Preventative Spend Research 2018

March 2021

Scottish Government
Riaghaltas na h-Alba
gov.scot

Preventative Spend Research

EKOS Limited, St. George's Studios, 93-97 St. George's Road, Glasgow, G3 6JA
Reg 145099 Telephone: 0141 353 1994 Web: www.ekos-consultants.co.uk

Direct enquiries regarding this report should be submitted to:

John Kelly, Director, EKOS

Email: john.kelly@ekos.co.uk

Tel: 0141 353 1994

Contents

1. Foreword

1.1 Introduction

This report presents the findings of research conducted by EKOS Economic and Social Research based on a commission from the Scottish Government's Consumer, Competition and Regulation Unit.

Its objectives were to undertake a review of existing research and evidence on the financial cost of scams to the Scottish economy to identify and measure preventative strategies designed to reduce their impact.

The Scottish Government is responding to this challenge and recognises the need to develop a more strategic approach, including increased emphasis on collaborative working and active, coherent methods to identifying and protecting those most at risk.

To support development of the strategy, it is recognised that a clear picture of the impact of scams on the Scottish economy is required as well as an understanding of the benefits of preventative interventions, and a comparative assessment of such measures.

1.2 Study Objectives

The detailed objectives of the research were:

- to review evidence and develop an assessment of the cost to Scotland's economy of scams;
- to identify existing preventative measures and strategies designed to protect people from scams, both in Scotland and across the UK; and
- where possible, to quantify the social and financial impacts of these preventative interventions.

The research brief also identified the following key tasks:

- assess the cost of scams on Scotland's economy taking into account both individual losses and wider costs to society;
- analysis of data, research and practice to identify existing preventative spend interventions in Scotland and across the UK;
- assess the impact of these strategies, including where possible quantifying their financial and social benefits; and
- provide recommendations of interventions that are likely to offer the greatest return for preventative spend.

1.3 Report Structure

The proposal has been prepared in line with the specific and detailed tender instructions, and is structured as follows:

- Chapter 2: Setting the Context;
- Chapter 3: Scope and Scale of Scams;
- Chapter 4: Scam Prevention Measures;
- Chapter 5: Stakeholder inputs ; and
- Chapter 6: Conclusions and Recommendations.

Appendix 1 provides details of the main organisations currently addressing the issue of fraud and scam and Appendix 2 sets out in some detail the different types of fraud and scam.

1.4 Research Support

In undertaking this research the consultants were aware that there was extensive wider concern for the issue of scams and the need for a more focused response to mitigate their impacts.

We are particularly grateful to the many organisations and individuals who contributed to our understanding and provided valuable insights and views on how best to tackle the issue.

We have included a list of those as an appendix to this report and offer up our kind regards and thanks.

2. Setting the Context

2.1 Introduction

This Chapter considers the background and wider context within which this research study has been conducted. It also seeks to set out the scope of the research and some of the issues which have impacted on it.

2.2 Overview Perspective

The context for this research was set out in Scotland's Nuisance Calls Commission Report and Action Plan which was published in late 2017. This identified a focus on three key areas:

- empowering and protecting individuals;
- encouraging better business behaviour; and
- improving government and public agency responses.

The Commission also recognised that "*the greatest threat to be tackled is the danger of scam calls, especially to vulnerable people, and that the problem of scams goes far beyond those perpetrated via unwanted calls. As a long term action, Commission members sought a strategic and coordinated response to scams from the Scottish Government and enforcement agencies".*

Nuisance calls are generally considered to be one of the banes of modern life with a recent report highlighting that three out of the top

four cities in the UK for nuisance calls were in Scotland and that in Glasgow over 50% of all calls were designated as “nuisance calls[1]”. While nuisance calls are a real problem for society, it is those that are defined as “scam calls” where the intent is to defraud individuals in some way that can cause the biggest problems.

While there is usually a financial consequence or loss for the individual there can also be wider costs to society including:

- social or health costs;
- emotional costs;
- crime investigation costs;
- Local Authority costs (Trading Standards);
- time costs;
- data collection costs; and
- technical costs.

It is estimated[2] that 17% of nuisance phone calls are scam calls, that a further 39% of calls are some form of mis-selling, and that only 44% of nuisance calls are legitimate.

2.3 A Definition Discussion

Prior to commencing the detail of the research we sought to define the scope of what is covered by the term “scam” in order to ensure a consistent approach.

Crucially, we do not believe there is a right or single answer to the question and there will be many definitions of “scams”. However, for

1 Scottish Cities top the table for nuisance calls: WHICH report 2016. Which press release - nuisance calls
2 Impact of Scam Calls in UK; trueCall Ltd [telephone call controller system provider]

the purpose of this research it is important to state up front a working definition.

Oxford English Dictionary (OED)

scam

Pronounced: skam
noun informal
plural noun: scams
a dishonest scheme; a fraud.
"an insurance scam"
synonyms: fraud, swindle, fraudulent scheme, racket, trick, diddle; informal con, con trick, flimflam, gyp, kite; grift, shakedown, bunco, boondoggle;
"the scam involved a series of bogus reinsurance deals"
verb: to scam
3rd person present: scams
swindle. "a guy that scams old pensioners out of their savings"

Citizens Advice Scotland
Scams are schemes to con you out of your money. They can arrive by post, phone call, text message or email or a scammer may turn up at your home.

An early finding is that scam is often seen as interchangeable with fraud which is in more common usage. It is also not always (or mostly) based on a telephone call. It can be on-line, doorstop, by post, by text or by individual (eg family member).

However, we would make the distinction that “fraud” is a broader category and can include non-financial aspects or acts of deception carried out for the purpose of unfair, undeserved and/or unlawful gain.

Scams always have a financial element to them and as such can be seen as a subset of both fraud and nuisance calls.

One particular definition was suggested as follows:

- fraud - unauthorised transaction where the victim has no initial knowledge or awareness; and
- scam - authorised transaction where the individuals has been "duped" or tricked in some way.

As Police Scotland state" not all scams are fraud but all frauds are scams". Scams are generally a sub-set of fraud. However, in practice the terms are imprecise and often used interchangeably.

However, we do not believe there is any benefit in over-analysing these definitions and we suggest that for this research scams can be equated to financial fraud[3].

Scams can be perpetrated on individuals, businesses or Government/ public sector.

- individuals - examples will include:
    - electronic fraud
    - banking
    - telephone scams
    - pensions
    - building works
    - energy

[3] Police Scotland web site- "fraud is sometimes also referred to by other names such as scam or con"

- business - examples will include:
    - insurance frauds
    - mortgage frauds
    - advertising scams
    - invoice frauds
    - procurement fraud
- society/ government
    - tax avoidance
    - VAT frauds
    - benefits claims
    - public purchasing.

A more detailed list of fraud/ scam types is provided in Appendix 2.

The focus of this research relates to the individual although we would highlight that this is only one aspect of the challenge. For example, fraud perpetrated on insurance companies will have a knock on effect on individuals as insurance costs rise.

2.4 A Crowded and Complex Landscape

One of the key challenges in undertaking this research is the crowded landscape which can be characterised as follows:

- from a policy perspective, the issue of scams is being seen as increasingly important across the wider landscape with a recognition of the scale and scope of the problem and that the incidences and challenges are increasing;
- there are many organisations already operating in the area seeking to address the issue covering legislative, regulatory, crime and justice, consumer rights, vulnerable groups; local authorities etc;

- some of these are very specific and focus on particular or very specific aspects eg pension scams or individuals with dementia;
- as well as many organisations operating to mitigate the impact of scams there are also many different initiatives being delivered by these organisations - many using different language and different delivery or communication channels;
- there is no robust evaluation evidence as to the success of these initiatives as many of the interventions are quite recent and still current, with no processes in place to measure impact. In fact we are not aware if any of these initiatives have any indicators which are being measured.

2.5 Data Challenges

There are also a number of data challenges in seeking to assess the true impact of scams/ fraud.

Our review has identified a number of different publications, reports and statistics which provide estimates of the scale of fraud, scams and cybercrime in the UK.

However, most do not provide disaggregated estimates for Scotland and additionally, the differing legal systems, police authorities and official data collection regimes mean that estimating the full impact of criminal fraud and scam activity is difficult.

Some data includes business and public sector, some is very specific (insurance fraud only) and some is focused on individual groups (eg vulnerable people).

There are also different data collection protocols and definitions which makes comparison or “read across” complex.

In addition, it is widely stated that most fraud goes unreported and therefore a “true cost” is harder to quantify. For example, different data sets suggest that the level of reported incidences could be as low as 3% with a high end estimate at 20%.

The truth is that we will never know, but we can be sure the bulk of scams are not reported, although it is likely that any data provided could be multiplied by anywhere between 5 and 30 times.

This is considered further in the next Chapter.

3. Scale and Scope of Scams

3.1 Previous Research

To highlight the difficulty in estimating the total cost of scams to the Scottish economy we would highlight a range of published headline research:

- Annual Fraud Indicator Report 2017
    - £190 billion[4] UK across all sectors (business/ charity/public/ individuals) of which around £7 billion relates to individuals
- Home Office 2016
    - £10 billion lost to UK individuals 2016;
- National Fraud and Cybercrime Centre
    - UK fraud and cybercrime costs £11 billion;
- Scottish Business Resilience Centre
    - fraud and cybercrime cost Scotland £384 million in 2016;
- IT Governance:
    - cost to UK business in 2016 of fraud and scams: £29 billion;
- Insurance Fraud Bureau:
    - costs of insurance fraud in 2016 - £3 billion;
- KPMG:
    - value of fraud reported to court system: £1.1 billion;
- Financial Fraud Action UK:

[4] Put into context, the scale of the problem is such that the cost of fraud to the UK is greater than the Gross Domestic product of 148 out of 191 countries

    - Financial fraud losses across UK issued debit and credit, remote banking and cheques totalled £768.8 million in 2016. This affected almost 2 million individuals;

- Age UK
    - in Scotland over 400,000 people believe they have been targeted by scammers with 70% not reporting it to an official channel;
- trueCall
    - estimate that the average amount lost by each older vulnerable person to telephone scams each year is £313, and that the social care cost attributable to scams for each older vulnerable person each year is £623l
- Money Advice Service
    - recent research suggests that there could be as many as eight scam calls every second – the equivalent of 250 million calls per year. 3.5 million Britons have fallen victim to telephone fraud since 2010;
- Ofcom
    - 8 billion unsolicited calls are made each year which are illegal in terms of privacy laws. Of these some use spoof numbers to give a false assurance of people's identities which subsequently turn out to be scams;
- The Pensions Regulator
    - published a figure in 2014 of £500 million being lost based on cases where action was taken;
    - Individuals reported nearly £19 million in suspected pension liberation fraud between April 2015 and March 2016 – this was twice as much as for the same period in

2014-15, and it may be that the actual amount of pension fraud is considerably higher due to cases that go unreported;

- Xafinity Pensions Consulting
    - in the financial year 2015-16, there were 30,000 ‘defined contribution’ scheme transfers. This represented £1 billion of assets. Xafinity Pensions Consulting estimates suggest that fraudsters could be behind as many as one in 10 pension transfer requests.

It can therefore be seen that the “true cost” of fraud or scams will vary significantly depending on definitions and what is being counted, data sets being used and the method of data collection.

We would also highlight a health warning as it is not possible to know how robust the data is or the sources used to arrive at these estimates or the assumptions used in their calculation.

For example:

- different data sets include different types of definitions (e.g. only cyber);
- some data includes individual and business and public while others do not;
- the data is based on that reported to the organisation publishing the data;
- there are different levels of geographical coverage;
- it is not always clear which groups are included (individuals, businesses etc)

While there is no single accepted source of data, the Annual Fraud Indicator report is probably the most consistent and time series based

data which has been published since 2012. This data show that fraud level in terms of individuals peaked in 2016 at £15 billion and dropped back to £7 billion in 2017.

The research report highlights that detected or reported examples of fraud do not represent the total cost of fraud, because much remains undetected. If we assume that Scotland has a similar pattern of reported fraud[5] to the UK this would suggest a total reported fraud impacting on individuals of £560 million in 2016.

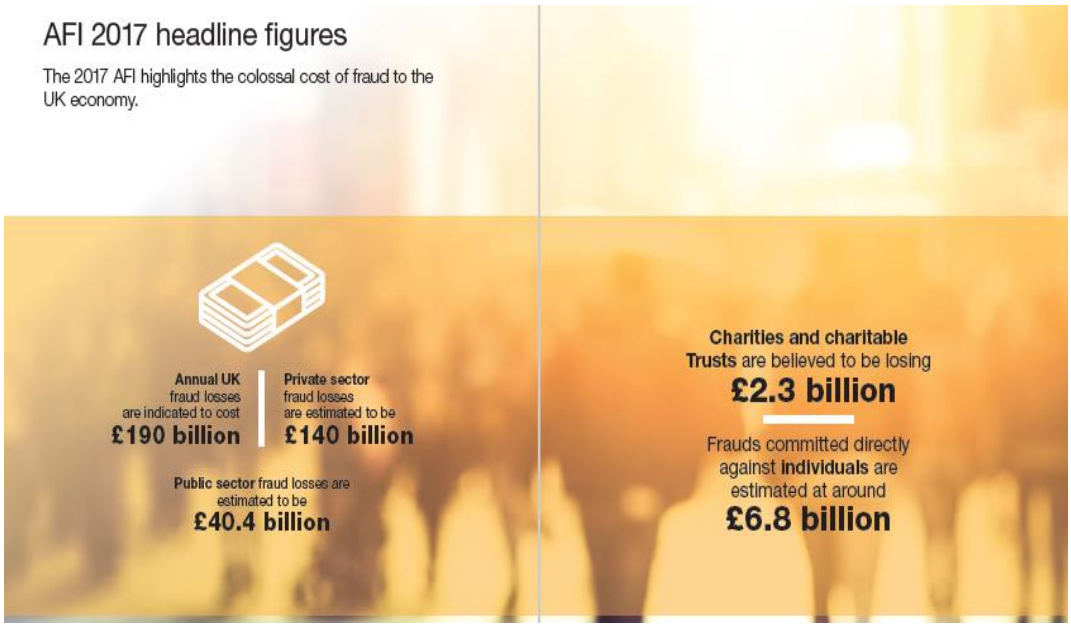
But note, this does not include fraud against business, public sector or charities and is only based on that which is reported.

Therefore the total figure for all fraud/ scams in Scotland is likely to be in the many billions.

See over for excerpt from Annual Fraud Report.

[5] Scotland currently has around 8% of total UK population

Excerpt from Annual Fraud Indicator Report



3.2 Crime Survey Data

This section presents comparable crime survey data gathered in Scotland and England and Wales, alongside recorded (and reported) crime statistics, to try and gauge the potential scale and scope of reported fraud in Scotland.

Firstly, the Scottish Crime and Justice Survey is a large-scale social survey which asks people about their experiences and perceptions of crime. The survey was previously undertaken with a sample of 12,000 adults every two years, including for the most recent release (2014/15). Future releases, including for the 2016/17 survey, will be based on an annual sample of 6,000 respondents.

The 2014/15 survey asked the following questions related to fraud:

- whether respondents have had their bank cards/details used to withdraw/spend cash without their permission over the previous 12 months, and the extent to which they are worried this could happen; and

- whether respondents have had their personal details used without their permission in order to commit fraud over the previous 12 months, and the extent to which they are worried this could happen.

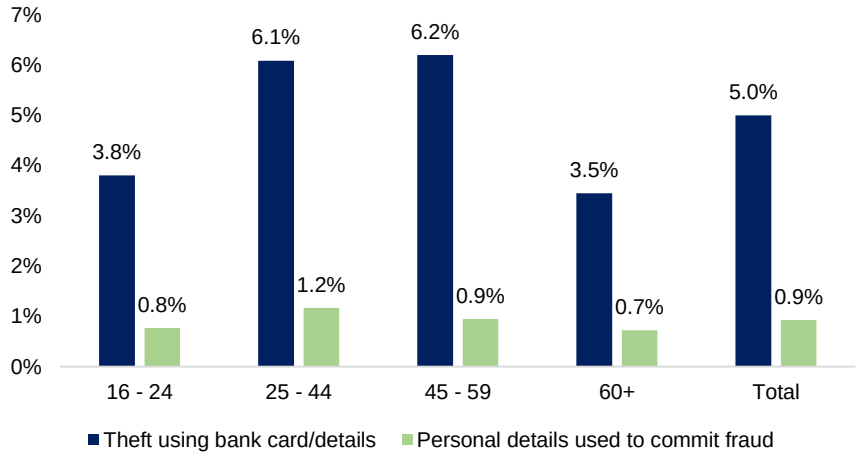
Experience of Fraud

Figure 3.1 shows the percentage of respondents reporting they have been a victim of each type of crime within the previous year, broken down by age.

The results indicate that those aged between 25 and 59 are most prone to this type of crime. There is no substantial variation when the results are disaggregated by gender, disability status, or if living in a rural or urban area.

By region, the lowest proportion of respondents reporting they have been victims of theft using bank/card details is in Argyll and West Dunbartonshire (3.2%), with the highest in Edinburgh and Lanarkshire (both 5.8%).

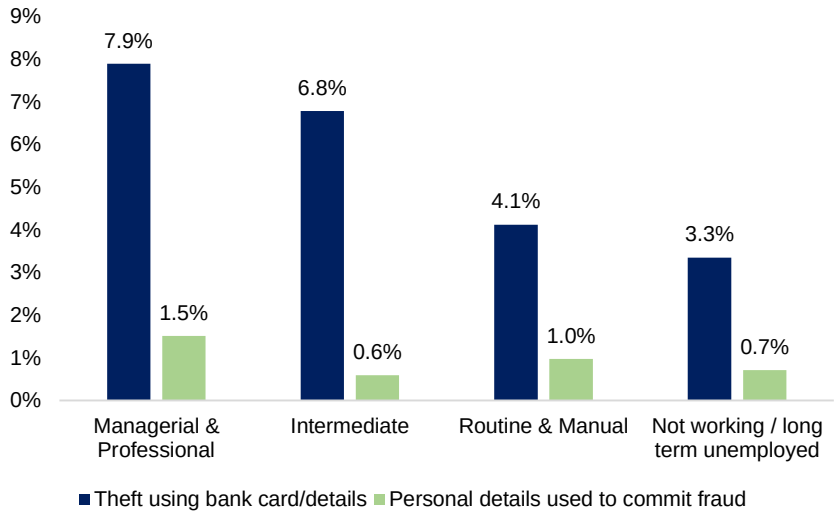
Figure 3.1: Victim of fraud in last year, by age



Source: SCJS 2014/15

The results show those in higher socio-economic groups are more likely to be victims of this type of crime.

Figure 3.2: Victim of fraud in last year, by socio-economic group

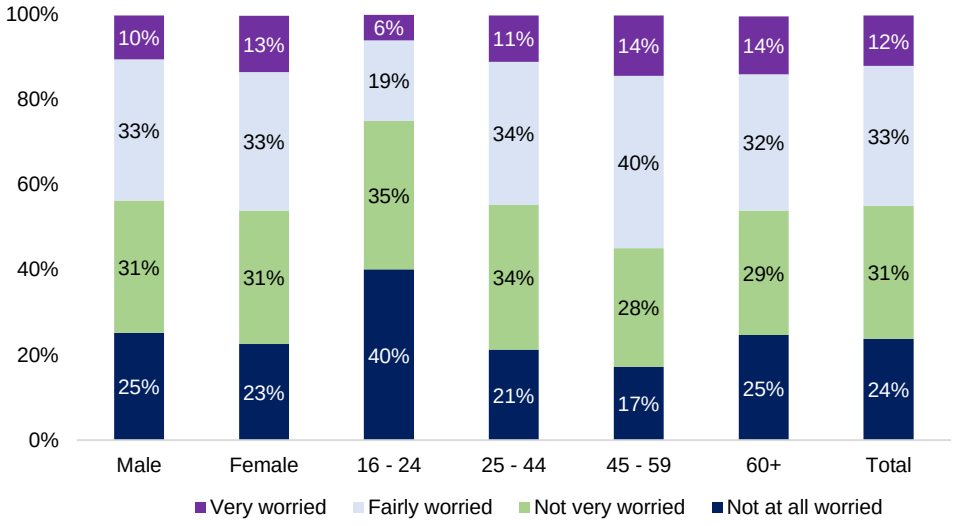


Source: SCJS 2014/15

Fear of Fraud

When asked about the extent to which they fear they may have their identity stolen, women are slightly more worried more men, while those in older age groups are more likely to be worried than younger age groups.

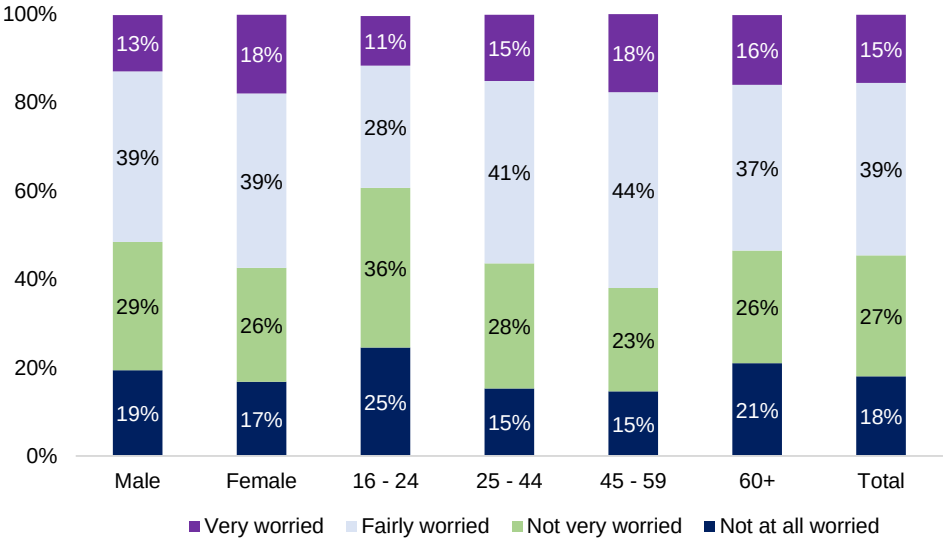
Figure 3.3: Extent of worry about identity being stolen, by age and gender



Source: SCJS 2014/15

Similarly, women and those in older age groups are more likely to be worried that someone will use their credit or bank details to obtain money, goods or services.

Figure 3.4: Extent of worry about theft using card/bank details



Source: SCJS 2014/15

England and Wales

Since 2015, more detailed information related to fraud and cyber-crime has been collected for England and Wales both by police forces, who have a requirement to flag crimes as 'cyber-crime' where appropriate, and in questions posed in the Crime Survey for England and Wales. As shown in **Table 3.1**, 5% of respondents reported they have been a victim of bank/credit account fraud, the same proportion as the Scottish survey **(Figure 3.1)**. This is by far the most common type of fraud, with half of it carried out online.

It would be reasonable to assume that – at a high level – the findings of the England and Wales survey will broadly apply to Scotland in terms of the prevalence of different types of fraud and its characteristics.

Table 3.1: Fraud and cyber-crime – England and Wales

	% which is cyber crime	Rate per 1,000 adults	With loss, not or partially reimbursed	With loss, fully reimbursed	Without loss
Fraud					
Bank and credit account fraud	49%	51.5 (5%)	5.0	35.9	10.6
Consumer and retail fraud	81%	16.1 (2%)	5.7	4.2	6.2
All other fraud	-	2.2 (2%)	1.0	0.03	1.2
Computer Misuse					
Computer virus	97%	20.7 (2%)	5.2	0.1	15.4
Unauthorised access to personal information (including hacking)		11.7 (1%)	-	-	-

Source: Crime Survey of England & Wales, year ending September 2017
Note: Cyber-crime represents cases where the internet or any type of online activity was related to any aspect of the offence

Nearly two fifths of fraud (39%) did not result in a financial loss, while 37% of incidents involved a loss of up to £249.

Table 3.2: Financial loss suffered by victims of fraud

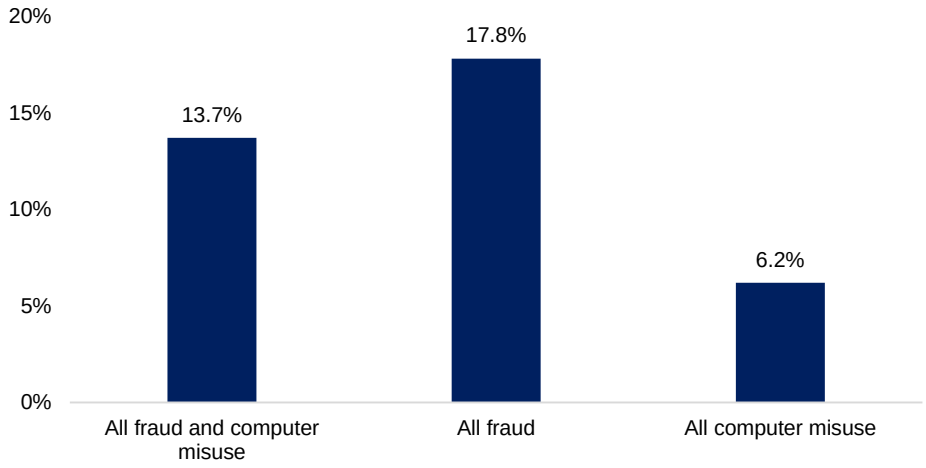
Amount lost	%
No financial loss	38.8%
Less than £20	5.6%
£20 - £49	8.7%
£50 - £99	11.0%
£100 - £249	12.2%

£250 - £499	9.4%
£500 - £999	5.9%
£1,000 - £2,499	4.9%
£2,500 - £4,999	1.8%
£5,000 - £9,999	0.9%
£10,000 - £19,999	0.8%
£20,000 - £39,999	0.2%

N=1,211. Includes all fraud incurring a financial loss, regardless of later reimbursement. Excludes computer misuse.
Source: Crime Survey of England & Wales, year ending September 2016

The proportion of fraud and computer misuse incidents that the police or Action Fraud were made aware of is low, at 13.7%. The proportion of computer virus incidents reported to the police is particularly low, at 1.9%, while computer misuse that involves unauthorised access to personal information (including hacking) is higher, at 14.7%.

Figure 3.5: Incidents that the police or Action Fraud were made aware of



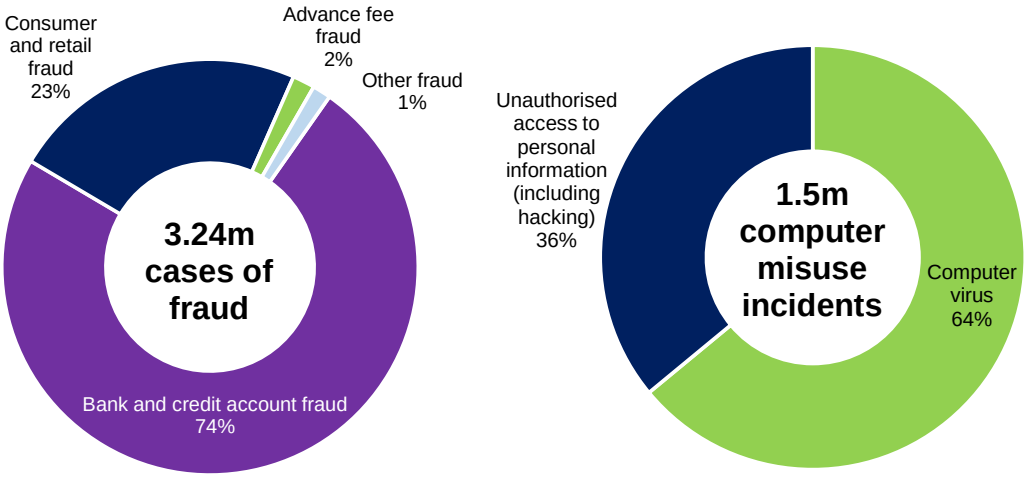
Source: Crime Survey of England & Wales, year ending September 2016

The most common reasons for not reporting were a lack of awareness of Action Fraud (66%), victims thinking the incident would be reported by another authority (10%) and victims thinking the incident was too trivial or not worth reporting (8%). The cases brought to the attention of the police/Action Fraud are therefore likely to be those where the financial loss or emotional impact on the victim is greater.[6]

Over the year to September 2017, 663,000 fraud offences and 22,000 computer misuse crimes are recorded in crime statistics for England and Wales, based on data compiled from Action Fraud (who collect from local police forces), Cifas and UK Finance (with the potential for some double or triple counting but the impact of this is felt to be negligible).

However, the Crime Survey data provides a better indication of the volume of fraud offences as it covers those incidents not reported to the authorities. This therefore gives a much higher number, with an estimated 3.24m cases of fraud and 1.5m of computer misuse. This means that fraud accounts for 44% of all crime, as estimated using the survey (but just 5.5% of crime reported to the police).

Figure 3.6: Total fraud offences, England & Wales, year to September 2017



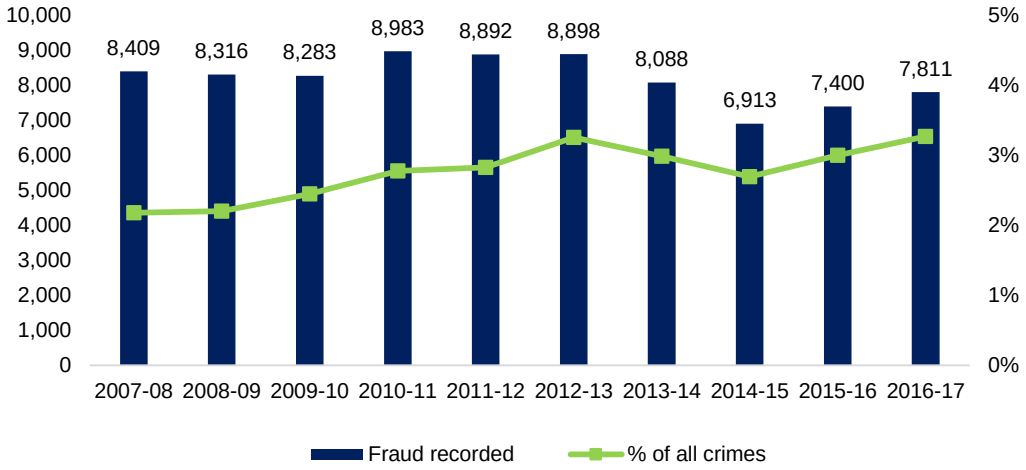
[6] Overview of fraud and computer misuse statistics for England & Wales, ONS, 2018

Source: Crime Survey of England & Wales, year ending September 2017

Recorded Crime in Scotland

Fraud data collected by the authorities in Scotland currently lacks the same detail as south of the border. The annual number of crimes of fraud has fluctuated slightly over the last decade, within the range of 6,900 to 9,000. However, with overall crime having fallen, the proportion made up by fraud has been on an upward trend, to 3.3% of all crime in 2016-17. By comparison, the 273,000 incidents reported to Action Fraud represent 5.5% of recorded crime in England and Wales.

Figure 3.7: Fraud offences in Scotland

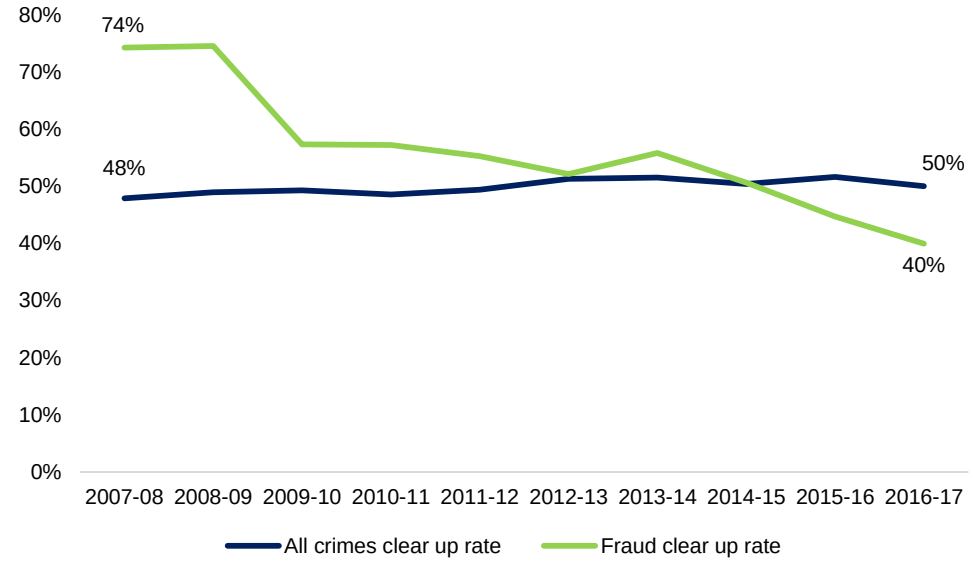


Source: Scottish Government, Recorded Crime in Scotland 2016-17

The clear up rate for fraud has fallen dramatically over the last decade, from 74% in 2007-8 to 40% in 2016-17. Over the same period, the overall clear up rate for crime stayed fairly even, at around 50%.

The clear up rate for fraud has fallen despite the number of incidents recorded being lower than a decade ago (albeit a higher percentage of all recorded crime). This could indicate that either less resources are being devoted to solving fraud or that cases of fraud have become more difficult to solve.

Figure 3.8: Crime clear up rate



Source: Scottish Government, Recorded Crime in Scotland 2016-17

Crimes under the Computer Misuse Act in Scotland are recorded under vandalism, with 30 in 2016/17, less than 1% of the total in this category.

What is perhaps surprising is the much lower level of fraud reported to the police in Scotland – around 8,000 incidents compared to the 273,000 in England and Wales that were recorded by Action Fraud, who do so on behalf of local forces. This means Scotland accounts for 2.8% of all fraud reported to the police in Scotland, England and Wales, despite having around 8.5% of the population.

However, Action Fraud proactively ask to be made aware of phishing and malware campaigns even where money has not been lost or personal details exposed, with a dedicated email, online chat platform and helpline number for this purpose, as well as an online form to complete if you have been a victim of a crime.[7]

[7] Action Fraud, Report attempted scams or viruses

In comparison, Police Scotland advise scam victims to go through their standard reporting approaches of dialling 101 or emailing the normal Police Scotland contact address, unless it is an emergency.[8]

The tailored approach to seeking reports of fraud/scams in England and Wales may account for the higher number of incidents recorded.

Even with this higher number, however, evidence shows that only a fraction of fraud – 18% of incidents in the year to September 2017 – is reported to the police. It is therefore clear that the vast majority of fraud incidents in Scotland will not feature in recorded crime statistics.

3.3 Cifas Fraud Statistics

Cifas is a not-for-profit fraud prevention membership organisation, which facilitates data sharing among its 400 members to reduce instances of fraud and financial crime. As mentioned, incidents recorded by Cifas are used in official crime statistics for England and Wales, alongside police data.

Cifas maps by region the confirmed fraud cases loaded to its database, split into six categories of fraud:

- Asset conversion: The unlawful sale of an asset subject to a credit agreement – for example, a car bought on finance and sold on before it has been paid off;
- Application fraud: When an application for a product or service is made with material falsehoods, often using false supporting documents;
- False insurance claims: False insurance claims occur when an insurance claim, or supporting documentation, contains material falsehoods;

[8] Police Scotland, Reporting Fraud

- Facility takeover fraud: When a fraudster abuses personal data to hijack an existing account or product – for example, a bank account or phone contract;
- Identity fraud: When a fraudster abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or product; and
- Misuse of facility fraud: The misuse of an account, policy or product – for example, allowing criminal funds to pass through your account or paying in an altered cheque.

Of these, facility takeover fraud and identity fraud are of most relevance to this study. The data indicates a low proportion of each occurring in Scotland. However, it is immediately clear that the number of fraud incidents being recorded on the Cifas database is double the police figure.

Table 3.4: Cifas Fraud Statistics – Scotland

	2015	2016	% of UK total in Scotland (2016)
Asset conversion	37	53	14%
Application fraud	4,777	2,804	9%
False insurance claim	29	28	6%
Facility takeover	724	940	4%
Identity fraud	5,463	5,827	3%
Misuse of facility	6,036	7,008	7%
Total	**17,066**	**16,660**	**5%**

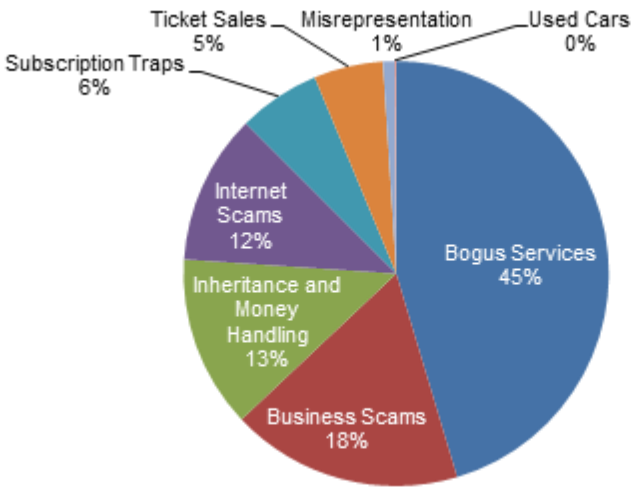
Source: Cifas National Fraud Statistics

3.4 Trading Standards Scotland

Trading Standards Scotland (TSS) is the national team for trading standards in Scotland, funded by the UK Government and overseen by COSLA. TSS coordinates cross boundary activity between trading standards departments within each local authority and offers specialist support to them.

TSS have supplied data for scams reported to them and logged in their database over the last few years. A breakdown of the 2,411 scams logged in 2016 and 2017 is shown below. When bogus services (45%) is broken down further, the most common specified were bogus computer services (10%), approaches from those purporting to represent a government agency (4%) and accident injury lawyers (2%).

Figure 3.9: Scams Logged by Trading Standards Scotland 2016-17



N=2,411. Source: Trading Standards Scotland.

TSS then undertook a more detailed analysis of scams logged in the final quarter of 2017. Of these, it was deduced that just under half (47%) would be more appropriate for the police to deal with.

This is particularly the case where complaints are purely financial and likely to fall under fraud e.g. phishing scams or payment for goods/services which are never delivered or provided.

Other sources

Other estimates on the scale and characteristics of fraud have been sourced, including:

- 91% of cyber-attacks start with a phishing email and 30% of phishing emails are opened (BDO, Private View on Cyber, 2017);
- the average age of mail scam victims is 74, and over half of people aged 65+ believe they have been a target of a scam (Age UK, Fraud Briefing, 2016).

4. Scam Prevention Measures

4.1 Introduction

This section provides an overview of some scam prevention activities that exist in Scotland – both a summary of some of the main national services and sources of information and case studies of specific initiatives which have been highlighted through this research.

It is intended to present a review of the wide range of preventative measures already being delivered.

4.2 Nuisance Calls Commission – Action Plan

The Scottish Government convened the Nuisance Calls Commission in 2016, bringing together key regulatory, industry and consumer group stakeholders with an interest in preventing nuisance calls. The Commission culminated in the publication of an Action Plan in September 2017.

"Unwanted phone calls that attempt to promote a product, service, aim or ideal that can cause the recipient a range of harm, from annoyance to lasting detriment, including emotional or financial damage."

It was recognised that nuisance calls are a complex issue that can only be solved by a combination of solutions, and would be difficult to eradicate altogether. The actions outlined are divided into three categories:

- empowering and protecting individuals:
    - fund 500 call blockers for vulnerable people, overseen by Trading Standards Scotland, building on good practice previously developed (see East Renfrewshire case study, below)
    - raise awareness of protection options by continuing to support/fund campaign activity

    - measure impact and ensure future actions are evidence-based (this report was published in December 2017, see below)

- encouraging better business behaviour:
    - raise awareness of existing regulations
    - explore future collaboration with financial providers
    - encourage best practice among businesses, e.g. becoming TPS assured
    - update the Scottish Government's Business Pledge to include criteria around protecting and supporting vulnerable customers;
- improving government and public agency responses:
    - update impact assessments to consider impact on consumers of new policy, e.g. nuisance call firms claiming to be affiliated with government initiatives such as energy efficiency schemes
    - ensure government schemes meet best practice e.g. preventing contractors from cold calling
    - amend telephone systems so that Scottish Government outbound calls start displaying their number, and work with other public agencies to do likewise
    - work to improve regulatory solutions
    - develop a scams prevention strategy to ensure a more co-ordinated cross-agency response to all types of scams.

Research undertaken by Antelope Consulting in 2017 looked at the effectiveness of the proposed measures, what impact they would have

on consumers, and made recommendations for the implementation of the Action Plan.[9]

More information: research on nuisance calls action plan impacts

4.3 Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber-crime, although it does not deal directly with the public or businesses in Scotland.

While it does not have investigative powers, the information is passed to the National Fraud Intelligence Bureau who use it to identify serial offenders, organised crime gangs and established as well as emerging crime types.

The Action Fraud website has a large amount of information on types of fraud as well as news and alerts on methods being used by criminals.

It has however limited information on Scotland and they were not able to provide us with any relevant data.

visit the Action Fraud website

4.4 Age Scotland

Age Scotland provide information and advice to people and families, operating a national telephone helpline for the last 20 years and providing printed information and online information for topics popular with older people.

They are also involved in public policy/public affairs influencing work that would have a positive effect on older people.

[9] Effectiveness of actions to reduce harm from nuisance calls in Scotland, Antelope Consulting, March 2018

In particular, they were a member of the Adult Protection Policy Forum (closed 2 years ago after the Adult Protection Support Act was mainstreamed). The Scottish Government lead this Forum and had Financial Harm as one of its priorities. In addition, the Financial Harm Co-ordination Group (currently led by Paul Comely, National Audit Protection Co-ordinator (based at Stirling University), of which Age Scotland is a member, is also being closed by the Scottish Government. Age Scotland also have a Money Advice Service funded project called "Money Matters", which focussed on boosting the financial capability of older people, but this will close in February with the MAS instead focussing its latest round of funding on younger people.

They take part in Scams Awareness Month, but use their own channels to advertise it. In previous years, they sent out 100,000 calendars (in which one month would give advice on how to protect themselves from scams), but Scottish Government funding for this has been discontinued. The calendars were made available through GP surgeries and libraries and every MSP was asked how many they wanted, who then distributed these through their own networks.

They now fund a smaller run of 20,000 calendars, but scams is now not included.

They have been involved in the Police anti-doorstep crime campaign – Operation Monarda, which involved media work, enforcement track-downs, targeting known persons of interest in local areas who get a knock on the door, with high profile arrests being made. They issue their own promotional materials on who may be vulnerable and give advice and guidance at the door.

Age Scotland are trying to get a more structured relationship with Police Scotland, The Pensions Regulator, Pensions Advisory Service

so that people can be referred direct to them and hope this will be in place soon (months, rather than years).

They aim to get the message out regarding doorstep crime and advise older people that if someone comes to their door, to say that they use Care and Repair to undertake any work that is needed, so that they are no longer perceived as a “good mark”.

They also encourage older people to make preparations in advance if they are losing capacity in promoting the use of a Power of Attorney (including setting restricted capacity), which should help in minimising scams when they become vulnerable.

4.5 Age UK

The Age UK network includes Age Scotland, Age Cymru and Age NI and more than 150 local Age UKs throughout England.

Age UK provides information and advice through its helpline and on its website through a dedicated advice portal for scams and frauds. It supports people through information and advice and advises how to spot, avoid and report common types of fraud, particularly those targeted at older people, such as pension and investment scams. There is also advice on the support available for scam victims.

Age UK signposts people who have been victims of a scam in general to Citizens Advice and/or Action Fraud.

Visit the Age UK website

The local Age UKs in addition to providing information and advice also provide other services like raising awareness in the community of doorstep scams and provide support to victims, which in one area involved funded intensive work with a befriending element included.

Work is ongoing from the City Bridge Trust which is funding 4 local Age UKs in London to pilot victim support, raising awareness and scam prevention which may be rolled out across the rest of the UK. This is being done in collaboration with Action Fraud in respect of the media, joint press on romance fraud and reporting fraud.

4.6 Angus Council – Operation Carpus

Operation Carpus was a joint initiative between trading standards, social work and Police Scotland in Angus, which identified those at risk of financial harm through scams and then provided them with support and assistance.

Through the National Trading Standards Board (the England and Wales equivalent of TSS), Angus Council Trading Standards were able to access the details of 193 occurrences on a so called ‘suckers list’ of names and address within Angus known to be susceptible to scams and circulated among criminals.

A screening process took place, removing those known to be deceased, admitted into care homes or moved to other local authority areas. Community police officers then visited the remaining addresses, with 111 visits completed and a feedback form filled out at each. The average age of those visited was 72, ranging from 32 to 95.

Of the 111 individuals visited, 16 (14%) had lost money to scams with a total loss of £155,005 (range of the loss was £25 to an estimate of £100,000).

More than half (55%) of the total, and 81% of those identified as most vulnerable. said they were still receiving approaches from scammers.

The potential savings identified for this small group within the Angus area was £1.5m. The operation also led to improved links between partners for scam prevention and provided a process for future victims. This includes information sharing between the police and trading standards.

4.7 The Banking Protocol

This new scheme is aimed at ensuring **banks** and police are more active in protecting customers. It is being run as a joint venture between the police, Financial Fraud Action - which represents **banks** - and National Trading Standards.

All bank staff are to be trained to spot signs that a customer may be withdrawing cash to give to a scammer.

Police hope the scheme will help reduce financial crime by spotting scams before money has been handed over.

The plan is also to train every single front-facing employee of banks, building societies and Post Offices.

4.8 Citizens Advice Scotland

Citizens Advice Scotland represents 61 member bureaux in Scotland, with 79 offices covering all 32 Local Authority areas.

Last year CAS advised on 590,000 new issues through their bureaux, of which 1203 issues related to scams, with a further 1033 being reported through their consumer helpline.

The Citizens Advice Scotland website provides general advice on spotting and reporting scams. If a victim has been scammed and lost

money, CAS advise them to report directly to Action Fraud or CAS assist them to report the scam.

If however physical violence or threat is involved, CAS encourage people to call the police.

CAS works closely with Trading Standards, and ask clients to phone the consumer helpline or pass their concerns direct to Trading Standards. The consumer helpline also pass client concerns to Trading Standards, who can take criminal action if appropriate.

Citizens Advice scams resources

CAS help organise Scams Awareness Month, a national campaign which takes place in June or July each year to increase awareness of fraud. Scams Awareness Month is done as part of a conglomerate called the UK Consumer Partnership and includes CAS, the Competition and Markets Authority, the Financial Conduct Authority and Trading Standards. CAS takes forward the Scottish part of the campaign.

The 2017 campaign focused on the 'life established' group aged 45-60s, young people, older people (over 70s) and socially isolated people, and sought to tackle underreporting and stigma associated with scams. The campaign ran for four weeks, each week focussing on one group per week.

In Scotland, 56 events were held by local citizens advice bureaux, engaging 7,600 people directly, with a further 65,500 reached through social media. 96 items were also carried in national and local media.

In 2016, the campaign looked at the different methods used by scammers, with 340 organisations being involved across the UK.

Citizens Advice Bureau and Trading Standards work together to put forward national messages to the public, however grant funding is also given to local bureaux so that the message can be tailored to target particular groups within individual communities, with an aim to raising people's awareness early and before they fall victim to a scam.

Campaign materials are distributed through GP Surgeries, libraries, local partners and community groups, coffee mornings, social media and local Trading Standards.

Training is undertaken with Social Policy Co-ordinators to spot social policy cases, of which there were 7000 last year.

All advisors are trained for 6 months and the CAB has an online advice portal (Advisornet) to which they can refer to ensure that advice is the same and consistent across the bureaux.

In addition, CAS has a self-help website called Advice for Scotland.

4.9 Cold Call Ban 2019

The government plans to introduce a pensions cold calling ban. This will not be included in the Financial Guidance and Claims Bill, meaning legislation may be delayed until 2019.

This will cover UK calls only though, and does not cover the EU/outwith the EU.

4.10 Consumer Protection Partnership

The CPP brings together consumer bodies covering all aspects of consumer protection. It represents consumer advocates and consumer law enforcers from all parts of the UK who are uniquely placed to work together to help tackle the issues facing consumers today.

It produces a yearly report which sets out the work that the CPP has undertaken over the previous year on behalf of consumers, and touches on the areas of concern for the coming year where the Partnership will prioritise its efforts.

Consumer Protection Partnership update report 2017

4.11 Crimestoppers

Crimestoppers is a national organisation, based in London, which yearly help to solve and prevent thousands of crimes. Their helpline gives people the power to speak up anonymously about criminal behaviour, crime that has happened or going to happen.

Contacting the Crimestoppers helpline anonymously ensures that the caller will not be contacted by police, be asked to give a witness statement or have to go to court.

Crimestoppers website also provides information on their website about how to avoid being scammed.

They helpline routinely take information about fraud, however scams is not a category that they currently routinely collect information on and is not identified separately. Their range of callers tend to be compared to the general public in terms of spread of age and sex, however there tends to be more calls from BEM groups, who may be more apprehensive about contacting the authorities.

Crimestoppers have a partnership with the Post Office which started as a result of cash in transit crime. Their joint working aims to highlight a whole range of frauds/scams such as romance fraud, medical scams, inheritance scams, prize draw scams amongst their customer base to try and help people avoid being victims. The partnership work closely with Age UK and Age Concern because of the mail scam demographic.

They share any relevant information with Action Fraud, some of which results from Government campaigns on social media, the Take 5 Campaign and Cyber Aware.

4.12 Cyber Aware

This is a Home Office led initiative which provides resources to companies and charities and has a similar message to Crimestoppers, Action Fraud and Lloyds Bank. It undertakes research around the messaging to keep yourself safe online.

This new scheme is aimed at ensuring **banks** and police are more active in protecting customers. It is being run as a joint venture between the police, Financial Fraud Action - which represents **banks** - and National Trading Standards.

4.13 Don’t Be Fooled - Money Mules Campaign

Don’t Be Fooled is a partnership between FFA UK and Cifas. It aims to inform students and young people about the risks of giving out their bank details, and deter them from becoming money mules, where ordinary bank accounts are used to hold and transfer payments on behalf of criminals.

money mules campaign

4.14 East Renfrewshire Prevention Team

East Renfrewshire Council has undertaken a range of activity aimed at tackling scam activity in the area.

In 2012, East Renfrewshire Trading Standards joined up with teams in Angus and East Dunbartonshire to assess the scale of the nuisance call problem, and to run a three month trial of different call blocking technologies.

It was the first time such a project had ever been undertaken in the UK, and following its success, has since been taken up by 150 other local authorities.

Building on this, the council established a dedicated Prevention Team in 2014 which works closely with other service providers (e.g. social work, NHS, Royal Mail and local charities/support networks) with a focus on tackling scams, particularly those targeting vulnerable residents.

This has included leafleting and poster campaigns and media activity to raise awareness of scams, and direct interventions to support those who have been victims or could be potential victims.

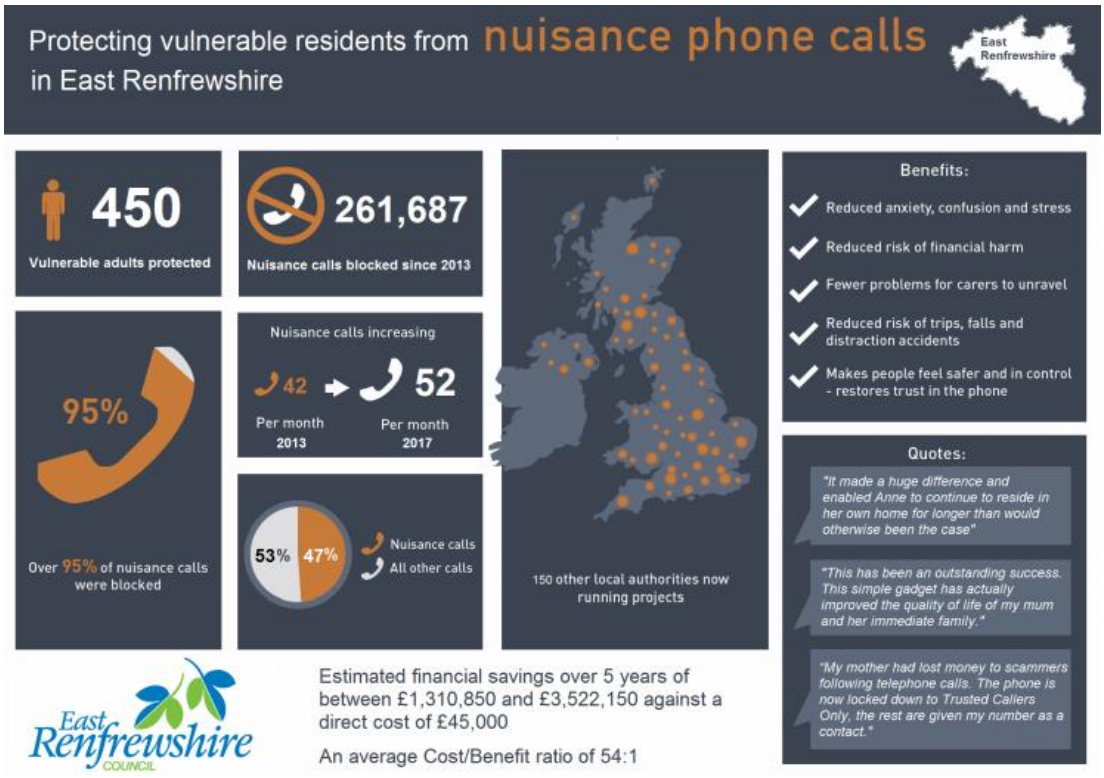
Key interventions have been:

- Call Blocking Equipment: offered free, with a cost to the council of £100 per kit, and rolled out to 500 residents. Over five years, estimated cost savings are in the range of £2,913 to £7,827 per resident, taking into account that it can allow older people in stay in their own homes for longer and reduces social care costs (by creating fewer problems for carers to tackle), as well as the direct savings made by avoiding fraud. The equipment has blocked 95% of nuisance calls, a figure of over 260,000. The infographic below provides more information on the scheme, with figures based on 450 kits being installed, with an estimated cost benefit ratio of 54:1;
- Confidence at Home Packs: 8,964 information packs with 'no cold calling' stickers and advice on avoiding scams were circulated. The council estimate potential cost savings of £100 per pack per resident and £100 per pack for public spending. If one in three packs were used, total cost savings have been estimated at just under £600,000;
- Scam Mail project: the council received 31 referrals regarding mail scams, where victims had lost a combined figure of c. £350,000. After intervention, which has included giving advice to victims and their family on mail redirection, providing links to support groups to tackle isolation and offering call blocker installation, this was reduced to £2,000.

The call blocking equipment used in East Renfrewshire has also provided useful data on the nature of nuisance calls.

In 2017, an average of 52 nuisance calls were received each month per kit, with 6% of participants receiving an average of 100 or more.

Figure 4.6: Impact of East Renfrewshire Call Blocker Scheme



More information can be found at: East Renfrewshire Council - scams resources

4.15 National Trading Standards

National Trading Standards is responsible for gathering important intelligence from around the country to combat rogue traders and tackle a number of priorities. These priorities currently include mass marketing and internet scams, illegal money lending and other enforcement issues that go beyond local authority boundaries.

NTS work closely with mail providers to provide training and guidance on how to identify scam mail. This involves a 2 day training course/guidance, then an audit is undertaken of trainees' opinions on the mail. If the trainer does not agree, the trainee has to go back and retrain. This relationship was borne of early partnership working

between Trading Standards, Fife Council and Royal Mail and has now been rolled out across the country.

They worked intensively to combat scams, with their National Scams Team of 18 now having a database of 300,000 victims and 90% of Local Authorities recording local victim information.

The organisation has both a data team and also a project team who run their campaigns, such as *Friends against Scams*. This involves getting friends/family to identify markers/signs of being a victim (for example through excessive use of their cheque books, loads of mail, loads of calls, other indicators such as not using their heat/light).

On 22 January NTS launched the *1 Million Friends by 2020* campaign and also have other projects, for example, Mail Marshalls which empowers scam victims to take a stand by providing the scam mail which continues to come to them to National Trading Standards.

Working as part of the Joint Fraud Taskforce, this work has included an investigation scheme to stop scam mail getting into the mail system in the first place and to date 9 million pieces of mail have been intercepted.

NTS also works with Banks, the Association of Adult Social Care, Public health, all Local Authorities, Citizens Advice and utility providers.

4.16 Neighbourhood Watch

Neighbourhood Watch's online knowledge database includes advice on how to prevent being a victim of a scam. It also gives other handy resources Neighbourhood Watch scams resources.

This includes links to (amongst others) The Metropolitan Police which gives similar advice to that of Police Scotland on how to identify

scams, how to prevent scams and how to report scams. Metropolitan Police - reporting fraud.

4.17 Neighbourhood Watch Scotland

Neighbourhood Watch Scotland has an online resource for Safer Communities which includes information on scams and provides a link so an individual (after registering) can be alerted to scams in their area.

There is no online reporting link to Police Scotland on the Neighbourhood Watch Scotland website.

Neighbourhood Watch Scotland - scam alerts

4.18 Ofcom

Ofcom work collaboratively with the Information Commissioner's Office. They co-operate with each other, giving technical advice and pass on information and seek advice on investigations which are underway.

They are also involved in *Project Falcon* with the Metropolitan Police which looks at scams enabled by telecoms, and work the National Crime Agency and City of London Police.

This includes trying to combat spoof numbers and smishing.

They are working collaboratively with the banks and telecom providers to update these messages to stop scams, as currently text message accumulators on mobiles will put these messages in with legitimate messages from your bank.

Ofcom also liaises with Finance UK to try to understand the scale of the problem as their customers complain to them if they have been scammed.

They are looking at the rules which are used to determine whether a website is legitimate or not and are also looking at incoming messages, data analytics and the use of AI.

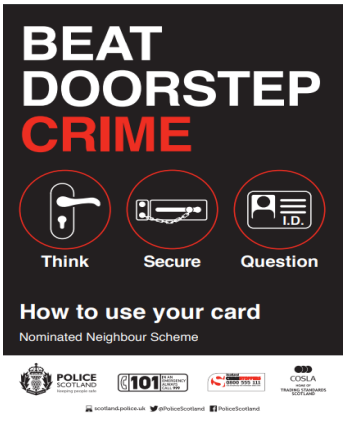
Authentication through third party certification is going to be extended to telephony. This is a new feature of telecoms which is being implemented throughout the world, recognising the danger of being able to put any identity into any phone call.

The authentication protocol will be rolled out over the next 3-5 years and will work in the background. This will identify any person who is not who they say they are and will help address the problem. North America and the USA are implementing this over the next 18 months or so, however there are a number of conditions which are president one of which is not enough people are on the new technology (ie SIP lines). Everyone has to be on SIP lines for this to work, so this could take up to 5 years to address.

They have put a number of measures in place (no detail provided) which have led to a decline in bulk calls which can lead to some criminal behaviour but mostly not.

4.19 Police Scotland

The Police Scotland website offers an overview of common types of fraud, how to avoid falling victim to them, and details on how to report fraud.



Police Scotland - fraud victims support

In 2014, Police Scotland ran a Beat Doorstep Crime campaign, with online advice and leaflets and posters made available. As part

of the campaign, a Nominated Neighbour Scheme was established in cooperation with Trading Standards Scotland. The scheme is aimed at over 60s and provides a mechanism whereby a neighbour is contacted in the event of an unexpected doorstep call. The neighbour then verifies if the caller is genuine and, if so, accompanies them to the house.

Police Scotland - beat doorstep crime campaign

4.20 The Pensions Regulator

The Pensions Regulator has an online resource which gives advice on how to protect yourself from being the victim of a pension scam and are working to raise public awareness of the issue.

The Pensions Regulator - Pension Scams advice

TPR acts as lead for *Project Bloom* and work closely with government, regulators, financial services bodies and criminal justice agencies through their *Scorpion* campaign to disrupt and prevent scams. This joint work includes investigation, arrest and prosecution, issuing executed warrants and closing down fraudulent websites. Individuals reporting scams to the TPR are directed to Action Fraud as the central point of collection. From there intelligence is matched with anything else they have or other partner who has an ongoing case.

Organisations they work with include the National Crime Agency, Serious Fraud Office, City of London Police (incorporating Action Fraud and the National Fraud Intelligence Bureau), regional police, regional crime units, Financial Conduct Authority, Insolvency Service, Solicitors Regulatory Authority, the Information Commissioner's Office, HMRC, DWP, the Treasury, Money Advice Service, Pensions Advisory Service, Pension Wise, industry groups, pension providers and administrators, the Pensions Liberation Group.

The Pensions Regulator provide campaign materials for use in transfer packs for those with pensions worth more than £30,000, however this is just provided and not mandated.

The TPR have taken action to ban people from acting as trustees of pension schemes over suspicions that millions of pounds were scammed from investors using schemes of which they were trustees. These people gambled scheme assets on high risk investments that are now worth a tiny fraction of what was put into them.

They have also alerted the public to rogue pension websites carrying anti-scam messages to try to trick consumers into believing that they are legitimate businesses.

4.21 Scam Smart

ScamSmart is a Financial Conduct Authority campaign providing information on how to avoid investment and pension scams.

As well as general advice, a drop down menu lists common types of investment/pension scam and provides information on the risks related to specific kinds of scam. There is also a warning list of firms to avoid and a link to the FCA's registered of regulated firms.

4.22 Take Five

Led by the FFA and backed by the government and a wide range of partners, Take Five is a national campaign that offers advice to help protect consumers from preventable financial fraud, including phone, email and online fraud. The campaign is based on the idea that preventing fraud 'can be as simple as encouraging people to take a moment to stop and think'. The advice is focused on helping consumers and businesses to spot the signs of fraud.

Take Five campaign

4.23 Telephone Preference Service (TPS)

The TPS is a free service which enables consumers to opt out of receiving unsolicited calls for direct marketing purposes, maintained by Ofcom and enforced by the ICO.

Research into the effectiveness of the TPS was undertaken in 2014[10], involving a randomised panel keeping a diary of all unwanted calls, comparing those using TPS and those without it. Key findings were:

- over two periods of four week research, those who became registered with TPS saw a larger decline in the number of live sales/marketing calls than those who did not; and
- almost half (45%) of those registered with TPS received no nuisance calls, compared with 26% of those who were not.

TPS covers more than half of households in all but one local authority area of Scotland (Eilean Siar), with a national average of 73%.[11]

4.24 WHICH?

Which? is a membership organisation which, as well as giving advice on product Best Buys/Don't Buys are all about championing consumer rights.

They launched a campaign about two years ago which looked at the UK Government's Joint Work taskforce.

They had noticed a theme within frauds which centred, in particular, around bank transfers (which are non-refundable and could be for a life-changing sum of money). In the last year or so they have been looking at what the regulator is currently doing and what more can be

[10] Ofcom & ICO – Research into the Effectiveness of the TPS, Ipsos Mori, 2014
[11] Effectiveness of actions to reduce harm from nuisance calls in Scotland, Antelope Consulting, March 2018

done by the regulator to stop consumers falling victim and being left out of pocket.

They put in a Super Complaint to the Payment Systems Regulator as no-one was recording this type of fraud and it was not much of a priority to the banking industry as it was not liable. As a result of the Super Complaint the industry now has to provide statistics and is getting better at reporting/sharing data. The first set of statistics from January to June 2017 showed that between January-June 2017 over £100M was lost by consumers (including businesses), with only £25M being reimbursed.

Which? works closely with Action Fraud and City of London Police, but also work with other charities – primarily Age UK – and have links with Trading Standards, Cyber Aware, the Home Office, Take 5, and the Consumer Protection Partnership.

Their work in Scotland has been primarily around nuisance calls. This is a separate campaign but is linked because nuisance callers could potentially be scammers too.

They have historically spent much time looking at payments systems and how scammers exploit these. They are now looking at campaigns going forward which looks at where other businesses in the chain can protect consumers eg Air BnB rentals – scammers ask individuals to contact them off the Air BnB website, so they lose the guarantees and protections on the website.

5. Stakeholder Inputs

5.1 Introduction

This Chapter presents the wider views and insights gathered through an extensive series of interviews with a wide range of organisations with a locus in the area of scams and frauds. In total we spoke with over 30 organisations and 40 individuals across a range of organisations.

Appendix 3 provides details of those organisations interviewed.

The interviews were conducted using an agreed topic guide which covered the following broad topics:

- introduction and organisation description;
- initial thoughts/ background research;
- types and incidence of scams;
- financial and other impacts;
- current preventative measures;
- governance and partnerships;
- future interventions; and
- further thoughts or insights.

The remainder of this Chapter sets out the outputs from these interviews.

One key point to highlight is the legal framework within which fraud/ scams exist with some aspect being devolved to Scotland while others (financial regulation) remain reserved matters.

5.2 Stakeholders Overview

Details of the organisations interviewed covered a wide range of focus including:

- legislative/policy making;
- regulatory agencies;
- enforcement agencies
- consumer groups;
- trading standards;
- financial networks; and
- individuals interest groups

It is clear that there is a wide range of organisations with an interest in frauds/ scams although these tend to be focused mainly on addressing their own particular audience. Other than government there is no single organisation which has a catch-all brief of operations covering all of the UK.

In a UK context, the Home Office has established the Joint Fraud Taskforce[12] to co-ordinate activity. The main partners are:

- Action Fraud
- Take Five - To Stop Fraud
- National Trading Standards
- Financial Fraud Action UK
- Cifas
- National Crime Agency
- Victim Support
- Cyber Aware
- National Cyber Security Centre
- National Fraud Initiative

[12] The previous National Fraud Authority was dissolved in 2014

Note: Action Fraud is the UK's national fraud and cyber-crime reporting centre but currently is limited in representing Scotland.

5.3 Overview and Context

There is a strong consensus that fraud/ scams are a growing and significant problem in Scotland.

- Criminals [scammers] are now more organised[13]
    - The activities of criminal groups rely on significant levels of planning and co-ordination. Business structures are to be found within fraud networks including chains of command, defined roles and remits, suppliers and service providers.
    - Fraudsters are networking online to share information and build criminal enterprises across the UK and overseas. Criminal tactics are constantly changing, as the criminals respond to our interventions and take advantage of new opportunities.

Criminals are more technically capable

- Criminals exploit the latest technology in a number of ways. They compromise computers to steal personal and financial data, both from individuals and in bulk. They use social networking to build trust with potential victims who are then duped or coerced into providing information needed for fraud or to pay money to fraudsters. Devices are used to disguise voices for telephony-based frauds.

- Criminals increasingly operate across borders

[13] Fighting Fraud Together: Strategic Plan to Reduce Fraud UK Home Office

- Frauds affecting the UK are often linked to networks of criminals operating across the UK and overseas. Fraudsters are also investing significant time and resources to hide their criminal profits. The Financial Action Task Force estimates that fraud is now the second biggest source of global money laundering. The increased efficiency of international financial transactions and variety of financial products means that funds can be moved across continents swiftly through different channels.

5.4 Scale and Scope

It is seen as increasingly difficult to “pin down” the costs of fraud/ scams and there is no central or single definition or repository of information. For example, some estimates are made by the finance industry but only in relation to bank and card frauds/ scams, while others only consider pension or doorstep crime data.

Notwithstanding this the strong consensus is that whatever the actual costs - it is a BIG number.

There are also issues around unreported fraud or scams - some of which while scams may not constitute an actual crime. There are also issues of double counting with different datasets using the same data to produce their own figures.

In addition to direct financial costs (to individuals) it is recognised that there are real knock on impacts in terms of:

- health and social care costs;
- regulatory and consumer standards costs;
- crime reduction costs;

- marketing and awareness raising costs.

There is no real sense of what the actual costs are although some attempts highlighted earlier have attempted to put a figure on these indirect costs.

An issue which was raised time and again was the impact of fraud/ scams on vulnerable or older people - see below.

5.5 Vulnerable and Older people

According to Age UK[14], more than 5 million people a year in the UK are victims of scams but only 5% of scams are reported. Also

- 80% of phone scam victims are over 55 years of age[15]
- the average age of a postal scam victim is 74 years[16].

While anyone can fall victim to a scam, older people can be at greater risk because scammers tend to target people who:

- live alone;
- are at home during the day;
- have savings or valuables; and
- are more likely to talk to them.

In addition, some older people might be suffering from dementia, which could affect their decision-making process or they might also feel lonely, which might make them more likely to talk to people.

[14] Age UK 'Only the tip of the iceberg', published 2015
[15] Financial Ombudsman - Calling time on telephone fraud 2015
[16] National Trading Standards. BBC news report - average age of scam victims

5.6 What is being done to address the problem

There is currently a wide range of initiatives (highlighted earlier) but they are generally focused on particular groups or with particular messages or for certain types of scam/fraud.

While we were able to identify many of these we are sure there will be other examples which were not drawn to out attention. Some points for consideration:

- many use different language to deliver the same message;
- there are many different delivery channels such as on-line, mass marketing, TV/Radio, leaflets and flyers, individual contacts, events, etc;
- there are different approaches using mass marketing or a targeted approach with the belief being that both are necessary;
- there is a strong move to enlist a wider society approach for example through engaging with bank tellers, postal delivery workers, retail staff and using Council communications[17];
- there are a few examples of some of the organisations coming together in a "partnership" but these are generally limited in membership or very specific in focus.

It is clear that there is already much going on to address the problem although we have no sense as to how effective this approach actually is in practice.

Finally we would highlight the "political" nature of the problem. Some of the aspects in relation to regulation are not devolved to Scotland but

[17] For example Police Scotland have been sending information leaflets out with Council tax renewal letters

remain with the UK. This will limit the potential for the Scottish Government to address some of the issues highlighted below which would require to be addressed at a UK level.

5.7 Addressing the Problem

Introduction

This Section considers how to continue to address the problem and is based around the views, opinions and insights presented by the organisations/ individuals interviewed for the research.

Combating Isolation

Scamming can happen as a result of social isolation which can happen to anyone at any age. This leads to some individuals having no-one to turn to, to discuss concerns or receive advice before they are scammed. In fact, even after an individual becomes aware that they may be a victim of a scam, they may continue the harmful relationship with the scammer or repeat their actions, as they have such a strong psychological need to prove themselves right.

Being scammed can have such a strong psychological impact on a victim that they may lose their confidence and may even become afraid of answering their door or no longer make their own financial arrangements. They surrender their independence and autonomy because of their experience. In addition, there could be impacts on their physical health and could affect their behaviour and may start drinking or drink more excessively, stop seeing people, lose or gain a lot of weight or self-medicate.

There are other not so obvious indicators that someone could have become the victim of a scam, and this could include a drastic decrease

in the amount of energy used by the victim as they can no longer afford to heat their home, or they perhaps stop answering the phone to legitimate callers as they are afraid it may be a scam, which further leads to social isolation.

Not only are there several and multiple impacts on the individual who is the victim of a scam, but there is also a societal cost. One statistic provided by a consultee is that an elderly individual who is defrauded in their own home is 2.5 times more likely to go into care or to die within a year[18]. This adds to pressure on public services, the NHS, the social care system, pension credit, and welfare benefits where people have lost their money.

Suggestions made to combat this include:

- the roll-out of a similar scheme to that adopted by Age UK which included a befriending element;
- the re-introduction of Community Policing as in the past, these officers would have known who the vulnerable people within their communities were, would have been a local point of contact and someone that could individuals could approach in confidence (this is of particular importance where perhaps familial abuse of trust is concerned);
- encouraging communities to be a bit more inclusive in including vulnerable people;
- using respite care facilities more to educate older people and those with disabilities with regards to scams;

[18] Source: National Trading Standards Scams Team

- involvement of utility companies to early identify those customers who may be at risk.

Encouraging Reporting

Stakeholders have identified that scammers are successful, in some part, due to the embarrassment or stigma of those who have been scammed not coming forward.

In addition, as some older people have either dementia or cognitive impairment, this may alter society's perception of what being old means, despite the fact that true mental decline does not happen until the last few months of an individual's life. This inaccurate perception can also impact on older people's willingness to come forward.

To counter this, it has been suggested that campaigning approach (perhaps in the same form as that used to encourage people to come forward for bowel screening, or to catch cancers earlier). This could be in the form of posters, TV or radio.

We are conscious that General Practitioners do broach the subject of Power of Attorney for those individuals who may have cognitive impairment but still have capacity to sign a Power of Attorney, and this should be encouraged, rather than legislated.

Doorstep Interventions

Police Scotland, Age Scotland and UK, Neighbourhood Watch, and Local Authorities and others continue to work to combat doorstep scams and to get the message out, this is however hampered by limited budgets and varying competing priorities.

It has been suggested that this could be combated in part by the re-introduction of Community Police, more so for those people who may

perhaps be housebound or those who interact less with the outside world.

Familial/Abuse of Trust Interventions

This is a difficult area to solve, as this mostly happens “behind closed doors”. It could be something as simple as a son doing his mother’s shopping on a weekly basis, spending say £35 on messages, and retaining £15 for himself for cigarettes/drink to large scale abuse where thousands of pounds may be diverted from an elderly parent to a grown up child’s bank account. This may be as the child is the parent’s carer and feels that they have “earned it”. Equally, the perpetrator may not be a member of family, but someone who has inveigled themselves into a trust relationship with the individual.

Non-familial abuse in its various forms are discussed further below, however of most import in combating familial abuse are Adult Support and Protection within the Local Authorities and Social Care Partnerships. Their work ensures that individuals do not suffer financial harm from what are sometimes their “nearest and dearest”. Government needs to ensure that Councils/NHS Scotland have sufficient budgets to ensure that they can continue to provide this protection.

Financial Controls

While the Banking Protocol is quite effective, it is also patchy and works less well in some parts of the country compared to others. It only applies to in-branch transactions and we believe that it would be useful to extend this to telephone or online banking. Use of AI or customer profiling may have to role to play in this.

The loss of bank branches will undoubtedly have an effect on the number and type of these scams, as local knowledge of regular

customers is lost. To counteract this, we are aware that some banks do direct customers from branches that have closed to the local Post Office and this should be further encouraged.

Work is ongoing by the Baking regulator with regards to payments architecture and confirmation of pay. This is currently voluntary for business to offer to their consumers, although it is mandatory if a bank receives a request from another bank. It was suggested that perhaps this should be made compulsory for all transactions.

In addition, last November the Banking Regulator announced that they would be introducing a contingent reimbursement scheme. This scheme looks at who was at fault and who could have done more. The scheme needs to be clear for thresholds, for standards, and what the consumer has done and what banks need to have done to show that they have done everything that they have to stop a scam.

We are unsure if there are any other stakeholders involved in this scheme but it has been recommended that encouragement of early action by the Regulator to bottom out how the scheme will work in practice.

Internet Interventions

With regards to internet fraud, it has been suggested that as well as the current efforts being made that encouraging intergenerational contact ie grandchildren teach their grandparents how to send an email, how to spot a scam, and gain general internet “savviness”.

This could also help combat some scams and educate older people on how to spot adverts (which can sometimes contain scam content as was evidenced in the charging for renewing TPS), rather than free content.

One particular example relates to Romance Fraud. There is potentially a greater role for dating websites in terms of spotting fraudsters with fake profiles using their systems, making it easier for users to be able to spot fraud and report it. In addition, some Fraud originates through Facebook through scammers setting up false profiles. This is a company with large resources, that could have an important role and that could be doing more.

There is perhaps a role for Government to play in tighter regulation of social media and internet platforms which are currently not see as being robust enough. These multi-million pound international companies could be the platform that scammers choose to use, and responsibility should fall at their door for due diligence when individuals are using these services to sell or sell a service which, when it fails, could lead to financial harm.

There is no doubt that as each generation is become more technologically aware, the increased use of the internet for a range of tasks, including (but not limited to) business, research and education purposes, personal banking and to engage in social media, etc increases the risk posed by scammers. Some time has passed since the introduction of the internet 28 years ago and over time it has become the norm for individuals to sign up to end user licence agreements (EULAs) in order to be able to access various software programmes.

However in order for individuals to now be able to access online services and use certain apps, they have had their personal data commoditised i.e. in order to be able to use a service and/or app they may have to give access to their contacts, location, messages, microphone, camera, metadata related to phone calls and SMS, and browsing history.

This personal data is sometimes given away at the “click of a mouse” with few taking time to read the terms and conditions and or the privacy policies of app providers. This is influenced in no small part by the unwieldy length of these documents, and a design akin to a EULA being used to “settle the nerves” of even the most privacy-concerned user.

Little or no thought is given to how this personal data may be used in future or how it may be shared (potentially with third parties/global third party providers or contractors who may not have the same data protection legislation as the UK/EU). Similarly, individuals may not be aware of how their personal data can be used to profile them, not only by legitimate sources but also by those who may intercept it nefariously.

With the introduction of the General Data Protection Regulation on 25 May, it is hoped that this will go some way to better protecting individuals’ data. However, there will be an ongoing role for government in directing policy, best practice and prevention campaigns to not only make individuals more aware of the impact of the “click to join”, “click to agree” buttons (and the sometimes too easily earned but not always justified trust we have in software/app providers), but also to have an influence on the sometimes unnecessary commoditisation of individuals’ data.

Pension Interventions

Pension scams can happen as a result of pension schemes being set up with the purpose of scamming people. All that is required is that a Trustee can pass the HMRC and regulator bar. There are no real barriers to entry and you don't have to be deemed fit and proper. Legislation should be tightened up to ensure that all Trustees are properly vetted prior to being appointed.

Authorised Financial Advisors details are available from the FCA website and appear as "Active" if a search of their name is undertaken. However there is no facility to check if an FA is "passporting". This is where an individual may be working for a legitimate company but they may be operating illegally within the UK.

It has been suggested that the FCA close this potential loophole by ensuring that individuals who are passporting can also be checked on the FCA website as well as domestic providers.

Postal Services

Royal Mail have been collaborating with many of the stakeholders we have spoken to during the consultation process, however they are legally constrained in what they can do. They have had successes in stopping big shipments at airports from overseas, however cannot currently do the same for the domestic market. We would postulate that most scam mail is posted using Response Services Licences or another Royal Mail product.

As these Licences and their stationery have to be approved by Royal Mail prior to use, could not the same apply to the content of large bulk mailings (perhaps over 250 items)? This could also be applied to their "Walk Sort" items.

The use of “No cold calling” zones could be widened and made easier.

Telephone Interventions

With regards to telephone scams, earlier introduction of SIP lines to all households will ensure that domestic scamming is reduced significantly, if not eliminated totally. In addition, the work being undertaken by the banks and mobile providers with regards to text message accumulators will also help.

This is not the case for non-domestic calls and we would encourage governments to work together with their foreign counterparts and their telecoms providers to find a solution.

Justice for Victims

The Courts could play a stronger role, as currently, in particular where the perpetrator of a scam is given a community payback order rather than a custodial sentence, this can reflect negatively in personal and community confidence. The disposal does not reflect the gravity of the situation and sends the wrong message out. This happens, despite the use of victim impact statements.

One of our consultees suggested that if someone “fleeces” a member of family for £100k, public expectation would be that you should go to jail and that they were never surprised by a sentence in court.

This can have a reputational impact on collaborative crime prevention/intervention/ care and support as the public will generally see that the system is not working correctly.

Joining it all Up

There is a feeling that there are many players and also a disjoint between the various groups trying to tackle scams/frauds in that:

- BEIS is responsible for mass marketing;
- the Home Office is responsible for fraud;
- the Department for Culture, Media and Sport (who fund Scotland too) are responsible for nuisance calls which are also scams;
- the Department for Health;
- Local Government Association – Social Services and Local Authority responsibilities;
- Ministry of Justice – sits above social care and public health;
- Office of the Public Guardian.

The general feeling is that everybody is in the same space talking about the same thing, but calling it different things, and there is no real strategy between these organisations. The message needs to be consistent.

Consultees highlighted a confusion about who owns what in cyber enabled crimes ie from the National Crime Agency, City of London Police, local police Forces, to Action Fraud, and that policing has really struggled to have a comprehensive response to it.

In addition, there appears to be challenges about policing response to fraud i.e. from frontline officers, to dialling 101 – the response is to report to Action Fraud, who take your details, put you on a database, and that no-one knows what to do, or use or investigate at a local level.

A comment was made that Police are still using 20th century tactics to solve 21st century crime and that all Police officers now need to be able to understand online crime as much as offline.

Some of the above suggestions have no cost implications and others may have significant cost implications,

6. Conclusions

6.1 Conclusions

The brief set out the research requirements as follows:

- to review evidence and develop an assessment of the cost to Scotland's economy of scams;
- to identify existing preventative measures and strategies designed to protect people from scams, both in Scotland and across the UK;
- where possible, to quantify the social and financial impacts of these preventative interventions; and
- provide recommendations of interventions that are likely to offer the greatest return for preventative spend.

Our research conclusions against each of these is detailed below.

6.2 Cost of Scams

We would concluded that it is currently not possible to identify the "true cost" of fraud or scams as any data or estimates will vary significantly depending on the scope of the analysis and what is being counted, data sets being used and the method of data collection.

There are also issues around how robust the data is and the sources used to arrive at estimates or the assumptions used in their calculation. Our analysis has shown that:

- different data sets include different types of definitions (e.g. only cyber);
- some data includes individual and business and public while others do not;

- some data is based on surveys with limited responses and unknown sample frameworks;
- the data is based on that reported to the organisation publishing the data;
- there are different levels of geographical coverage; and
- it is not always clear which groups are included (individuals, businesses etc) or what is being counted.

However, it is important to be able to make some estimate as to the scale of the problem and based on the Annual Fraud Indicator report highlighted in Chapter 3, it was suggested that (at a minimum) the cost of fraud/scams to individuals in Scotland could be around £560 million.

However this excludes fraud/ scams on businesses, public sector or the charity/ third sector AND the cost of policing/ regulating/ addressing it AND the high level of unreported incidences. At a high level we would suggest that fraud/scams cost the Scottish economy many billions of pounds with the problem likely to continue into the long term.

6.3 Preventative Measures and Impact

The problem of scams/ fraud are well recognised and are already being addressed by a range of policy/ legislative organisations/ regulators/ individual sectors/ public sector/ Police and Crime/ support organisations and consumer groups.

As was highlighted earlier, there are a wide range and type of intervention already being delivered but again these a multi faceted some with particular target groups and some only dealing with particular types of fraud/ scam.

We do not intend to repeat the information provided in Chapter 5 which provides a comprehensive list of the kinds of interventions already under way.

We have been unable to find any evaluation evidence or monitoring of the effectiveness of current interventions which would allow us to comment on effectiveness.

Anecdotally, most of the organisations delivering preventative measures believe they are making a positive difference.

This is an issue which we return to in the next section of the report.

6.4 Recommendations

In considering recommendations it is clear that it will not be possible to totally eradicate fraud/ scam activity – so we start with a real challenge. As one interviewee said – “new laws or regulations won’t stop the bad guys”.

There is a strong view that it will not be possible to either legislate or regulate to fully address the issue and this must be complimented by preventative, awareness and education approaches.

Section 5.7 highlighted some of the approaches to mitigation which are currently being delivered together with how these might be expanded. In a more generic perspective we would suggest the following recommendations.

- Scottish Scams Prevention Forum
    - provision of a “policy forum” for all interested organisations to come together and give a profile to activities. Roles could include:
        - co-ordinate activities
        - share best/ other practice
        - develop common language / messages
        - agree targeted approach for different groups
        - clarify roles and responsibilities
- Better Understanding of the Problem
    - better quality data collection to understand the scale of the issue and changes over time
    - share data/ research

    - central repository for research

- Measure effectiveness and impact
    - develop monitoring and evaluation protocols and framework
    - develop common set of indicators
- Using technology
    - support for cyber technology development in Scotland
    - technology awareness
- Engaging wider community
    - build on current activities through training front line staff
    - widen groups to include retailers and public sector

Appendix 1: Organisational Footprint

Action Fraud

- Action Fraud is the UK's national fraud and internet crime reporting centre.

Age Scotland (UK)

- Age Scotland is the leading charity representing older people in Scotland and supporting their rights and interests. They provide information and run awareness campaigns on the issue.

Alzheimer Scotland

- The leading dementia organisation in Scotland. They campaign for the rights of people with dementia and their families and provide an extensive range of innovative and personalised support services. They offer advice and run campaigns in relation to scams as it impacts on individuals.

British Retail Consortium (BRC)

- The BRC is the lead trade association representing the whole range of retailers, from the large multiples and department stores through to independents. The provide research and advice to their membership.

Cheque & Credit Clearing Company (C&CCC)

- The industry body that manages the cheque clearing system in Great Britain, including the processing of bankers' drafts, building society cheques, postal orders, warrants and government payable orders.

Cifas

- Cifas is a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime.

Citizens Advice [and CA Scotland]

- Online free advice from Citizens Advice to help you find a way forward, whatever the problem.

Crimestoppers

- An independent UK-wide charity working to stop crime. Currently working with Post Office Limited to prevent elderly victims from being conned like this

Direct Marketing Association

- Membership organisation with a network of more than 1,000 UK companies. They provide industry best-practice guidelines, legal updates and a code that puts the customer at the heart. We represent a data-driven industry that's leading the business sector in creativity and innovation.

Financial Conduct Authority

- FCA is the conduct regulator for 56000 financial services firms and financial markets in the UK and the prudential regulator for over 24000 of those firms. Provide protection in relation to bank accounts to mortgages, credit cards, loans, savings and pensions.

Financial Ombudsman Service

- The official independent expert in settling complaints between consumers and businesses providing financial services.

Financial Fraud Action UK

- A constituent part of UK Finance, responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK.

Fraud Advisory Panel

- The FAP is an independent voice of the anti-fraud community. They champion best practice in fraud prevention, detection, investigation and prosecution. Membership includes public, private and third sectors.

Fraud Defence Test

- An online quiz that can be used to assess your vulnerability to becoming a victim of fraud and cyber-crime and steps you can take to better protect yourself.

Friends Against Scams

- A National Trading Standards Scams Team initiative that aims to protect and prevent people from becoming victims of scams by empowering communities to... 'Take a Stand Against Scams.'

Get Safe Online

- A joint initiative between the Government, law enforcement, leading businesses and the public sector. The aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely.

Home Office

- The Home Office is the lead government department for immigration and passports, drugs policy, counter-terrorism and police.

Insurance Fraud Bureau

- The IFB is a not for profit organisation funded by the insurance industry, specifically focussed on detecting and preventing organised and cross industry insurance fraud.

Money Advice Service

- The Money Advice Service helps people manage their money. They do this directly through their own free and impartial advice service. They also work in partnership with other organisations to help people make the most of their money. They are an independent service, set up by government.

National Crime Agency

- National body dealing with serious and organised crime, plus computer crime.

National Trading Standards Scams Team

- Helps tackle mass marketing scams and disrupts the operations of perpetrators behind mail scams. It works in partnership with agencies across the country to identify and support victims of mass marketing fraud.

Pension Regulator

- TPR is the UK regulator of workplace pension schemes. They work with pension scheme trustees, scheme managers and employers to help protect workplace pensions.

Royal Mail

- Reporting scam mail - Potentially fraudulent mail should be reported to Royal Mail:

SAFERjobs

- SAFERjobs (Safe Advice for Employment and Recruitment) is a non-profit, joint industry and law enforcement organisation created in 2010 to raise awareness and combat criminal activities that may be attempted on those seeking a job, or through the services provided by the recruitment industry.

ScamSmart

- ScamSmart gives consumers tips on how to spot and protect themselves from investment fraud, and hosts the FCA Warning List.

Scottish Business Resilience Centre

- The Scottish Business Crime Centre is a non-profit making organisation created in 1996 under the Business Crime Reduction Strategy for Scotland, to establish a unique partnership approach between the police, business community and Government.

Telecommunications UK Fraud Forum

- A forum for the exchange of information and the promotion of a united effort against telecommunications fraud.

Trading Standards Scotland

- Operationally, TSS has a duty to coordinate and enforce cross boundary and national casework as well as undertake the specialist functions of tackling illegal money lending and ecrime. It is a resource intended to add capacity to local authority trading standards teams in these areas of activity.

The Scottish Police Authority

- The Scottish Police Authority (SPA) is a public body of the Scottish Government which holds Police Scotland, the national police service, to account.

UK Finance

- UK Finance is a new trade association which was formed on 1 July 2017 to represent around 300 firms in the UK providing credit, banking, markets and payment-related services. The new organisation brings together most of the activities previously carried out by the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Which?

- Which? has more than 1.5m members and supporters, making it the largest independent consumer body in the UK. It supports consumers and campaign on more to be done to reduce incidence of scams

Appendix 2: Types of Fraud and Scams

Sources: Action Fraud UK; Citizens Advice; WHICH; National Trading Standards; Scamwise; Financial Fraud Action UK; Police Scotland

Advance Fee Fraud

- This is when a payment is made to fraudsters who claim to be in a position of authority, such as a foreign government official, to transfer money or for a promise of employment, wealth or gifts.

Brexit Scam

- This is where people are being phoned up to see if they are European Citizens. It plays on people's fears and is advising them that they have to pay extra for this or that. It's a relatively small problem currently, but is worsening over time.

One Ring and Cut (Wangiri Scam)

- This involves a fraudster calling a mobile phone at random and then hanging up after one or two rings. After seeing the missed call an individual calls back but are connected to a premium-rate recorded message based overseas.

Lottery Scams

- The scam involves being informed of a non-existent lottery and in order to receive the prize victims must send some money or personal information in advance.

Counterfeit Cashiers Cheques

- Fake cheques are given as payment for goods/services over the actual value. The victim then refunds the purchaser with the excess payment prior to the cheque being discovered as fraudulent.

Dating Scam

- This happens when a victim is befriended romantically and over a period of time is convinced to send money to their new love for a variety of emotive reasons.

Fraud Recovery

- This is when fraud victims are targeted by criminals posing as recovery agents, claiming to be able to recover their lost money, in order to get personal details and additional money.

Inheritance Fraud

- Fraudsters send out a mass mailing to people who share the same surname. Each one is told there is cash from an inheritance that has been located in their name and in exchange for personal information or money, the agent can take forward their claim.

Medical Scams

- Victims are tricked into paying for tablets which claim to cure disease and or dietary products which claim to enhance weight loss. These products as well as being ineffectual could have potential safety issues as they are often ordered through the internet from non-domestic sources who may not have the same screening of such drugs/products as in the UK

Rental Fraud

- Victims are tricked into paying upfront fees/rent for the rental of property which either does not exist or is not for rent. In some cases properties are rented to multiple victims at the same time.

Other Advance Fee Frauds

- This is when fraudsters contact victims and persuade them to pay an upfront fee for a service that does not exist. Common examples of this fraud include cold call offers to make PPI claims on a victim's behalf for a fee, or an offer of employment that requires a fee for security checks.

Lender Loan Fraud

- A situation when a victim receives a cold call offering them a loan that has been arranged for them for a fee. Fraudsters will ask victims to send money (usually via an electronic medium) but no loan will materialise.

Share sales or Boiler Room Fraud

- Boiler room fraud is a fraud where victims are cold-called by fake stockbrokers and encouraged/persuaded to buy shares or bonds in worthless, non-existent or near bankrupt companies.

Pyramid or Ponzi Schemes

- Pyramid schemes are scams in which investors are promised abnormally high profits on their money. These schemes encourage investors to recruit new members to increase earnings from a scheme which is unsustainable.

Prime Bank Guarantees

- This is an investment scheme where the victim is offered discounted bank guarantees with the promise of a high return when they have been resold. The victim is encouraged to send money to a foreign bank where it is eventually transferred to an off-shore account that is in the control of the fraudster.

Time Shares and Holiday Club Fraud

- Fraudsters will contact a victim at home, often by phone and tell them they have won a 'free' holiday. These holidays are not free and can involve fees for extras. Sometimes victims are also forced to attend a presentation on a holiday club.

Other Financial Investment

- This fraud consists of a range of investment opportunities to convince victims to part with their savings. The word "investment" is widely used in connection with a wide range of schemes offering income, interest or profit in return for a financial investment.

Online Shopping and Auctions

- This involves a product being advertised for sale through internet shopping and auction sites that either does not exist or doesn’t match the original description. This also includes when a legitimate seller does not receive payment for goods sold online and is unable to contact the purchaser.

Consumer Phone Fraud

- This happens when victims are targeted through missed calls, text messages and ring tone scams. These contacts are to

make unsuspecting victims respond via premium rate telephone calls and SMS messages.

Door to Door Sales and Bogus Tradesmen

- Bogus tradesmen, door-to-door sales or doorstep fraud involves fraudsters trying to scam victims after knocking at their door. Such frauds involve promoting goods or services that are either never delivered to you or are of a very poor quality.

Other Consumer Non Investment Fraud

- This fraud occurs when victims are shown, or test a product that is not received, false or stolen. An example of this fraud is when a car is purchased by a victim who finds out that it is actually stolen, or a victim who buys a laptop only to find out the bag is empty.

Computer Software Service Fraud

- A fraud which involves the victim being contacted and told that there is a problem with their computer and for a fee this can be fixed. No fix actually occurs.

Ticket Fraud

- Ticket fraud occurs when a victim purchases a ticket in advance over the phone or internet, only to discover that the tickets are not valid or never received. This can occur for concerts, events, flights, etc.

Retail Fraud

- This is fraud committed against retailers. It is committed through refund fraud, label fraud or when goods are ordered with no intention of paying. It does not involve plastic card sales, cheques or purchases online.

Charity Fraud

- This occurs when fraudsters organise the fraudulent collection of money using names of genuine charities or fictional ones.

Fraudulent Applications for Grants from Charities or Lottery Fund Organisations

- This fraud occurs where charities have provided grants based on false information, or where they have received grant applications that contain false representations and so no grant was paid.

Banking and Credit Industry Fraud

- This is when fraud is committed against a bank or financial institution using a false identity, credit or debit cards, cloned cards, cheque books or online accounts.

Cheque, Plastic Card and Online Bank Accounts (not PSP)

- This fraud occurs when there is fraudulent use of a cheque, plastic card or online bank account. This does not include companies that deal with electronic money transfers.

Application Fraud (excluding Mortgages)

- This occurs when fraudsters open an account using a stolen identity or false information.

Mortgage Related Fraud

- This fraud covers a wide range of deceit, from simple overstatement of income to planned abuse by organised crime groups.

Mandate Fraud

- This happens when fraudsters get victims to change a direct debit, standing order or bank transfer mandate. They do this by pretending to be an organisation a victim makes regular payments to e.g. a business supplier.

Dishonestly retaining a wrongful credit

- This fraud occurs when money is received wrongfully or in error, and the recipient decides to keep or spend the credit instead of alerting the most appropriate authority.

Insurance Related Fraud

- Insurance fraud is where policy holders obtain money or replacement goods through false insurance claims or obtain policies by submitting false details.

Insurance Broker Fraud

- This is where victims get insurance cover from a broker or fraudsters pretending to be brokers. When a claim is made or the policy checked, they discover that they are not insured, or the cover is not the same as they thought they paid for.

Telecom Industry Fraud (Misuse of Contracts)

- This is when contracts are obtained by fraudsters from service providers, using false details or stolen identities with no intention of paying.

Corporate Employee Fraud

- This is where employees or ex-employees obtain property or compensation through fraud. It also covers the misuse of corporate cards and expenses.

Corporate Procurement Fraud

- This occurs when excess goods are ordered using company funds and then sold on by the fraudsters. Or where goods of a lower quality are delivered to those paid for, with the offenders pocketing the difference.

Business Trading Fraud

- A person is guilty of an offence if they knowingly carry on business trading with the intention of defrauding creditors or for any other fraudulent purposes.

Accounting

- False accounting fraud happens when company assets are overstated or liabilities are understated in order to make a business appear financially stronger than it really is.

Bankruptcy and Insolvency

- Fraud relating to bankruptcy and insolvency can involve companies fraudulently trading immediately before being declared insolvent, or phoenix companies.

Passport Application Fraud

- Passport fraud occurs where fraudsters obtain or try to obtain a United Kingdom passport by false representation to the HM Passport Office.

Department for Work and Pensions Fraud

- This fraud occurs when benefits given out by the Department for Work and Pensions are claimed fraudulently.

Distraction Burglary

- This normally involves more than one perpetrator. The individuals pretend to be from a utility company and/or the Local Authority. They gain access to someone's property. One individual will keep the victim busy, while the other steals their money and/or jewellery, with the victim may only becoming aware of same sometime after they have left.

Familial Abuse/Trust Abuse

- This occurs where a member of family and/or friend could asked by the victim to perhaps shop for them and/or perhaps use the victim's bank card to withdraw funds. Goods could be bought for less than the amount charged and/or money retained by the friend/family member.

Fraudulent Applications for Grants from Government Organisations

- This is where Government funded Organisations have provided grants based on false representations or where they have received grant applications that contain false representations and so no grant was paid.

HM Revenue and Customs Fraud

- This fraud occurs when fraud is commitment against HM Revenue and Customs.

ITunes Vouchers

- This is where someone has done a google search to apply for a loan. Part of the application procedure involves the company asking an individual to prove they have the capacity to set up eg standing orders and/or buy an iTunes online. The voucher is purchased and nothing is heard of the company again who converts the vouchers into cash.

Pension Fraud by Pensioners (or their Estate)

- This is where the pension provider is defrauded by a pensioner or by the pensioner‘s estate following their death.

Pension Fraud committed on Pensioners

- This is where the pensioner is the victim of fraud on their pension.

Pension Liberation Fraud

- This is where a pensioner is persuaded to ‘liberate’ their pension early for a large cash sum. The payment is considerably smaller than they expected because of fees and taxes.

Other Regulatory Fraud

- This crime type is used to record fraud from regulators that is not covered elsewhere. Examples would include fraud against the Land Registry, Insider Dealing at the stock exchange, or the Gambling Commission.

Fraud by Failing to Disclose Information

- This fraud occurs when there is a failure to disclose information by an individual to another person when they have a legal duty to so. An example of this fraud could be when a solicitor fails to disclose information to one client to benefit another.

Abuse of Position of Trust

- This is when someone abuses their position of authority or trust against another person, for personal or financial gain, or to cause loss to another.

Computer Viruses\Malware\Spyware

- A virus is a computer program that can replicate itself and spread from one computer to another by using code. It is usually sent over a network/internet or introduced to a computer on a disk drive or memory device. Malware/spyware can also collect information or data from infected devices and pass them on to another device.

Denial of Service Attack

- A denial of service attack (DoS attack) or distributed denial of service attack (DDoS attack) is an attempt to make a website or email address unavailable to its users. These types of attacks bring these networks down by flooding them with useless traffic.

Denial of Service Attack Extortion

- This occurs when a victim is blackmailed with a threat of a denial of service attack.

Hacking – Server

- Computer hacking is the unauthorised modification of any computer server. It is usually committed by persons illegally accessing the server, but it can be committed by persons with lawful access to the computer as well.

Hacking – Personal

- Computer hacking is the unauthorised modification of someone's personal computer. It is usually committed by persons illegally accessing the computer, but it can be committed by persons with lawful access to the computer as well.

Hacking - Social Media and E-mail

- This crime is the hacking of any form of email accounts and social media accounts, for example Twitter and Facebook.

Computer Hacking – PBX/Dial Through

- A private branch exchange (PBX) hack is a remote attack on telephone systems that contain features such as call forwarding, voicemail and divert.

Hacking (Extortion)

- This occurs when a victim is blackmailed with a threat of computer hacking.

Other Fraud (not covered elsewhere)

- Other frauds are where false representation or obtaining services dishonestly have occurred that aren't covered in other crime types.

Trusted agent phone scams

- These cold call scams typically involve fraudsters deceiving people into believing they are speaking to member of bank staff or other trusted agency

Premium rate number scams

- Premium rate number scams try to snare people who are searching online for telephone numbers of government advice services. Here's the lowdown...

Tax scams

- The first quarter of any new year sees an increase in fraudulent tax emails, appearing to come from HMRC. Don't be fooled by these scam tax emails.

Door to door scams

- Can take many forms, but instead of relying on the anonymity of online communications, they simply knock on your door. While they can be investment and pension scammers as well, they can also try and scam in a more practical way –selling a product or service. EG a person claiming to be a builder who happened to notice some damage to your roof when they were passing. Fake charity collectors and salespeople are other examples.

Smishing

- Text message based scam. Scammers will contact you claiming to be from your bank saying you need to update your personal details, or there is some kind of issue. The text might contain a link (like a phishing scam), or a phone number to call. The phone number is fake and, when you call, the fraudsters will attempt to get you to reveal your details.

Pharming

- Similar to phishing, but instead of sending you an email directly, the scammers target the website you are visiting. You type in the correct website address, but you then get directed to a fake version, where you inadvertently put in your login details and secure information.

Pension scams

- Since the pension freedoms were introduced in 2015, retirees are able to access large sums of money from pension pots. An unfortunate side-effect has been this group is now being targeted by scammers because they can potentially access large amounts of cash. Pension scams will usually follow a similar path to investment scams, with contact normally being made by telephone.

Investment scams

- Generally a phone based scam, although you might be targeted in other ways, such as email or people coming round to your front door. Although investment scams vary, the principle remains the same. You are encouraged to hand over money to invest in a company or product, which in some cases doesn't

exist. In other cases it could be that the investment does exist but involves a portfolio scam or blended exotic investment (eg Brazilian Rain Forest/tea trees) gives cashback or cashback in the guise of commission. In general these are long term investments where people are locked in for 5 years and although there might be warning signs after year 2, you can't get your money out.

Psychics and clairvoyants

- You may receive a letter from a psychic or clairvoyant offering to reveal something to you in exchange for money. Sometimes these scams are used to set you up for lottery scams by giving you lucky numbers. The letters may be sinister or threatening.

Pyramid schemes

- You may be invited to invest in a business with high returns and low risk. You have to pay to join and you get rewards for recruiting other investors. You may get some small payments at first to persuade you to invest more but usually the investment is worthless or doesn't exist.

No hang-up phone scam

- The scammers ring posing as someone from a reputable organisation, then tell you to call the organisation (eg your bank) to verify what they're saying and give them your personal details. The scammer will pretend to hang up while you do this, but they'll keep the line open – you'll think you have got through to the organisation but you'll still be talking to one of the scammers. They can use fake dialling tones so you don't notice anything is wrong

Holiday fraud

- This type of fraud is increasing. Scammers sell non-existent holidays or holiday add-ons. They'll often encourage you to pay by direct bank transfer away from a main holiday booking site – perhaps by saying you'll get a better deal if you book that way. You might only realise you've been a victim when you arrive at your destination and find the booking doesn't exist

Missed call

- Scammers may use automated systems to dial numbers very briefly, leaving a missed call on your phone. Calls are often from numbers starting 070 or 076. They are actually premium rate numbers and if you call back, you'll be charged a high rate for making the call. Scammers also send text messages to mobile phones that seem like they're from an ordinary individual trying to contact their friend. If you call or text them back you'll be charged a high rate

Copycat websites

- You search online for a Government service such as passport renewal, driving licenses or European Health Insurance Cards. You click on the first website in the search results. It looks legitimate. In fact it's a copycat website and you end up paying more for a service that should have been free or much cheaper

Fake solicitors and legal services scams

- You have received a letter or email from a solicitors firm you do not use, or about a legal matter you are not aware of. The correspondence looks legitimate. They offer legal services in return for a fee or claim that legal action has been taken against

you that you must pay to settle. Often the legal firms are fake, or a fake person claims to work at a legitimate firm.

Miracle health cures

- Miracle health cures or ‘scientific breakthroughs’ offer health products to cure a problem such as arthritis, diabetes, or cancer, or to help you lose weight. These are also known as "snake oil" remedies. The seller often promises a no-risk money-back guarantee or a free trial. There are often quotes from doctors and happy customers. These types of products and medicines are unlikely to do you much good, and might even harm you. Talk to your GP before you buy any of these products.

Telephone Preference Service Subscription

- This particular scam focusses on cold calling consumers who had previously signed up to the TPS to be told their subscription to the service was running out. The caller would then ask the victim to supply their credit or debit card details to renew their TPS subscription (a free service). In some cases the caller already had some of the victim’s personal details (such as name, address and telephone number) which made the contact seem more plausible.

Appendix 3: Stakeholders Interviewed

Organisation
Action Fraud
Adult Protection Services
Age Scotland
Age UK
Alzheimer Scotland
Angus Health and Social Care Partnership
Citizens Advice Scotland
Clackmannanshire and Stirling Adult Support and Protection
Crimestoppers Scotland
Direct Marketing Association
Federation of Small Business
Fife Council
Financial Conduct Authority
Fraud Advisory Panel
Get Safe Online
Information Commissioners Office
Money Advice Service
Money and Mental Health
National Centre for Social Research
National Trading Standards
Ofcom
Police Scotland
Royal Bank of Scotland
Scottish Business Resilience Centre
Scottish Commission for Learning Disability
Society of Chief Officers of Trading Standards in Scotland [SCOTSS]
The Pensions Regulator
Trading Standards (Aberdeen Council)
Trading Standards (West Dunbartonshire Council)
Trading Standards Scotland [COSLA]
UK Finance
WHICH?

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80004-843-0 (web only)

Published by The Scottish Government, March 2021

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS845826 (03/21)