that your answers will be kept strictly confidential at all times. If you qualify, the interview will focus on your expertise on the psychological impact of scam or fraud online on victims and there will be no repercussions as a result of taking part. You also have the right to withdraw your consent to process the information you provide at any time by contacting a member of staff. We will share the researcher's contact details with you before the interview.

Do you consent to take part on this basis?

3. Yes
4. No

If code 2, thank and record reason for refusal

Recruiter Declaration

I confirm that this interview has been carried out with the respondent named, and that it was done in accordance with the instructions of [recruiter] and the Code of Conduct of the Market Research Society.

Recruiter Name:
Recruiter Signature:
Date:

Appendix D – Discussion Guide for victims of scams and fraud

Ofcom – Scams and Fraud Depth Discussion Guide
60 minutes

Research Objectives:

The overall objective of this research is to explore the various paths of scams and fraud and their emotional impact on victims.

The specific objectives of this research are to:

- Explore specific characteristics of different user journeys associated with those experiences
- Understand users' attitudes and the emotional impact of different kinds of online frauds/scams

This document sets out the format for discussion but should not be considered a questionnaire and is by no means exhaustive in terms of the questions that may be asked in each session.

Questions may be asked in a different order to that recorded here and the moderator will exercise their own judgment when probing participants. The moderator will also seek to probe any responses on points of interest that may or may not have been anticipated.

Notes for moderators:

- A blob tree is available for use if participants are struggling with how they articulate their feelings

1. Introduction (5 minutes)

- Introduce moderator and Yonder
- Research is on behalf of Ofcom who want to understand more about the impact of online scams and fraud on individuals
- There are no right or wrong answers and everything you say will be kept confidential and anonymous – none of your personal details will be used in reporting
- You also have the right to withdraw at any point and not to answer anything you don't want to
- Session will last 60 minutes
- Ask participant for permission to record, then start recording

2. Warm up (5 minutes)

- Name
- Age
- How would you describe your online usage (e.g. frequency / confidence / common activities)
- What would you say your attitude was toward online scams in general, before your experience?
    - How aware were you of different online scams?
    - Why were you aware of these?
    - What sort of people do you think tend to fall for online scams?

3. Wider experience of scams (5 minutes)

- Do you think certain platforms are more likely to have scam content than others?
    - Explore perceptions and why
    - Do you avoid certain platforms for this reason?
- What, if anything, do you think platforms currently do to prevent scams on their platform?
    - Explore perception of impact / effectiveness

4. User Journey (15 minutes)

Moderator to explain we are now going to focus on their personal experience with scams and fraud

- First of all, could you tell me how long you considered the scam/fraud lasted?
    - Was it quick / a couple of minutes?
    - Conducted over a long period of time?
    - Why did you say so?

Moderator to explain that we would now like to hear about 'the journey' of the scam, from how you were first approached to when it was over

- When did you first come across the scam / scam content / scammer?
- Can you remember what you were doing at that moment?
    - Busy/relaxed mood
    - At home / out
- What device were you using to access the internet at the time?
- How did the scammer approach you? Or did you see any particular post or content online?
    - What kind of message did they send or did you see?
    - Who did the message come from?
        - Did they pose as someone you knew / someone you could trust?
- Which communication channel did they approach you through first?
    - Did you stay in contact with them on the same channel or did they move to different platforms/channels?
    - [If moved channels]
        - Explore why they moved channels
        - Explore if they were prompted by the fraudster
        - What reason(s) did the scammer give to justify moving the interaction away from the original platform/channel?
        - Explore their perception of why they were encouraged to move to a different channel
        - Was it your impression that it was always the same individual / there were multiple fraudsters?
- What was it that grabbed your attention / made you engage?
    - Thinking with hindsight, was there anything suspicious about their initial message at all?
- How did you respond?
    - Explore why they responded
        - Did you have any suspicions about the content/message at all?
        - [If yes] Why did you respond despite these?
    - What were you expecting to happen?
- How long did you stay in contact / engage for?
    - What were these messages like?
        - Explore tone, content, style

  - Were there any points at which you questioned their motive / any red flags at all?
- If you had to map out a timeline from initial communication to when you realised you were being scammed, what key points would you plot? ***Moderator to encourage participant to walk through the engagement from their perspective, probing:***
  - What were you thinking at this point?
  - How did the fraudster build and gain your trust to this point?
  - Were there any points where you felt hesitant or concerned? Explore why / why not
- How long did it take from engaging with the content (e.g. clicked on the advertisement, followed specific instructions, replied to a message) for you to realise it was a fraud or scam?
  - What was it that made you realise it was a scam?
  - Was it anything specific or a culmination of details?

5. Practical Impact (10 minutes)

Moderator to explain that we would now like to talk a bit more in-depth about some of the practical impacts you have experienced as a result of being scammed

- Did you lose money as a result of the scam?
  - Probe for those who didn't lose money – did you feel that you had been affected in any way practically
- How did they approach asking for money / were you expecting something in return for money (product/service etc)?
  - Did they put pressure on you / make it appear time sensitive?
  - Do you remember how you felt when asked?
  - With hindsight, were there any signs that this was a scam?
- How did you make the payment(s)?
  - Why did you make the payments that way? Explore scammer/victim preference
- When did you realise you lost money?
  - How did you find out?
    - Was there a specific trigger/moment?
  - How would you describe your feelings at this time?
- How much money did you lose?
- How did the amount of money lost impact you? What was the impact as a result of losing this money?
  - Was there anything you had to change / couldn't do as a result?

6. Emotional and mental impact of being scammed (10 minutes)

Moderator to explain we'd now like to explore the emotional impact of being scammed. Moderator to re-emphasise that they can stop at any point if they would like a break or would rather skip over some questions.

Moderator to refer back to key points identified in journey mapping. For each key point probe and use blob tree if appropriate:

- How were you feeling at this point of time?
- How did this change as you moved to the next key point?
  - Explore how and why
- How did you feel when you discovered you were being scammed?
  - What were your initial thoughts? Why?
  - How did you immediately react?
  - Did you ever consider you might be a victim of online scams?
- What would you say the impact, if any, of this experience was on your wellbeing in the short term?
  - Explore impact on short, medium and long term
  - For moderator reference, potential answers may include, please explore as referenced
    - Feeling of guilt
    - Decreased confidence online
    - Increased anxiety
    - Reduced self-esteem
    - Negative impact on relationships with friends and family
    - Feeling of social exclusion
    - Distrust of the content on the online service you were scammed on
    - Reluctance to engage online at all on any service or platform
    - Not affected at all
- Has this impacted you in other ways?
  - Probe:
    - Trust in other people
    - Confidence
- How did your habits change (if at all) since engaging with the scam/fraud? Explore
  - Explore how / what they do differently
  - Probe on:

        - Became more suspicious, spent less time online, avoid online payments, spend less time on specific platforms/ stopped specific kinds of online activity (such as accepting unknown friend requests) etc
- Since your experience, have you noticed more suspicious content on the sites you visit and services you use?
    - How can you spot them?

Are there any signs or clues you would like others to be aware of?

7. Action Taken/ Reporting (5 minutes)

- When you realised you had been scammed, if any, which action did you take?
    - Explore why they did / didn't take any action
- Could you explain the reporting process you went through after being scammed?
    - How did you go about finding where to report?
    - Did you try multiple avenues such as contacting the platform, bank, police or consumer bodies? If so which ones and in which order?
        - Why?
- Was there anything which was particularly helpful? Explore what and why
- Was there anything particularly unhelpful? Explore what and why
- Did you ever flag content? If so, was the reporting button/ mechanism easy to find and use?
- How do you think a platform can help avoid scams? i.e. send an alert to remind people that content has not been fact checked
    - Does this vary by platform, in your experience? Explore how
    - What improvement(s) do you think could be introduced to make reporting online fraud and scams easier/ a better experience? **Moderator to probe as necessary:**
        - Improved mechanisms for reporting scams on platforms
        - Clearer sign posting to organisations like Action Fraud
        - Evidence that action will be taken as a result of reporting a scam

8. Impact on platform usage (5 minutes)

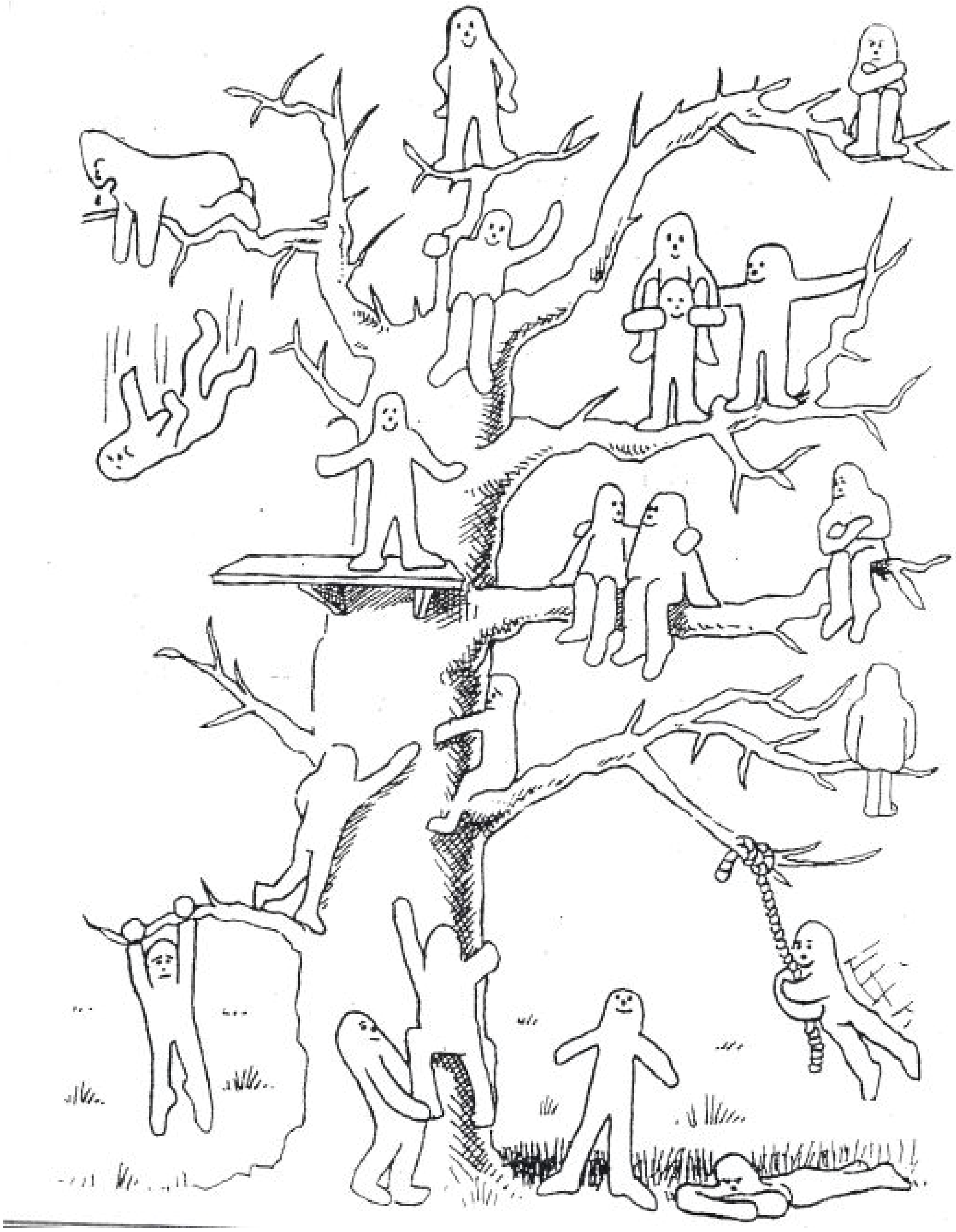
- Did you have any communication with the platform where the scam happened?
    - Explore why / why not
- [If they had communication with the platform]
    - Did you have the post reviewed/ content taken down?

    - If the platform didn't take action, what reason did they platform give for not taking down the content/removing the user/ taking action?
- Following the experience, did the way you used the platform change at all? Explore
    - Did you use tools on the platform to increase your privacy or block contact from the scammer in future?
    - How did you feel after this? More / less secure? Explore
- Have you been put off using certain platforms since the experience? Explore which
- Do you feel more cautious about interacting with content online at all? Explore why/why not

9. Wrap up (5 minutes)

- Thank you all for your time and contributions
- Moderator to inform that the research was on behalf of Ofcom and to reassure that all answers and participation is completely confidential and anonymous
- Moderator to confirm incentive process
- Moderator to provide leaflet with list of support services

Stimulus A: Blob Tree



Appendix E : Discussion guide for experts who have supported victims of online scams and fraud

Ofcom – Scams and Frauds Depth Discussion Guide with Experts
60 minutes

Research objectives:

The overall objective of this research is to explore the various paths scams and frauds and their emotional impact on victims.

The specific objectives of this research are to:

- Explore specific characteristics of different user journeys associated with those experiences
- Understand users' attitudes and the emotional impact of different kinds of online frauds/scams

This document sets out the format for discussion but should not be considered a questionnaire and is by no means exhaustive in terms of the questions that may be asked in each session.
Questions may be asked in a different order to that recorded here and the moderator will exercise their own judgment when probing participants. The moderator will also seek to probe any responses on points of interest that may or may not have been anticipated.

1. Introduction (5 minutes)

- Introduce moderator and Yonder
- Research is understanding scams and frauds and their emotional impact on victims.
- There are no right or wrong answers and everything you say will be kept confidential and anonymous – none of your personal details will be used in reporting
- You also have the right to withdraw at any point and not to answer anything you don't want to
- Session will last 60 minutes
- Ask participant for permission to record, then start recording

2. Warm up (5 minutes)

- Could you please introduce yourself?
  - Name and age
- Role and responsibilities
  - What is your job role?
  - How long have you been in this sector?
  - What are your main responsibilities?
  - What challenges can you face in your role and why?

3. Experience with victims of scams and fraud (5 minutes)

Moderator to explain we are interested in hearing about their experience in working with victims of scams and fraud

- Can you tell me about some of the fraud victims that you have worked with?
- Have you observed any common traits in them?
  - Do they have much in common
    - Life stage / lifestyle / personality

- Do you think there is a 'type' of person who is more prone to being scammed?
    - What are the contributing factors?
    - What are the factors that make them reply to scammers?
- Why do you think victims of fraud decide to come to therapy / seek support?
- What are the main issues they are looking to address in therapy / through contacting support services?
    - Confidence, shame, guilt

4. Friends and families of victims (5 mins)

- Do you ever work with people who have been affected by scams/fraud but indirectly? E.g. friends/family of victims
    - Have you observed any common traits in them?
- What are the main issues they are looking to address in therapy/through seeking support?
- What impact can scams/fraud have on them?

5. Scam trends and methods (1o minutes)

- Have you observed any trends in terms of scam methods / techniques / types of scam?
    - Which is the most common?
    - Which is the least common?
- Which is the most effective? Why?

Moderator to ask participant to think about the kinds of victims they've worked with. What are some of the commonalities they have observed in terms of:

- Approach
    - How do scammers approach their victims
- Type of message
- Content of message
- Length of time invested in the scam / fraud
- Length of scam
    - Minutes / hours / days / weeks etc
- Building trust
    - What are some of the methods/techniques they use to build trust
    - Why do you think they are effective?
- Channels
    - Are there particular platforms/channels that scammers use
    - Are there any channels which you think are perceived to be 'safe'/regulated to prevent scammers? Explore which and why
- Do you have any opinions about why people scam?
    - What do you think motivates them?

6. Emotional Impact (10 minutes)

Moderator to explain we would like to talk in-depth about the emotional journey a scammed person can go through.

- What are the different stages in the emotional journey from when they first realise they've been scammed?

  - How does this change/develop over time?
  - Is there a crucial stage for intervention/support?
  - Are there any patterns across victims' journeys?
- What are the kinds of feelings and thoughts they have?
  - How do they feel when they've realised they've been scammed?
  - What is their first reaction?
  - Do they tend to blame the platform for hosting the content? Explore why/why not
- What is their emotional state when they first come to therapy/seek support?
  - How are they feeling about the scam?
    - Explore any feelings of responsibility / self-blame
- Do they have any long-term emotional impact? If any, which kind?
- Are there any repercussions on people related to the victim (friends/family etc)? Explore

7. Practical impact (5 minutes)

- Have you ever noticed any practical changes in how victims use the internet / social media platforms
  - Using less / more
  - More wary of content
- Do you think behaviour changes as a result of being scammed tend to last for a long time / or do they revert back? Explore what and why

8. Prevention (5 minutes)

- What could be done to better protect people from scams/fraud in the future?
- Thinking about the victims you work with, what do you think would be the best channel to reach them?
  - What kind of messaging would resonate with them? Explore what and why
- Explore strengths/weaknesses of each of the following areas as means of promotion:
  - Online alerts (such as a pop up message on the platform / an occasional pop up warning to remind of the importance of staying alert)
  - Online promotion (such as social media posts on advice about keeping safe online)
  - Offline promotion (posters/advertisements in bus shelters / texts from bank/credit card company etc)

9. Future support for victims (5 minutes)

- What are some of the long term needs that victims of fraud can have?
  - Explore what and why
- When is it most important to offer support services and help to victims?
- In your opinion, how can victims of fraud be better supported? Explore how and why

10. Wrap up (5 minutes)

- Thank you all for your time and contributions
- Moderator to inform that the research was on behalf of Ofcom and to reassure that all answers and participation is completely confidential and anonymous
- Moderator to confirm incentive process