Money & Pensions Service

THE BEHAVIOURAL INSIGHTS TEAM

June 2023

PENSION SCAMS IN THE UNITED KINGDOM

Evidence review

Contents

Acknowledgements

We would like to thank MaPS' MoneyHelper team, Aviva, the Financial Conduct Authority, Legal & General, The Pensions Regulator and other professionals for the interviews and for sharing their invaluable experiences. Most importantly though, we thank those with personal experiences of scams for their courage to share their stories with us - this is not an easy thing to do and their input was invaluable.

List of acronyms

Acronym	Full Title
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ASIC	Australian Securities & Investments Commission
BIT	Behavioural Insights Team
CAFC	Canadian Anti-Fraud Centre
DWP	Department of Work and Pensions
FCA	Financial Conduct Authority
FSCS	Financial Services Compensation Scheme
FTC	Federal Trade Commission
HMT	HM Treasury
MaPS	Money and Pension Service
NCPQSW	The National Centre for Post-Qualifying Social Work
NFIB	National Fraud Intelligence Bureau
OECD	Organisation for Economic Co-operation and Development
ONS	Office of National Statistics
PSG	Pension Safeguarding
PSIG	Pension Scams Industry Group
QROPS	Qualifying Recognised Overseas Pension Schemes
TPR	The Pensions Regulator

Executive summary

About this report

In 2021, reports of pension scams increased by 45%, with fraudsters stealing over £2m from people in the UK in just 6 months (Action Fraud, 2021; FCA, 2021). This is also likely to be a significant underestimate of financial losses, as the Financial Conduct Authority (FCA) estimates that less than 1 in 5 scams are reported. However, there is little rigorous evidence on what governments and the industry can do to reduce pension savers' susceptibility to fraud.

This report presents the findings from an evidence review on: the scale of pension scams; the impact on those affected; the types of scams and tactics used; key risk factors; and current trends. It also recommends actionable and evidence-based strategies and interventions that the Money and Pension Service (MaPS) and other stakeholders can adopt to lower the risks of scams and offer better support to those affected.

We combined this review of the academic and grey literature with interviews with six people affected by scams and ten professionals working for pension providers or MaPS helplines, as well as conversations with relevant Government and regulator teams.

Headline findings

Evidence on the true scale of pension scams is limited (Section 3.1): Measuring the scale of pension scams in the UK poses challenges due to underreporting and inconsistency in data collection. Scams are grossly underreported, with those affected by scams often taking years to realise and report the incidents. Additionally, there is inconsistency and gaps in data collection because different actors use varied databases and definitions. This lack of clarity inhibits governments and the industry understanding the true prevalence of pension scams in the UK.

The financial and emotional cost of pension scams is high (Section 3.2 - 3.3): Once a pension saver realises they have been affected by a scam, they may experience feelings of self-blame and shame for spending weeks, months, or even years confiding in a scammer. The impact of scams goes beyond financial loss, potentially leading to a loss of confidence and trust, detrimental health outcomes and breakdown of relationships with family and friends. People who have been affected by scams are more likely to need financial support and public services such as social care, all of which can amount to significant impacts on the economy.

Scammers adapt their techniques to the context (Section 4.1 - 4.2): Changes in regulation, technology and external events lead to the types of scams evolving constantly. For example, the ban on cold-calling in the UK has led to scammers using targeted ads on social media or contacting pension savers from abroad. Reports of fraudulent activities and

computer misuse crimes have increased by 25% since 2020. Importantly, while always unethical, not all scams are illegal. However, it is impossible to present comprehensive up-to-date evidence on current trends because of the underreporting and data gaps. Frontline staff working for pension providers are often the first ones to identify new approaches. Potential future trends identified by our interviewees working in the sector include a surge in pension liberation scams when the minimum age to access pensions increases from 55 to 57 in 2028 and the exploitation of the new pension dashboard as pension savers become aware of their smaller pots and might share this information with the scammers.

Scam tactics are subtle and seamless (Section 4.4): Scammers use a variety of techniques to target pension savers, execute the scam and avoid detection. Though the tactics used to trick pension savers are complex and varied, behavioural sciences can offer insights into what these techniques look like; why they are effective; and how to reduce people's susceptibility to these tricks. For example, scammers often tell their targets that an opportunity is scarce, that they must act now to protect their savings or make the most of an opportunity, thereby exploiting people's tendency to see scarce opportunities as more valuable and their desire to avoid a loss.

Scams can happen to anyone (Section 5): Understanding who is more susceptible to being scammed and why is crucial to prevention. Risk factors include having higher levels of education; being overconfident in their ability to make sound financial judgments; approaching retirement but dissatisfied with their future income; and struggling with stress or isolation. However, the group of those affected is highly diverse, making early identification very difficult. Ultimately, anyone can be affected by scams. Once an individual has been targeted, there is also a significant risk of re-targeting. This can be linked to recovery fraud (where scammers exploit pension savers' search for redress), the characteristics and circumstances that make an individual likely to be a 'super target', or the sharing of previous targets' contact details between scammers.

What works - proposed solutions

MaPS and other pension scam prevention/ victim support organisations in the UK - such as pension providers - have at their disposal a range of touchpoints which lend themselves to interventions informed by the evidence presented in this review. Combined with already existing approaches, they can provide strong protection against scams.

Objective 1: Preventing Scams

While effective awareness campaigns can provide a first layer of protection, successful prevention will rely on impactful interventions at critical points when pension savers are about to make a decision related to their pension. We propose:

1. Introducing an additional point of reflection after the Pension Safeguarding Appointment required to complete a flagged transfer request and delivered by MoneyHelper[1],

[1] MoneyHelper joins up money and pensions guidance across a number of channels, including a website and helplines, bringing together MaPS' support services.

2. Increasing the salience of the risk of a transfer in communication with the pension saver,
3. Supporting pension savers to take alternative safer steps to make progress towards the financial goals they are seeking to achieve,
4. Involving the pension savers' social network (i.e. their family and trusted friends) to challenge their decision, either when the transfer request is made or when the individual comes closer to retirement age,
5. Creating teachable moments through spoof campaigns, and considering (by relevant authorities) the introduction of government-backed independent advice.

Objective 2: Encouraging those affected to seek support

In addition to mitigating the negative impact on individuals' wellbeing and offering opportunities for recovery of (some of) the funds, encouraging uptake of support services can help with the detection of ongoing scams. We propose:

1. Simplifying access to support, in order to lower the burden placed on those who want to seek redress, for example by assigning a dedicated caseworker,
2. Reducing stigma by avoiding terms such as 'victim' and involving people with lived experience in support provision,
3. Encouraging the social network to refer those affected for support.

Objective 3: Lower the risk of being affected by a pension scam more than once

To lower the risk of secondary scams, we propose:

1. Making the risk more salient at touchpoints such as the Pension Loss Appointment delivered by MoneyHelper, and
2. Implementing ideas such as a dedicated caseworker to reduce the risk of individuals seeking help from illegitimate claims management companies.

Supporting people at risk of 'super targeting' would likely require:

1. Involving the social support network,
2. Checking in after completion of an amber-flag transfer to help individuals spot a scam early - potentially limiting the damage.

Conclusion

This report presents evidence-based insights on pension scams, combining existing literature with insights from interviews with affected individuals and industry professionals. The key findings underscore the significant impact of scams on the lives of those affected, including individuals who took extensive precautions in their pension decision-making and thus eroding confidence in the financial services industry. Similar to investment scams, pension scams are found to exploit the fears and needs of savers. The findings also highlight the methodological challenges in estimating the problem's scale but emphasise the valuable contribution of sector professionals as a source of information on future trends that should be shared across the industry. Implementing the proposed ideas can strengthen the existing services of MaPS, while a collaborative multi-agency approach is crucial for optimising defence capabilities and providing comprehensive support.

1. About this report

1.1 Background

In 2021, **reports of pension scams increased 45%**, and **fraudsters stole over £2m from people in the UK in just 6 months** (Action Fraud, 2021; FCA, 2021). This is likely to be a significant underestimate of financial losses, considering the Financial Conduct Authority (FCA) estimates that less than 1 in 5 scams are reported. However, we do not have a detailed understanding of the scale and nature of pension scams. There is also little rigorous evidence on what governments and the industry can do to effectively reduce pension savers' susceptibility to fraud.

The Money and Pension Service (MaPS) therefore commissioned the Behavioural Insights Team (BIT) to review the evidence around pension scams in the UK and worldwide to better understand the problem of pension scams. This report presents the findings from this review as well as solution ideas for how MaPS can contribute to preventing scams and to better support those affected.

This report aims to investigate the scale, nature, and causes of pension scams in the UK, along with the tactics employed by offenders and the regulatory gaps they exploit. Additionally, it explores various types of scams, their interactions, and emerging trends. Our objective is to identify individuals at risk of pension scamming, understand their key characteristics, and assess the impact of scams on pension savers affected and the economy. Furthermore, the research investigates effective strategies to prevent scams and address the needs of vulnerable groups.

The research methodology, including research questions, approach, and limitations, is detailed in Appendix 1. Our study involved a comprehensive review of both academic and grey literature, supplemented by interviews with individuals affected by scams, as well as professionals from pension providers and government bodies.

The rest of this report is structured as follows: Section 2 introduces a definition of pension scams. Section 3 presents the evidence on prevalence of scams and the impact on those affected and on the UK as a whole. Section 4 provides an overview of types of scams and tactics, and what trends have been seen in relation to this. Section 5 outlines what we know about who is most likely to be affected by scams. Section 6 presents ways to prevent scams and to better support those affected, drawing on the evidence from this review and the behavioural science literature.

2. Definition

Pension scams come in various forms, ranging from ethically questionable practices, to violations of financial regulations, to criminal fraud. Regardless of their legality, the impact of pension scams on those affected can always be significant. Moreover there is no consensus on the definition of a 'pension scam' with even the word 'scam' seen by some to trivialise the issue (TPR, 2022). For the purpose of this evidence review, we use the definition agreed in a government consultation (2017) led by HM Treasury (HMT) and the Department for Work and Pensions (DWP).

Pension scam definition:

'The marketing of products and arrangements and successful or unsuccessful attempts by a party (the 'scammer') to:

- *release funds from an HMRC-registered pension scheme, often resulting in a tax charge that is not anticipated by the member (A)*
- *persuade individuals over the normal minimum pension age to flexibly access their pension savings in order to invest in inappropriate investments (B)*
- *persuade individuals to transfer their pension savings in order to invest in inappropriate investments where the scammer has misled the individual about the nature of, or risks attached to, the purported investment(s), or their appropriateness for that individual investor.' (C)*

This definition encompasses a range of harm to savers, including the most prevalent forms of harm, although it does not reference fraud (TPR, 2022).

(A) are known as **pension liberation scams**. They involve convincing individuals under 55 to **transfer** their **pension from a legitimate scheme to a fraudulent one** established by the scammer, in order to access their savings. This often results in a complete loss of assets and a significant tax bill of 55% of the funds withdrawn, as access to pensions before the age of 55 is only permitted in rare circumstances.[2]

(B) and (C) are **pension-related investment scams**. With (B), the scammer convinces pension savers over the age of 55 to **withdraw money** from their pension scheme and invest it in either fraudulent investments (with the scammer taking the money) or legitimate but high-risk investments (such as overseas property and hotels or cryptocurrency), with the scammer charging high fees for their unsuitable advice. With (C), pension savers under 55 are convinced to **transfer their whole pension scheme** to one where their savings can be accessed and invested in similarly financially detrimental schemes. There are many variations of these scams, which we describe in Section 4.

[2] After the age of 55, savers are typically allowed to make withdrawals from their pension fund including 25% as a tax-free lump sum.

3. Scale and impact

3.1 What is the extent of the problem? *Noting the challenges of measuring the scale of the pension scams, such as* ***underreporting*** *and* ***inconsistency and gaps in data collection****, we find two ways of estimating the* ***prevalence of pension scams in the UK****:*

- *Looking at the* ***total pension assets vulnerable to scams,*** *which yield a high-end estimate of £2.5tn. These assets tend to be through private sector schemes, where liabilities are backed by an asset pool, compared to a typical public sector scheme consisting of unfunded defined benefit entitlements.*
- *Combining the* ***data from surveys, reports to fraud/ scam helplines, or enforcement agencies,*** *which yield more conservative estimates. Between March 2019 and February 2020, 1.9 million UK adults lost money to scams (not all of them are related to pensions). In 2022, just 253 crime reports were made to Action Fraud.*

3.2 How do scams impact those affected?

- ***Finances.*** *In 2018, the average financial loss reported by an individual affected by pension fraud was £82,000. Pension savers affected told us they were resigned to a less secure and comfortable retirement, delaying their retirement date or planning to sell their home to fund their retirement.*
- ***Confidence.*** *Being tricked by a scam can undermine a person's belief in their ability to make good financial decisions, negatively impacting on their ability to rebuild their savings.*
- ***Well-being.*** *Scams significantly harm an individual's physical and mental well-being. Shame, embarrassment and self-blame are common responses. Many individuals become depressed, with some reporting feeling suicidal.*
- ***Relationships with friends and family.*** *Those affected often try to keep the financial loss a secret, resulting in increased stress and distrust when the truth is revealed or when family members attempt to prevent repeat cases.*

3.3 What are the wider impacts?

- ***Economy.*** *Widespread fraud can negatively affect assessments of a country's safety as a reputable financial centre, in turn impacting business and trade.*
- ***Society.*** *Organised crime groups are involved in pension scams, providing challenges to law enforcement.*
- ***Public services.*** *Scams strain public services by shifting the cost of care for the elderly onto the public balance sheet. Dementia patients are especially vulnerable to scams, adding pressure to community and residential care services.*
- ***Younger generations.*** *A rise in pension scams would require younger generations to forgo more of the current income to support older generations and fund their own retirement.*

3.1 What is the extent of the problem?

Difficulties associated with estimating scale

One of the objectives of this review was to estimate the scale of the problem in the UK. However, our own research and conversations with experts confirmed that there are two significant challenges associated with this: (1) **underreporting:** scams are significantly underreported and even for those that are eventually reported, this often happens years later; (2) **inconsistency in data collection:** data is captured by a variety of actors in different databases and using different definitions.

Underreporting

Similar to other forms of fraud, pension scams are vastly underreported, which scammers exploit to evade detection. (This is discussed further in Section 4.4). For people affected by scams, the reasons for underreporting include lack of awareness of the scam and embarrassment. Pensions are long-term investments that people tend to ignore until they approach retirement age. As a result, it can take several years before someone realises they have been scammed (FCA, 2017b; Action Fraud, 2021).

"And the advisor came back and he sent me an email ... [The advisor says 'The market has] been down ..., and blah blah blah, give it six months to the next review, and we'll see where we are.' I said 'Fine, no problem'. So that was like 2017. And then I got the statement through and lost money again" - Person affected by a scam

Furthermore, people affected by scams often feel a sense of embarrassment or have been manipulated by the scammer to not report. Surveys that target the population in general may encourage more honest reporting; however, they usually only cover a recent time period (e.g. the current year) and would thus not capture scams that happened in the past which the person affected has only recently become aware of. Pension providers, on the other hand, are not required to report suspected scams (TPR, 2021). One interviewee suggested some may be reluctant to do so in case it creates an impression that pensions are not safe (Pension professionals interviews, 2023). In 2021, the Pensions Minister wrote to approximately 90 more pension schemes requesting that they share scam data with Pension Scams Industry Group (PSIG), the industry's voluntary group (currently 51 organisations participate), in an effort to address underreporting by providers and gain a clearer understanding of the scale of the problem (DWP, 2021).

Inconsistency and gaps in data capture

The second challenge is that there is not a single source of information on the number and type of pension scams. Rather, there are multiple sources each containing part of the issue, attempting to capture the scale of the problem in different ways. These include:

- **Reports of scams** by those affected to Action Fraud, the police, the ombudsman

services, the FCA and various MaPS helplines.
- **MaPS** reporting on guidance appointments.
- **Data held by pension providers.**
- **Data captured via the FCA's Financial Lives survey**, with the latest available data covering 2020.
- **Data captured on fraud by the Crime Survey of England & Wales**, with the latest available data covering the year ended 30 June 2022.

Determining the extent of pension scams in the UK is challenging, firstly, due to different organisations labelling data differently. This makes it very difficult to match data across databases. For example, the figures reported by the police and the pensions industry do not agree, which is partly due to the distinction between the funds lost to 'illegal activities' and those lost to 'unethical practices' (that are not illegal). Additionally, there is no clear separation between pensions scams and other forms of investment or financial fraud (TPR, 2021) - some (but not all) pension scams are also investment scams, and vice versa.

Secondly, adding up data that is held by different actors might lead to double counting. For example, a scam recorded by a pension provider and also reported to Action Fraud might be counted twice. In addition, reporting data, such as the data held by Action Fraud or the MaPS helplines, captures past scams. Scams that happen today may only be reported in a few years' time, which prevents the sector from getting a real-time picture of both the scale and, importantly, trends in tactics.

MaPS offers several services for people who have been or might have been affected by pension scams. These services include Pension Safeguarding (PSG) appointments, which take place when a pension provider raises an amber flag on a pension transfer that could be a scam[3]; Pension Loss appointments; and a Financial Crime helpline for individuals who may have been affected by a scam. MaPS collects various data from these services that provides a real-time indication of potential scams, such as the number of appointments made and calls received by its helplines.

More granular information is available from amber and red flag data which is, for example, used by the government and regulators for estimation purposes. The only reliable and complete databases sit with the providers. Additionally, it comes with caveats: firstly, it only covers pension transfers, but not the withdrawal and reinvestment of funds. Secondly, it

[3] A pension provider has the power to flag a transfer request as "amber" when (1) the member has not provided a complete response to a request for evidence to demonstrate an employment link or overseas residency, (2) the member has provided a complete response to a request for evidence but is unable to demonstrate an employment link or overseas residency, (3) high risk or unregulated investments are included in the scheme, (4) the scheme charges are unclear or high, (5) the scheme's investment structure is unclear, complex or unorthodox, (6) overseas investments are included in the scheme, (7) you are aware of a sharp and unusual rise in the volume of transfers going to the same scheme or involving the same adviser. A pension saver requesting a transfer that is flagged amber has to attend a Pension Safeguarding Appointment with MaPS to receive further guidance. A pension provider has the power to flag a transfer request as "red" if (1) the member has failed to provide the required information, (2) the member has not provided evidence of receiving mandatory guidance from MoneyHelper, (3) a person may have carried out a regulated activity for the member relating to the transfer without the appropriate regulatory status, (4) the member has requested a transfer after unsolicited contact, (5) the member has been offered an incentive to make the transfer, (6) the member has been pressured to make the transfer. A transfer with a red flag is blocked (MaPS, 2021). The flag criteria are being reviewed by the DWP.

captures heterogeneous reporting habits. From our conversations with professionals, we know that there is significant variation in the percentage of transfer requests that different pension providers flag. While some of them might reflect differences in the profiles of pensions and customers, at least some of this variation is due to different interpretations of the regulation requiring them to flag suspicious transfers. Additionally MaPS will only know why an amber flag was raised if the consumer tells them, but the consumer may not remember or even know. Different pension providers have different policies for disclosing this information. Some providers never provide the rationale because they are concerned the scammer will coach the consumer on what to say to MaPS. On the other hand, some always provide the rationale so that the consumers can receive more tailored guidance from MaPS.

We have attempted to visualise the data gap in Figure 1: the orange striped area represents the scams committed in 2022 that are never captured; the red striped area represents those that will eventually be reported, but potentially only years later. The crucial point is that we don't know the actual size of these areas, making it impossible to give a concise estimate of the scale of the problem. Below we outline the estimates of successfully committed and attempted scams available at this point.

Prevalence of pension scams in the UK

Skidmore (2020) estimates that, annually, pension savers are estimated to suffer £4bn in losses.[4] However, this is only one of many numbers attempting to estimate the prevalence of scams in different ways.

One set of data sources provide estimates of the scale of potential scams: in 2016-18, pension savings amounted to £6.1tn, representing 42% of total household wealth, surpassing other sources such as property and financial savings (ONS, 2018). Of this £6.1tn, it is estimated £2.5tn is theoretically vulnerable to scams, as it is backed by an asset pool rather than consisting of unfunded defined benefit entitlements[5,6] (Skidmore, 2020). Estimates provided by industry experts vary between 5% to 50% of transfers raising concerns.[7] This

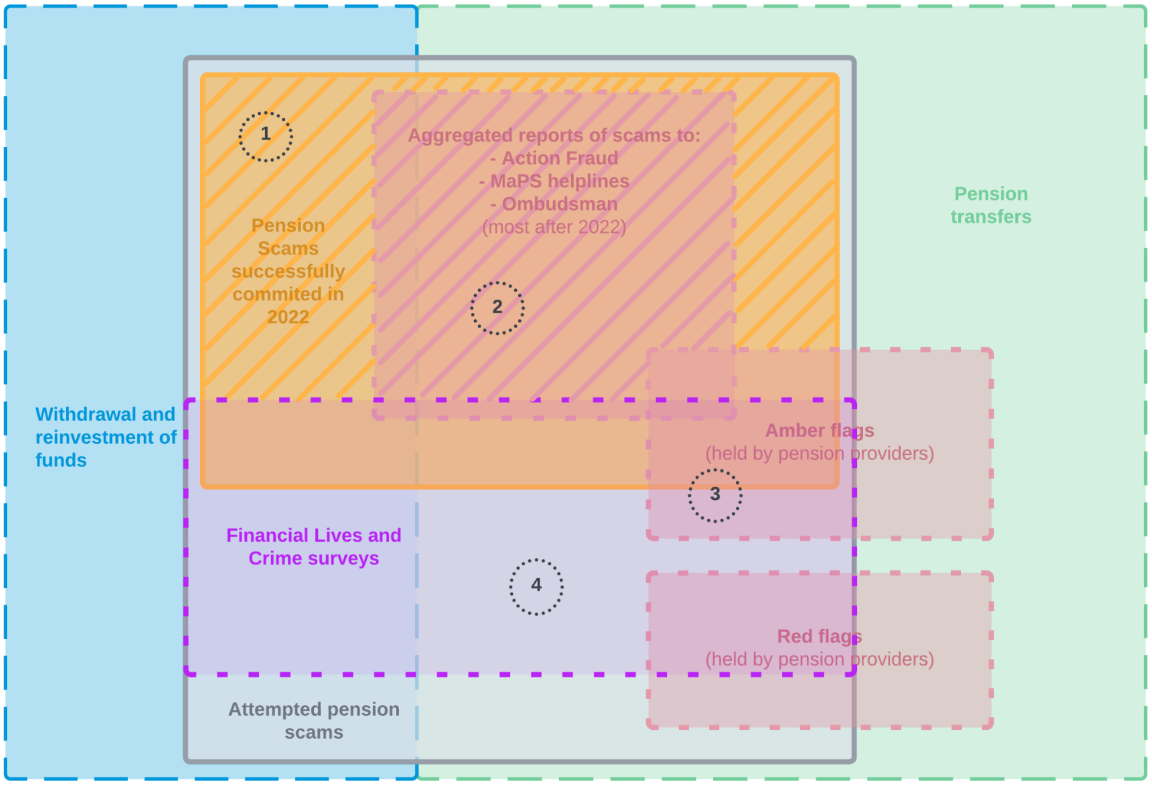
[4] This figure is based on the volume of pension transfer requests received by three pension providers assessed to have contained at least one characteristic that may indicate a pension scam; these are risk markers adopted across industry to aid frontline practitioners in identifying a scam, including the role of an unsolicited sales call, unregulated intermediaries, or members displaying limited awareness of the recipient scheme or adviser (PSIG,2018).

[5] Skidmore (2020) estimated that the £2.5tn are split between £1.7tn in backing-funded defined benefit pensions (excluding the Local Government Pension Scheme), £250bn in contract- and trust-based defined contribution (DC) schemes, £420bn in non-workplace DC and £119 designated for drawdown.

[6] Since April 2015 members of unfunded defined benefit (DB) pension schemes have only been able to transfer to another defined benefit scheme.

[7] These numbers are based on a consultation led by The Pensions Regulator (TPR) and the National Fraud Intelligence Bureau (NFIB), with one respondent estimating that less than 5% of transfers raise concerns, while another stated that up to 50% of transfers may result in negative outcomes for the member.

Figure 1: Data on pension scams in the UK, committed in 2022.[8]



disparity is likely due to differences in the definition of transfers considered problematic and differences in the schemes and members based across the industry (e.g. a large administrator vs. the trustee of a single scheme) (TPR, 2022). DWP collected data directly from pension providers for the calendar year 2022, covering 290,000 completed transfers - that is, either transfers that went ahead, or that have not and will not go ahead. Of these transfers, 2,400 (i.e. less than 1%) received an amber flag. Of all amber flag transfer requests, 96% went ahead. The most common amber flags were those raised by (1) an overseas investment being included in the receiving scheme; (2) a high-risk or unregulated investment being included in the scheme; (3) the scheme charges being unclear or high. Only 300 transfers received a red flag, with almost 50% of these cases being linked to incomplete information being provided by the pension saver requesting the transfer. Although a very low proportion of reported transfers were completed with a red or amber flag present, it must be noted that the proportional breakdown on an aggregate level isn't representative of what every provider or administrator is experiencing (DWP, 2023).

Other data sources reveal the extent to which people sought help, capturing scams that would have taken place at various points in the past. Following a media campaign, 3,145

[8] The four numbers are illustrative examples: (1) a successfully committed pension scam that consisted of the withdrawal and reinvestment of funds (i.e. not covered by the amber/ red flag system); (2) A successfully committed pension scam that consisted of a pension transfer. It *should* have been captured by the amber/ red flags system, but wasn't. It is reported in a later year to one of the reporting lines; (3) A successfully committed pension scam that consisted of a pension transfer. It was flagged as amber, but went ahead. It was also captured in the Financial Lives survey, as it was reported here by the pension saver affected; (4) an attempted, but ultimately unsuccessful scam that would have consisted of a pension transfer. It was reported in the Financial Lives survey.

people daily sought help from the ScamSmart website (FCA, 2018c). Online searches for support after losing money to pension and investment scams have seen a significant increase. During the 2022 period just 253 crime reports were made to Action Fraud, the UK's national centre for reporting fraud and cybercrime (TPR, 2021). From Oct 2021 to Sept 2022, there was a 133% rise in Google searches for 'Can someone steal your pension', a 50% increase for 'Investment scam', and a 33% increase for 'state pension scam' (Donelly, 2022). However, only 40% of callers to MaPS helplines who discover they have lost their savings actually take any action (MaPS, 2021).

Finally, relying on self-reports in surveys, the FCA's Financial Lives data suggests that 9.3 million UK adults experienced one or more unsolicited approaches about pensions or investments between March 2019 and February 2020 - these could, but do not necessarily have to, be scams (FCA, 2021a). 1.9 million lost money to fraud (not just related to pensions) over the same period of time.

Other countries use approaches similar to those used in the UK to estimate the scale of pension scams and fraud in general, relying on surveys, reports to fraud helplines, and data collected by anti-fraud centres. They face similar challenges when estimating the scale of pension scams, or fraud more generally.[9]

[9] Survey evidence conducted by Ipsos (2020) for the European Commission across 30 countries found that 56% of people have been exposed to at least one scam in the last two years, with experience varying substantially across EU Member States. In Canada and the US, reports to anti-fraud centres indicate high losses due to fraud, with the Canadian Anti-Fraud Centre estimating that only 5-10% of instances of fraud are reported (CAFC, 2021). In Australia, the Australian Competition and Consumer Commission estimated one-third of those losing money did not make a report (ACCC, 2022).

3.2 How do scams impact those affected?

"They're like grey people [...] when they're speaking to us, you can picture them with all the blood drained out of their face because they're clutching at straws, that maybe we can give them some help which probably doesn't exist. For us it's quite depressing. For them it must be absolutely unacceptable. For example, your wife's left you; your kids won't talk to you; you're living in a hostel or something like that. It is devastating. Scams are absolutely devastating in their worst extreme" - Pension professional

Impact on finances

Pension scams predominantly target individuals that have already accumulated a sizable pension pot, during a time in their lives when their sources of income become more limited and they have fewer opportunities for financial recovery. They can steal decades of savings. The average financial loss for an individual reporting pension fraud to the police in 2018 was £82,000 (FCA, 2019a). For context, the Office of National Statistics (ONS) estimated people yet to retire aged 55 years to State Pension age had median pension wealth of £37,600 (April 2018 to March 2020) (ONS, 2022b). The FCA, as part of their ScamSmart campaign, estimated it may take 22 years for a saver to accumulate a pension pot of the size of the average loss (FCA, 2019b). Some lose even more, with some reported losses exceeding £1 million.

"[The memory of the scam] just keeps coming back, and it doesn't feel like it will ever go away, because when I get to 55 I'll get that reminder oh, well, I'll be able to release some of my pension and that, but it's actually gone. And then [when] I get [to] 65 it's gonna come back again because I'm not gonna have the money there." - Person affected by a scam

In addition, those affected by pension liberation fraud face harsh tax penalties from HMRC - of 55% of the sums withdrawn, along with other fees, regardless of the circumstances of the offence (FCA, 2017b). Typically these individuals will have already paid fees of 20% to 30% of their pension fund to the scammer for making the bogus arrangements (FCA, 2019b).

"I'm 57 this year, my wife is 60 this year. So she's retiring full time. I've had to go back [to work] because the pension pot sort of wasn't exactly what it was supposed to be at this point in time" - Person affected by a scam

The individuals who were affected by scams that we interviewed expressed concern about their future and ability to survive due to the impact on their finances. They were mindful of their advancing age, of limited time to rebuild their pension savings, and of fewer income sources. As a result, some had to work longer hours or extend their working years beyond their planned retirement age. One interviewee shared that they would have to sell their home to secure capital for their retirement.(Pension Saver interviews, 2023).

"But then, this property [their home] is all I have. We'll have to sell it, we have to downsize to get some more money - Person affected by a scam

Even when people did get their money back, they may have a reduced pension income because of a loss of investment growth while it was sitting outside their pension scheme (Pension Saver interviews, 2023).

"I've got my money back, or what I started with but I've lost 6, 7 years of investment, … I'm never going to get it back, you know it's never going to be what it could have been" - Person affected by a scam

Impact on confidence

Falling for a scam can have a profound negative impact on a person's confidence in their financial decision making, which is crucial in retirement planning (Parker et al., 2012; Anderson, Baker and Robinson, 2017). Those affected by fraud often experience a substantial loss of trust in financial institutions (e.g., Giannetti & Wang, 2016; Gurun et al., 2018) and other business practices (Button, Lewis and Tapley, 2009). They may adopt avoidance strategies to prevent being exploited again by limiting participation in financial activities (Shapiro, 1990). They are less willing to take financial risks, moving their savings from investments in the stock market (e.g. Malmendier and Nagel, 2011; Andersen, Hanspal and Nielsen, 2019) to low-yield cash deposits (Gurun, Stoffman and Yonker, 2018), which further hinders their ability to rebuild their savings (Brenner et al., 2020). Similarly, our interviews with those affected by scams found evidence of both an unwillingness to take up financial advice, potentially leading them more vulnerable in the future, and an unwillingness to save into another pension (Pension Saver interviews, 2023).

"[My advice is] don't trust financial advisors because that's where I went wrong. I trusted them because I thought that's what he was paid to do. Don't put your trust in any of it" - Person affected by a scam

"[Starting a new pension] is at the bottom of my list of things to do. [because of his experience and worry of being scam again]" - Person affected by a scam

The impact on confidence is exacerbated by the fact that people often believe that they are invulnerable to financial harm and that the world is intelligible (Perloff, 1983; Janoff-Bulman, 1985). They may take for granted that their pension is secure or guaranteed by the government. When a person loses money because of a scam, this traumatic experience can greatly challenge this perception of invincibility (Perloff, 1983; Spalek, 1999), undermining their sense of financial security. It can also lead to disillusionment with life (Maguire and Bennett, 1982) and feelings of distrust (Katz and Mazur, 1979).

Impact on well-being

"I was diagnosed with depression. It was very severe, acute depression. I was referred to talking services. I was put on medication. I was suffering from anxiety, not being able to sleep. [I had] panic attacks" - Person affected by a scam

Scams and fraud can cause significant harm to an individual's well-being, both physically and mentally. Research indicates that the individual's cognitive functioning and ability to make financial decisions are negatively impacted following the discovery of fraud or financial exploitation, whereas retrospective record review found few significant differences in physical health and cognitive functioning between those affected and those not affected prior to the occurrence of the fraud (DeLiema, 2018).

Cross et al. (2016) interviewed 80 individuals affected by an online fraud; they reported suffering sleeplessness, nausea and weight loss. Ganzini et al. (1990) interviewed 77 individuals who had lost money as a consequence of a financial scheme fraud; they reported suffering heart palpitations (18%), headaches (18%), stomach pain (14%), a sensation of a lump in the throat (11%), and chest pain (10%).

Those affected often experience a range of emotional and psychological responses, including anger and anxiety about money (Spalek, 1999; Button, Lewis and Tapley, 2014). Shame, embarrassment, loneliness, and depression are also common responses, and some individuals report feeling suicidal or even attempt suicide. Evidence suggests that, like survivors of sexual or violent crimes, those affected by fraud tend to blame themselves (Levi and Pithouse, 1992; Titus and Gover, 2001) feeling that others would consider them stupid for being deceived. People affected by scams and pension professionals that we interviewed made similar observations.

"Oh, yes, it's huge because from their point of view, that overwhelming feeling that they've been completely stupid, that doesn't go away, no matter what happens" - Pension professional

One interviewee expressed their distress about needing to recall the details of being scammed, when dealing with the investigation process that occurred after they sought help

"You've got all those pieces [of evidence] all over your bed, all over the floor, all over everywhere. I put them [the documents] back in order. They are currently under the desk behind me in a red box. I've hidden [the box] with a blanket because I can't look at it. It makes me physically sick" - Person affected by a scam

Impact on relationships with friends and family

Individuals have reported that the theft of their pension funds had a more devastating impact on their lives compared to any physical violence, burglary, and car theft that they had suffered. Pension professionals (2023) that we interviewed made similar observations. The devastating impact is unsurprising, considering the large financial value of the pension funds and the extended period of time during which the individuals have to endure the effects of the theft (Spalek, 1999). Those affected often try to keep the financial loss a secret from family members, resulting in increased stress and distrust when the truth is eventually revealed (Button, Lewis and Tapley, 2009). Fraud incidents can strain relationships with friends and family, leading to family breakdowns in over 17% of cases. Relationships are most likely to deteriorate when family members attempt to prevent repeat cases (9.1%) (Button, Lewis and Tapley, 2014). Older individuals may experience distress at the loss of their children's inheritance (Deevy, Lucich and Beals, 2012), or feel shame and fear about exposing their vulnerabilities to family members (Segal, Doron and Mor, 2021).

3.3 What are the wider impacts?

Pension scams have profound impacts on the wider economy and society. They can therefore be characterised as inferring negative externalities on the wider economic system and fabric of the UK.

Impact on the economy

Pension scams can undermine people's trust in saving for their future and in the financial system as a whole (Spalek, 1999). Peoples' financial well-being and an economy's vulnerability to poverty and growth prospects are strongly related (Sacks, Stevenson and Wolfers, 2012; Griggs *et al.*, 2013). Fraud can harm a country's international and economic reputation, and widespread fraud can negatively affect assessments of a country's safety for conducting international trade and business. This is especially relevant to the UK where maintaining the integrity and reputation of the UK's financial services sector is of vital economic importance (Wood *et al.*, 2021).

Impact on society

The involvement of organised crime groups in pension scams (particularly those involving investment fraud) has been uncovered, which provides challenges to law enforcement. Such scams often involve multiple layers of deception to convince pension companies, industry regulators, and pension savers. This includes imitating legitimate business strategies and product marketing tactics, acquiring authorised status from regulators, and recruiting legitimate professionals to participate in the unlawful schemes. A case study by Skidmore for the Police Foundation described the identification by fraud investigators of a 'loose cartel of enablers and businesses across the UK with an organised crime group at its centre, with links to other crimes such as serious violence and money laundering as well as numerous fraudulent pension companies.' (2020, p.4).

Impact on public services

Scams put additional strain on public services that are responsible for safeguarding individuals from financial abuse by shifting the cost of care onto the public balance sheet. The Care Act 2014 recognises the harm that financial abuse can cause to an adult's health and well-being and imposes a duty of protection on local authorities. People who have been exploited by scams are more likely to need to go into care homes, but the fall in their income and wealth can make it difficult for them to contribute to the costs of their health and social care. This further increases the financial burden on society for providing future care. People with dementia are particularly vulnerable to financial abuse and scams, putting additional pressure on community and residential dementia care services (NCPQSW, 2018b).

Impact on younger generations

While many retirees currently enjoy the benefits of a final salary pension, which guarantees a steady income throughout their retirement, most modern workers contribute to defined contribution pensions, which are generally less generous. These pensions involve a fund of money that is contributed to by both the employee and employer. Unfortunately, almost 90% of middle-earning private sector employees are not saving the amount recommended by the Government's Pensions Commission. The Institute for Fiscal Studies has suggested that this

will result in a less comfortable retirement for future generations than for current retirees (IFS, 2023). Any rise in pension scams in the short term would require younger generations to forgo even more of the current income to support older generations and in the longer term further increase the proportion of people (i.e. the current young) who will face financial difficulties in their retirement years.

4. Types and tactics

4.1 Types of pension scams *There are a variety of pension scams. They depend on the type of pension plan a saver has, their ability to access the underlying assets, and their desire to release funds or invest for higher returns. Once scammed, individuals are often targeted with a secondary scam that pretends to offer solutions to mitigate the effects of the previous scam.*

4.2 Recent trends in pension scams *Scammers evolve their tactics to adapt to changes in legislation and context. Reports of fraudulent activities and computer misuse[10] crimes have increased by 25% since 2020. Future trends predicted by interviewees working in the sector include a surge in pension liberation scams when the minimum age to access pensions increases from 55 to 57 in 2028 and the exploitation of the new pension dashboard as pension savers become aware of their smaller pots and might share this information with scammers.*

4.3 Scammer disposition *Successful scammers often utilise the techniques of legitimate entrepreneurs - such as aggressive sales techniques. Moreover, experts have compared scammers' methods to those employed by individuals engaging in coercive control grooming.*

4.4 Tactics used by scammers *Pension scams involve three stages*

Targeting *Scammers adapt their style and content to make them appeal to the demographics they are targeting. Scammers can obtain contact details from both legitimate (open-access directories; asking targets to recommend them to their social network) and illicit sources (e.g. bulk purchase of profiles from the dark web). Scammers are increasingly making contact remotely via search engines, investment comparison websites, or social media platforms - enabling them to target more people at very low costs and without the risk of being detected easily.*

Executing *Scammers use various tactics, often implicitly informed by behavioural science. They can exploit emotional decision-making, creating false urgency by claiming limited or exclusive opportunities, or preying on people's desire for prosperity or financial security. They establish trust by using overt markers of authority (e.g. company logos); by building personal relationships with the pension saver through flattery; by establishing a rapport; or by invoking reciprocity (e.g. offering a free pension review).*

Avoiding detection *Scammers anticipate that individuals' affected by scams may feel too embarrassed to reach out to authorities.They may specifically target people who are less likely to report, such as older people, or discourage the discussion of finances with friends or family. They may exploit remote operations to avoid face-to-face contact, and can operate in legal grey areas where it is hard to identify a scam as breaking the law or the legal jurisdiction under which it falls.*

[10] Computer misuse crimes in the UK involve illegal activities such as unauthorised access to computer systems, theft or destruction of data, and the creation or distribution of malware.

4.1 Types of pension scam

"[I had a pension scam case of a man that] was convinced that he had 1 million pounds plus in cryptocurrency" - Investigative journalist

Pension scams range from unethical practices, to the breaching of financial regulations, to criminal fraud. This section provides an overview (ASIC, 2002b; Graham, 2014; NCPQSW, 2018a; Wilkinson, 2020; TPR, 2021; Volant, 2022; TPR, n.d.). Note that, often, several of these types will be combined. For example, a pension liberation scam might also be a fake investment scam.

Proposed use of pension

To convince pension savers to make a withdrawal or transfer to their pension, scammers offer a range of different 'products' in order to gain access to some or all of the pension pot. The nature of scams can vary based on several factors, such as the kind of pension scheme[11] an individual has, their access to the underlying assets, and their inclination to unlock funds or seek higher returns through investment. Scammers may employ tactics such as outright stealing of assets or imposing excessive fees to obtain money.

Pension liberation scams: Scammers mislead pension savers under the age of 55 to access their pension pots.[12] The individuals are unaware that they will incur a tax charge and potentially fines for engaging in tax evasion. Typically, the scammers deliver a large portion of the released funds to the pension saver in the form of a lump sum, in exchange for a fee of 20-30% of the fund's value. This fee reinforces the individual's trust, because their adviser seems to be putting in effort and is therefore entitled to compensation, which decreases the risk of detection in the short term.

In one high-profile pension liberation scam, more than 100 UK investors were sold seedlings inoculated with truffle spores which turned out not to exist. As well as losing their money, pension savers were pursued by the tax authorities for withdrawing their pension money too early (The Insolvency Service, 2018)

[11] Defined benefit pension schemes are retirement plans where an employee is promised a specific amount of income during retirement, usually based on their salary and length of service. The employer is responsible for managing the investments and assumes the investment risk to ensure that the promised benefit is paid out. Defined contribution pension schemes are retirement plans where an employee and/ or employer regularly make contributions to an investment account, which is managed by a pension provider. The final pension benefit is determined by the performance of the investment account and the accumulated contributions. The individual assumes the investment risk.
[12] Under the Pension Freedoms Act, from the age of 55, pension savers with defined contribution pension pots can access their pension without extra tax penalties.

Investment scams: Scammers promise pension savers an attractive investment opportunity. There are two types:

- Fake: the scammers take the pension saver's money, although the investment opportunity may actually exist.
- Real: the risks and rewards of the investment opportunity are misrepresented so that the savers take on a far higher level of risk than is appropriate for their financial circumstances. Examples of such unusual, high-risk investments include cryptocurrency, overseas property and hotels, renewable energy bonds, forestry, parking, storage units, care homes and biofuels.

The Dolphin's Trust offered individuals the opportunity to invest their pension savings in a scheme to redevelop German listed buildings into luxury apartments. Properties were left derelict and the firm filed for bankruptcy, owing an estimated £378 million to UK investors (BBC, 2020)

Terms-of-Service scams: Scammers offer an investment opportunity, but impose excessive charges by creating convoluted or multi-tiered business structures, through which the pension saver's funds are routed. For example, an advisor might sell the product to the pension saver. Multiple intermediaries then each skim off high charges, a practice known as fractional scamming. While this may not be illegal, it is a deceptive business tactic, where the terms of the contract are either concealed in the fine print or agreed to by unsuspecting or desperate clients

Pension mis-selling: Scammers persuade the pension saver to swap their defined benefit pension, which pays a secure retirement income with inflation protection, for either a pension with lesser benefits or a cash lump sum.

In a 2017 scandal, almost 8,000 British Steel pension scheme members were persuaded to transfer their pensions by advisers who then pocketed huge fees. The average loss was £80,000 with some losing up to £489,000 (Jones, 2022)

Annuity mis-selling: Scammers sell overpriced or inappropriate products to people considering purchasing an annuity.

Claims management scams: Scammers claim savers have been mis-sold a pension and then ask for an advance fee (see Advance fee fraud below) to begin a claims process.

Employer-related investment scams: Employers neglect their responsibility to manage the employee pension scheme in the best interests of the employees. Instead, they redirect the

employees' pension contributions to make inappropriate investments in their own business, resulting in financial losses for the savers.

Approximately £500 million was embezzled from the pension funds of Mirror Group Newspapers and other companies by their owner, Robert Maxwell, in the 1980s. He used the funds to cover up his failing businesses and personal finances, leaving thousands of employees without their expected pensions. (Spalek, 1999)

Imitation

Scammers may impersonate different types of legitimate institutions or individuals to gain the trust of the pension saver:

Advice/ review scam: Scammers present as financial advisors. Pension savers are unexpectedly enticed with 'free' pensions advice and a review of their savings and investment returns with the objective of gathering information or authority to transfer a pension, or acting as a lead for other scams, particularly investment scams.

Scam pension schemes and providers: The scammer sets up a pension company to deceive both pension savers and their existing pension provider who is required to transfer their savings. To facilitate this, these scam schemes gain authorisation from the regulators and tax authorities. Such schemes range from organisations having both illegitimate and legitimate arms, employing staff unaware that they are executing a scam, to short-lived organisations whose only purpose is to execute scams, to ‘clone’ firms (see below).

Clone Firms: These are fraudulent pension schemes and providers that mimic legitimate entities. The scammers use the name and registration number of firms authorised by the FCA, but provide their own contact information, sometimes claiming that the registered information is outdated. They may also pose as an overseas firm without full contact or website information registered. The scammers may duplicate the website of an authorised firm but make slight changes, such as the phone number. For example, in a well-known case, a clone imitated the insurance company and pension provider Aviva in 2020 (FCA, 2020). Peter Hazlewood, their Group Financial Crime Director said at the time 'we’re working round the clock with the authorities to have these types of websites taken down. Unfortunately, as soon as one is taken down, a new one inevitably pops up' (Silvani, 2021).

Impersonation of trusted organisations: The scammer pretends to be from a trusted organisation such as a pension provider, a government department like the DWP or HMRC, or a guidance provider like MaPS. This is done either with the goal of obtaining personal details such as passwords to allow the scammer to access someone’s pension directly or to trick the pension saver into authorising the transfer of money into an account controlled by the scammer (so called **authorised push payment, or APP, scams**). Techniques include:

- Phishing: The sending of emails or other messages purporting to be a reputable organisation.

- Number spoofing: The scammer can impersonate another person's or company's telephone number.
- Smishing: A technique where scammers tap into an existing text message chain to make it appear that their own message is from a genuine source.

"I spoke to somebody recently and he said, 'No, it was all genuine. It was through Nasdaq,' and I said, 'Oh, give me the website,' and he gave me the website, and it did have Nasdaq in the website name, but when you actually followed the link, it had a blurred-out image of Nasdaq" - Pension professional

Repeat scams

Individuals may be scammed again in a secondary scam. Pension professionals (2023) that we interviewed explained that the new scammer will often reassure the individual that they understand the problem and pretend to offer solutions to mitigate the effects of the previous scam. Such secondary scams often involve **advance fee fraud**, which involves the pension saver being asked to pay a fee in advance of the scammer 'helping' them, for example:

- **Recovery fraud:** Scammers contact someone who has previously been affected by a fake investment scam, offering to recover their lost investment in exchange for an advance fee.
- **Advance fee securities scam:** A pension saver is told that a person is interested in buying their investment at a premium to the current market price, but that they must pay a fee first.

A pension saver we interviewed shared their experience of losing money by investing in airport parking spaces. Later, another organisation approached them with an offer to purchase these parking spaces for an inflated amount, but they required the interviewee to pay a £7,000 licence fee beforehand. The interviewee realised that this was a scam because the offer seemed too good to be true (Pension savers interviews, 2023).

4.2 Recent trends in types of pension scams

"Scammers spot trends. They spot whatever is the trend at the moment, that's what they'll go for" - Pension professional

Over the past two years, there has been a significant rise in fraudulent activities and computer misuse crimes. Since March 2020, reports of fraud offences have increased by 25% with 4.5 million incidents reported. The increase was mainly attributed to a considerable rise in advance fee fraud and consumer and retail fraud (when a person suffers from a financial loss involving the use of deceptive, unfair, or false business practices, Fontinelle, 2022). Furthermore, the percentage of fraud incidents that were cyber-related increased from 53% to 61% during the same period (ONS, 2022a).

Even where the tactics used by scammers to deceive their targets remain largely the same (see below), the *type* of scams are constantly evolving to adapt to changes in the external context. Changes in legislation are a major driver of their evolution. For example, the Pension Schemes Act 2015, which introduced pension freedoms, has resulted in a decrease in pension liberation scams. However, scammers have now shifted their focus to investment scams and terms of service scams. The high fees charged to those affected by scam pension transfers are of particular concern among some industry participants. Conversely, advice provided by intermediaries on the suitability of transfers from defined benefit to defined contribution schemes has improved (TPR, 2022).

Two years later, the Finance Act 2017 introduced tax changes that have reduced the appeal of international transfers to Qualifying Recognised Overseas Pension Schemes (QROPS). QROPS are outside of UK jurisdiction and therefore easier for scammers to raid (Jakubowski, 2020). However there are now more transfer requests to international self-invested personal pensions (SIPPs). They are often marketed by foreign intermediaries to scheme members living abroad as UK-registered pension schemes which facilitate overseas investments (TPR, 2022).

In 2018, the Privacy and Electronic Communication Regulations implemented a ban on cold-calling within the UK for the sale of pension schemes. However, scammers have found ways to circumvent the rules by initiating their initial calls from outside the UK and then passing on referrals to representatives based in the UK. Moreover, there has been a rise in scammers generating leads through the use of the internet and social media. This includes ads presenting opportunities on social media platforms. To combat this, the Online Safety bill intends to impose a duty of care on platforms to protect users from fraudulent advertisements (TPR, 2022; Pension professionals interviews, 2023).

"I think people are contacted more via social media - Facebook, LinkedIn. [...] if you just click a link, advisors can reach out and make contact, just from you having a look at the page. I think that's, now, a major difference from previously" - Pension professional

The Pension Schemes Act 2021 limits people's statutory right to transfer their pension when there are signs of a scam through the amber/ red flag system (see Section 3.1). However, MaPS has observed through its scams and fraud support services that scammers are bypassing these restrictions by encouraging savers to withdraw cash from their schemes instead of transferring the entire amount (MaPS, 2023).

In addition to changes in legislation, scammers stay up-to-date with the latest news and take advantage of changing situations. For example, the COVID-19 pandemic offered them new opportunities (TPR, 2022) by increasing people's fears of economic insecurity, concerns about health, and social isolation (Which?, 2022). Similarly, the cost of living crisis has led savers to believe that their pension pots need protecting, which may result in unwise decisions about their finances, such as investing in cryptocurrency (MaPS, 2023) and one-quarter of consumers served by the FCA (2022) would withdraw savings earlier than planned to cover their additional costs. Even the climate emergency has been exploited by scammers as a way to promote investment opportunities, such as fraudulent 'forestry for the purpose of carbon capture' schemes (Pension professionals interviews, 2023).

The professionals we interviewed raised several concerns regarding future trends in pension scams (Pension professionals interviews, 2023). Firstly, beginning in 2028, the minimum age to access pensions will increase from 55 to 57. This change may lead to a surge in pension liberation scams, as individuals who had planned to access their savings at age 55 may still seek to do so, potentially putting them at risk of fraudulent schemes. This phenomenon has already occurred when the minimum age increased from 50 to 55. Secondly, scammers may try to circumvent the regulations set by the Pension Schemes Act 2021 (including the amber/ red flag system) by subjecting pension savers to a two-part scam. In the first part, pension savers are convinced to transfer their pension to a scheme that has more flexible rules over the type of assets that can be invested in. Initially the scammer recommends the saver to keep their savings invested in regulated investments. This avoids raising any suspicions about the transfer. Once the transfer is complete, in part two of the scam, the scammer persuades the saver to invest in high-risk, unregulated investments. Thirdly, one interviewee expressed concerns that the new pension dashboard may facilitate scams as pension savers become aware of smaller pots and might share this information with the scammers or scammers persuade savers to take a gamble. For instance, scammers may convince pension savers to invest *any discrete small pension pots in high-risk investments*. While smaller pension pots have so far not been the main target of scams, this may be subject to change. Auto-enrolment and changing job patterns has led to an increase in the number of small pension pots; research by Aegon (2021) shows over a quarter of adults have at least one pension pot of less than £5,000, with 15% saying they did not know whether they had one. Finally, one of the pension professionals interviewed raised that there

has been a recent increase in *phishing attempts*, where scammers obtain pension savers' log-in details to their pension platform. One warning signal is when both the phone number and address are changed in rapid succession (Pension professionals interviews, 2023).

4.3 Scammer disposition

Combating scams requires an understanding of scammers' motivations, how they operate and the techniques used to separate individuals from their money. Despite its significant impact, there is a lack of academic research into the threat posed by economic crime. While research has been conducted into offender motivations, there are gaps in the evidence about how individuals become involved in economic crime and their connections to serious and organised crime (Home Office, 2021).

Personality traits of scammers

Sandhu (2020) lists a large number of sometimes contradictory features that increase the likelihood of someone committing fraud, including: ego (Sutherland, 1983); financial shortfalls and personal problems (Cressey, 1953); sudden lifestyle changes (Kaplan and Reckers, 1995); extraordinary intelligence, ability to lie with conviction and to handle acute stress (Wolfe and Hermanson, 2004); ignorance, determination and overconfidence (Mohamed, Khair and Jon, 2015); reputational anxiety and obsession to outperform others (Murphy and Free, 2016) and a tendency to rationalise unethical behaviour (Farber, 2005).

The scammer as an entrepreneur

Button and colleagues coined the term 'scampreneur' (2009, p.5) to describe scammers, as to be successful they require entrepreneurial traits such as over-optimism, risk-taking, the need for achievement, autonomy, and the desire to have control over their own actions. Scamming represents a low risk, high reward business for the malefactor as pension savings constitute most people's largest financial asset and so are significant wins for the scammer (Wilkinson, 2020). Furthermore, the risks of prosecution are low, as evidenced by the fact that there were only 25 convictions involving 'scams and unauthorised business' in the UK between 2012 and 2020 (HoC Work and Pensions Committee, 2021).

"[In my job we] tap into call centres that we know are running criminal scams. You're talking about a multitude of extremely large businesses [that scam people]. I'd estimate easily in the hundreds outside of the UK. And mainly in South Asia, whose sole reason for existence is to defraud people"[13] - Investigative journalist

The scammer as unethical, but not criminal

The risk of prosecution for scammers is further reduced when their scams, rather than illegal, are unethical, such as charging exorbitant fees, misrepresenting investment opportunities, or engaging in aggressive sales tactics that mislead or pressure individuals into making poor

[13] A case study describing scamming on an industrial scale by a boiler room operation is provided in Appendix 2

financial decisions. In many cases it can be difficult to prove criminal intent or wrongdoing. Intermediaries may be unconsciously acting unethically since aspects of the legitimate market have prized profits over integrity e.g. the use of pushy lead generators offering free pensions review and then passing clients onto a financial adviser has been a tactic used by lawful intermediaries. Large commission fees may be paid to incentivise intermediaries to promote high-risk schemes to naive investors, and the, often overseas, companies that receive the investment funds are either unaware or unconcerned about their source (Skidmore, 2020).

The scammer as a groomer

Scammers often employ psychological grooming techniques similar to those used in domestic violence and coercive control, which can make it difficult for individuals to recognise they are being scammed and seek help or break away. Scammers may establish a rapport with their targets, using charm and persuasion to gain their trust, before manipulating them into repeatedly making unwise financial decisions. Individuals affected may feel protective towards the scammer and are groomed to cooperate (NCPQSW, 2020 and below), further lowering the rates of reporting.

"... one woman I can think of lost about half a million quid to an investment scam. Those scams take place over months, and are very much more slow and considered, and all about crafting a kind of fairy tale and beautiful reality for the person that you're talking to" - Pension professional

4.4 Tactics used by scammers

Scammers employ different tactics for the different stages of the scam. Button et al (2009) describe three different stages: firstly, targeting the pension saver; secondly, executing the scam; and finally, avoiding detection. We discuss the tactics for each stage below.

Tactics used to target individuals

Tailoring the type of scam

"The first thing they've got to do is get your attention… they'll say, 'We can help you make lots of money out of your predilection for [collecting] stamps" - Pension professional

Scammers often tailor their schemes to target specific groups, adapting the style and content of their approach to appeal to the demographics most likely to fall for their tricks. For instance, individuals between the ages of 45-54, who can transfer their pension scheme but

not yet access their savings, may be targeted with a pension review scam. Meanwhile, those aged 55-64, who can also access their savings, may be targeted with a pension advice scam (Citizens Advice, 2016). We discuss risk factors that make an individual more likely to be successfully exploited by a scam in Section 5.

Obtaining potential targets' contact details

Scammers use various methods to acquire lists of potential targets. Legitimate sources include open access directories or databases such as phone directories, registers of directors or shareholders. Alternatively, they may purchase private commercial telemarketing lists. In addition, scammers may place small ads in reputable publications or online to elicit responses from interested individuals from which they can build a contact list.

They may ask those contacted to recommend friends or colleagues who then inadvertently recruit more targets, leading to a 'snowball' effect. Affinity groups such as faith groups or club members are also targeted. (ASIC, 2002b; Shover, Coffey and Hobbs, 2003; Button, Lewis and Tapley, 2009; Skidmore, 2020). A pension professional interviewee described how when people need money they may take the honesty of those making recommendations for granted.

Illicit sources of targeted lists include those generated through phishing (Skidmore, 2020) or purchased on the dark web. The cost of purchasing such lists has decreased significantly from around £2 per profile in 2007 to less than 50p in 2021, with scammers usually bulk-buying them (Harding and Sales, 2022). Once an individual has been successfully exploited by a scam, they are likely to be re-targeted or subject to additional scams due to their inclusion on 'suckers lists' (Button, Lewis and Tapley, 2009). These lists of 'easy touches' are circulated among scammers, either for free, or more likely for a fee, to earn the scammers more income (Levi, 1988).

Contacting targets

Scammers use a range of methods to reach their targets, including unsolicited emails, text messages, and phone calls (FCA, 2018b). While it is now illegal to make cold calls to sell pensions in the UK, individuals may inadvertently give permission for their details to be added to marketing lists by ticking a box (or failing to untick one) indicating that they wish to be contacted (Smart Pension, 2021). Scammers may also create fake websites that appear to be official, in order to trick targets into providing their contact information and consenting to being contacted (MoneyHelper, n.d.). Furthermore, overseas cold calling does not fall under the jurisdiction of the UK legislation (TPR, 2022). The investigative journalist that we interviewed described how scammers will pay an overseas call-centre to make the first contact with targets, and by using number-spoofing techniques the calls can appear to be made from within the UK.

Scammers are increasingly targeting individuals who search for investment opportunities online, often through search engines like Google and Bing, investment comparison websites, and pension review websites. Posting scams on social media platforms such as Facebook and LinkedIn is also becoming more and more common. (FCA, 2017b; TPR, 2022). From our interviews, pension professionals agreed that initial contact was increasingly being made via

social media and some affected by scams confirmed that this was how they had been contacted.

Remote communication is typically an integral part of scammers' modus operandi (TPR, 2022), partly as it reduces their chance of being caught (discussed below). Additionally, the use of information and communications technology allows scammers to target a larger number of individuals. While in-person scams, where a smartly dressed scammer carrying convincing identification presents authentic-looking documentation on the doorstep (Smart Pension, 2021) or at the factory gate (cifas, 2020) still occur, cyber-enabled fraud allows scammers to target more individuals and increases the number of potential targets (NCPQSW, 2018a).

Tactics used to execute the scam

"[The scammers] have very highly crafted scripts, which they've been taking years to refine and they will tweak to reflect, for example, the current geopolitical situation, in the world, whatever the news is that week. The scripts are designed to make people panic, to make people feel fear. [They're saying] you absolutely have to do this now, and the reason you have to do it now is because if you don't [...] you're gonna lose your money" - Investigative journalist.

When individuals make changes to their pension, such as revising investments or switching advisers, they are making complex and risky decisions that involve choosing between various alternatives with different potential outcomes and chances of success.

Scammers do not just use one technique to execute their scam but, depending on its type, employ a variety of often (implicitly), behaviourally informed tactics. To sell what they are offering, scammers may arouse an individual's emotions so that they do not think clearly; use persuasive tricks to build a relationship with their target; and exploit individuals' innate behavioural biases - the mental short-cuts we all use to navigate the world around us.

Manipulating emotions

Exploiting emotional decision-making in a 'hot' state. 'Hot' states are those in which people's decision-making is influenced by emotions - they can be brought about by feelings such as hunger and pain, but also by evoking strong emotions. Scammers take advantage of this by using social influencing tactics, such as visceral cues (discussed below), to alter individuals' emotional states. By moving them from a 'cold' state, where they think calmly, to a 'hot' state of e.g. fear or greed, individuals are more likely to take risks, less likely to notice the clues that a communication is a scam and more likely to make unwise financial decisions (Langenderfer and Shimp, 2001; Loewenstein, 2005; Kieffer and Mottola, 2017).

Presenting an opportunity as scarce. Our interviewees described scammers using the

tactic of scarcity to create a false sense of urgency, either by claiming that the opportunity is scarce, such as an 'exclusive opportunity' or 'one-off investment,' or that time is limited to get the best deal or to avoid potential losses as 'the market's about to crash'. This tactic is promising for a number of reasons: Firstly, scarcity results in the individual perceiving the opportunity as more valuable (Worchel, Lee and Adewole, 1975). Langenderfer and Shimp (2001) noted that tactics which highlight the immediacy or exclusivity of the opportunity being presented are also commonly employed in legitimate marketing practices. Secondly, loss aversion - the tendency to experience losses more severely than equivalent gains (Kahneman and Tversky, 1979) - may motivate the pension saver to proceed with the investment for fear of missing out, despite any reservations. Finally, scammers might present an offer as time-limited. They may even encourage pension savers to transfer their pensions quickly by sending couriers or personal representatives who wait until the pension saver signs the documents (ASIC, 2002b; TPR, 2022; Which?, 2022). This decreases pension savers' ability to process information objectively and thoroughly (Petty *et al.*, 1986). As a result, they may not check the information that scammers provide.

Exploiting people's desire for prosperity. Conversely, another visceral urge that scammers prey on is desire for material wealth. They dangle the prospect of wealth using phrases like ' guaranteed return', 'loophole', 'cashback', 'savings advance' and 'upfront cash' (Age UK, 2022; TPR, 2022). Pratkanis and Farquar (1992) describe this promise of unrealistic or unattainable wealth as planting the seed of 'phantom riches', which can lead to irrational judgements (Ariely et al., 2009). The closer the reward, the stronger the visceral reaction (Langenderfer and Shimp, 2001).

People tend to systematically overweigh the value of a long shot at a large prize, which could explain why they fall for the chance of a large investment gain (Kahneman and Tversky, 1979). Moreover, people tend to judge situations as more likely when they are easily recalled, which is known as the availability heuristic (Tversky and Kahneman, 1973). Thus, if people have seen significant increases in the value of a certain market, such as cryptocurrency, they may overestimate its value as an investable asset. Scammers can exploit this by citing relevant news.

Creating trust

Building credibility.

"I've got this glossy magazine ….: Thank you for taking part in investing in Harbour Pensions" - Person affected by a scam

'Source credibility' is a tactic used by scammers to take advantage of the fact that people are more likely to believe, trust and obey individuals in positions of authority or organisations that

appear to be legitimate.[14] Scammers often impersonate trusted organisations by adopting their overt markers of authority (see Section 4.1), including visual cues like company logos, impressive brochures, and prestigious offices (Rusch, 2008). They may also use authoritative language that closely mimics the words and terminology used in the financial services industry, or make direct appeals by offering the pension saver to speak to their 'line manager'. Alternatively they can impersonate a reputable organisation using the tactics described above (Skidmore, 2020). Interviewees that had been affected by scams (2023) described receiving glossy brochures or visiting impressive websites. However, some pension professionals pointed out that although some scammers' materials are professionally designed, other material is very low quality but still manages to convince.

"For example, with the stocks and shares…I could just copy and paste off somewhere and slap them on to a website page. It's meaningless... So that's the difficulty: people don't appreciate that it isn't genuine" - Pension professional

Just as individuals tend to have greater trust in doctors who wear a white coat (Rehman *et al.*, 2005), this same level of trust may also extend to legal professionals, making investment recommendations by solicitors more convincing. According to the Solicitors Regulation Authority (SRA), 'promoters of investment scams often try to legitimise them through the involvement of solicitors and law firms. It lends credibility to what they are doing and provides comfort to investors.' (2016, p. 6).

Building relationships. People tend to act in a manner that boosts their self-image (Dolan et al., 2010). To create a positive feeling in targeted pension savers, scammers often employ flattery, like complimenting investors for their expertise. For individuals who consider themselves financially savvy this confirms their beliefs about themselves. Research by ASIC (2002b) discovered that scammers employ language intended to evoke a feeling of identity and self-respect in their targets. This includes praising investors for their knowledge and portraying their possession of money as a personal ability rather than a simple fact about their finances. This frames the act of investing as carrying meaning about the investors as individuals.

Invoking reciprocity. When people are given something it can trigger an innate tendency to respond by giving something back (Gouldner, 1960). Scammers can leverage this by offering a free pension review - a classic distraction trick (FCA, 2022) which may lead the pension saver to believe that they should accept the advice in return.

Creating likeability. The tendency to favour and trust someone we like is called 'liking bias' (Cialdini, 2007). When a scammer is able to establish a strong rapport with their target, the target is more susceptible to complying with the scammer's requests. For example, Age UK (2018) illustrated a case of an elderly gentleman who experienced substantial financial losses but persisted with investing due to the promoter's 'friendly' demeanour.

[14] The power of source credibility is seen in Milgram's (1963) classic work on obedience, where he argued that authority figures must be perceived as legitimate for people to obey them.

Exploiting other behavioural biases

Social proof. Especially in affinity scams, which are based on people affected by scams recruiting more targets from the same social group, scammers may take advantage of group trust as a highly effective means of bypassing people's doubts, leading to both naive and seemingly knowledgeable individuals falling for scams. The stronger the appearance that everyone else in a group is holding a certain belief, or participating in a certain behaviour ('everybody does it'), the more inclined an individual is to conform and align with said group (Asch, 1956; Comet, 2011; Pratkanis, 2011; Perri and Brody, 2012). One of the pension professionals interviewed (2023) mentioned that people often assume the accuracy of recommendations from their colleagues, friends, or family members, especially when they are in dire need of money.

"So basically a friend of mine from work was getting some financial advice from a guy. And he put me into [contact] with him….[The financial advisor] says 'What we can do is invest - take [your pension] out and invest it and I'll give you a return' " - Person affected by a scam

Consistency. People like to think of themselves as consistent: once they agree to a small request they are more likely to comply with larger and most costly requests. This is known as the 'foot-in-the-door' technique (Freedman and Fraser, 1966). Fraudsters may ask their targets to undertake a small, seemingly harmless action, such as downloading a piece of 'antivirus' software to protect themselves. Having undertaken this first small action, and wishing to stay consistent with their past behaviour, individuals are then more likely to undertake larger actions, such as transferring their bank balance to their new account.

Cognitive dissonance. The pension saver's response to a scam can reflect the ability of scammers to create a situation where doubt is intolerable, a concept known as 'cognitive dissonance' (Festinger, 1957). This occurs when holding two conflicting thoughts causes mental conflict. Research by (Nickerson, 1998) demonstrated that people have a tendency to seek or notice information that confirms existing beliefs (known as confirmation bias). This makes some investors susceptible to fraud, e.g. positive online reviews can be used to reassure individuals, even when they are written by the scammers themselves (FCA, 2018a). Individuals targeted by the scam are not choosing to ignore warning signs, but instead are unable to tolerate conflicting information (Which?, 2022).

Optimism bias. This is a cognitive bias that causes people to overestimate the likelihood of positive outcomes and underestimate the likelihood of negative outcomes (Sharot, 2011). People do not tend to think something bad is going to happen to them, and, in this case, it simply may not occur to them that they are being scammed.

Tactics used to avoid detection

As discussed above, scams are underreported and scammers might exploit or even encourage this further.

Encouraging and exploiting individuals' tendency to underreport

Anticipating individuals' sense of self blame or shame. Those affected by scams may feel too embarrassed to reach out to authorities (ASIC, 2002). They may also suffer from self-blame; according to Mason and Benson (1996), individuals who blame themselves or the perpetrator and themselves are less likely to report the crime. They may also be hesitant to report criminal activity if tax rules were broken, either because they feel complicit in the crime or they are concerned about being pursued by the tax authorities (Skidmore, 2020). People affected by scams may also refuse to accept that they have been scammed and instead believe they have simply made an unsuccessful investment (Button, Lewis and Tapley, 2009) or may feel a sense of protectiveness toward their scammer (NCPQSW, 2020).

"People don't want to admit what happened, which of course, can make it harder for them to get compensation" - Pension professional

Targeting people who are less likely to report. Scams are especially underreported among older people (NCPQSW, 2018b). Age-related decline in cognitive abilities, which may increase susceptibility to scams (see Section 4), can also impact their ability to report the scam and pursue legal action (Segal, Doron and Mor, 2021).

Encouraging individuals not to discuss their finances. Secrecy is crucial to scammers' success, since the involvement of the target's friends or family can hinder the scam's success. Scammers use tactics to foster secrecy from their target without arousing their suspicion. They can exploit the 'legitimate secrecy' arising from the routine/private nature of the activities they persuade the pension saver to carry out. People typically do not discuss details of their personal finances - e.g. one-third of over 55 year olds surveyed by the FCA (2017a) were reluctant to discuss their investment decisions with others. Furthermore, if a scammer can successfully groom a pension saver, they will try to isolate them from opportunities and motivation to seek help, making reporting unlikely (NCPQSW, 2020). Even if a person's social network does become aware of the fraud, if they do not encourage the person to report the crime, the individual is much less likely to do so (Mason and Benson, 1996).

Exploiting the environment

Operating remotely. To reduce suspicion and avoid detection, scammers often operate

remotely and avoid face-to-face contact with the pension saver they target. They may not allow the pension saver to call them back, or have only mobile phone numbers or a PO box address as contact details (MoneyHelper, n.d.). More sophisticated scams may employ various services-for-hire to create an appearance of legitimacy for their organisation, such as companies to process legal documentation and renting prestigious office spaces (Skidmore, 2020). Scammers in boiler rooms frequently relocate to evade law enforcement, a strategy known as 'rip and tear' (Shover, Coffey and Hobbs, 2003). After targeting individual pension savers intensively, they move to a new location before local police can catch up with them, often leaving behind local sales staff who might not even be aware they were involved in a scam (Stevenson, 1998). There is also evidence that the use of remote technology reduces the scammer's empathy for the pension savers targeted and their guilt for betraying them (Duffield and Grabosky, 2001; Grabosky and Duffield, 2001).

"About 2 or 3 years after [making the investment] I didn't see anything, that is, I didn't get any updates, and then I tried to contact them a couple of times about the investment [and got no answer]" - Person affected by a scam

Leveraging legal ambiguity. Many scams operate in a legal grey area, where it is difficult to definitively identify criminal fraud rather than aggressive business practices. For example, the fine print in the contract documentation may accurately describe the situation, even if it contradicts what the pension savers were promised. This ambiguity reduces the likelihood that individuals affected will report the scam, even if they suspect that they have been defrauded. Other individuals may be unsure about which agency to report the offence to, which also reduces reporting. For example, in the UK, pension scams can and should be reported to several different institutions, including the FCA, Financial Services Compensation Scheme (FSCS), the TPO, MaPS and Action Fraud. The correct point of contact may depend on the type of scam. Even when the case is reported, law enforcement agencies may be hesitant to take action, as they may view it as a civil, rather than criminal, matter. In cases where the scam operates across borders, it can be unclear under which country's jurisdiction the scam falls. Additionally, many boiler room scams operate in countries where law enforcement authorities are uninterested in pursuing such crimes, as long as their own citizens are not targeted. Even if scammers are convicted, they may receive light sentences (Shover, Coffey and Hobbs, 2003; Button, Lewis and Tapley, 2009).

5. Characteristics of those affected

5.1. Attributes of impacted individuals. *Although difficult to build a profile due to the heterogeneity of cases and the widespread nature of scams, we consider two approaches:*

Scam detection ability. *People can be split into three groups based on their ability to spot scams: (1) those who lose money often lack prior knowledge of scam tactics and may believe they are immune from scams; (2) near-misses initially engage with scammers but become sceptical and withdraw before harm is done (3) evaders display the highest levels of vigilance, knowledge of scam tactics, financial and media literacy, and social support.*

Dimensions of vulnerability. *Scammers exploit individuals' vulnerabilities. FCA guidance identifies four drivers of vulnerability: capability, (many people lack the ability, interest and confidence to manage their finances effectively); life events, (external events may distract individuals and impede their ability to focus); resilience (social isolation and loneliness increase the risk of scam participation in older adults due to the lack of opportunities to discuss financial decisions with others); and health (as people age, cognitive abilities important for making informed consumer decisions, tend to decline).*

5.2 Repeat targeting. *Individuals who have lost money to scams may become repeat targets for scammers, either by the same scammer or by others. With each subsequent occurrence, the likelihood of further targeting increases, with some people becoming what is known as 'chronic' victims or 'super targets'.*

Traits that make individuals more susceptible to repeated targeting include enjoying risk-taking or having unfulfilled emotional or financial needs. Chronic targets may not even realise they are caught up in a scam. This makes it challenging to intervene and help them break free from the cycle.

5.1 Attributes of impacted individuals.

"The thing is that anyone who's been scammed,...[they're] the last person usually to know because, of course, no one's going to knowingly put their money at risk. No one's going to do that. You are convinced you are doing the best thing for yourself, and someone has sold that to you, and you are completely convinced. It's only afterwards - and that adds insult to injury because you're let down by someone that you thought you trusted, so there is no straightforward profile [of those targeted]" - Pension professional

Understanding the profile of those more susceptible to being scammed is crucial for the targeted design of anti-scam interventions. There is a common perception that those who suffer from scams or consumer fraud are old, greedy, gullible or irresponsibly ignored warning signs (Scheibe et al., 2014; NCPQSW, 2020). This is not only untrue but also excuses the criminal behaviour of scammers.

The more a demographic group is targeted, the more likely it is individuals from this group will lose money to a scam, even if they are not more likely to fall for a scam than other groups (Kieffer and Mottola, 2017). It is not possible to disentangle whether a demographic (e.g. older adults) is disproportionately represented among those affected because they are more likely to be targeted - they have more pension assets (Scheibe et al., 2014) - or because they are more vulnerable.

Affluent, financially literate men living in urban centres and highly rural areas in the South East of England are the largest group who lose money as a consequence of investment crime (Graham, 2014). But ultimately, anyone can be affected: those who lose money through financial scams are not restricted to common demographic and socio-economic factors such as gender, age, marital status, education, employment status, place of living, household income or household assets (Kadoya, Khan and Yamane, 2020).

In this section, we present two ways to consider the attributes of those more likely to be affected: firstly, an individuals' ability to spot scams as a predictor of being affected and secondly, dimensions of vulnerability. One other approach, identifying "character traits", is included in Appendix 3.

Scam detection ability

In 2019, the FCA conducted a survey to investigate the awareness, attitudes and behaviours of the public towards known risk signals of pension scams. The survey revealed that 42% of the respondents remained vulnerable (FCA, 2019a). One approach which researchers of both general and investment scams have used to understand the likelihood of someone losing money through a scam is by classifying people on their ability to spot scams (ASIC, 2002a; Kieffer and Mottola, 2017; HTBSC, 2021). People can be split into three groups - those who lose money due to a scam, near-misses, and evaders - and the likelihood to fall into any of these categories will be correlated with the vulnerabilities presented below.

Those who lose money through financial scams often lack prior knowledge of scam tactics. They may believe that they are immune to scams or can recover losses (HTBSC, 2021). Some people who do not recognise an offer as a scam still 'escape' because they are just not interested in what the scammer is selling (ASIC, 2002a).

Near-misses are individuals who engage with scammers but manage to avoid being scammed. Demographically there is little to differentiate them from those who lose money, and they may initially believe the scam represents a good bargain, or that the scammers are sincere. However, 'near-misses' are more vigilant than those who lose money and tend to have better knowledge of scam tactics. They become sceptical before acceding to scammers' requests. Others were 'saved' by some external event, such as the intervention of friends or family (Kieffer and Mottola, 2017; HTBSC, 2021).

Evaders display the highest level of protective attitudes and behaviours, such as vigilance, knowledge of scam tactics, financial literacy, and social support. They claim that they do not entertain scam approaches and usually ignore calls, texts, or emails from unknown senders. Evaders' scam alerts for cold-calling investment scams included: the opportunity came 'out of the blue', was 'too good to be true', 'didn't add up' or its foreign nature was suspicious (ASIC, 2002b). Evaders have high self-esteem and the lowest levels of impulsivity, compliance, and complacency. Conscientiousness is also an essential trait of evaders. Those with higher conscientiousness are less vulnerable because they are more likely to judge offers logically, which protects them from scams (Kadoya, Khan and Yamane, 2020; HTBSC, 2021).

Dimensions of vulnerability

Effective scamming relies on the perpetrator's ability to exploit a person's vulnerabilities - anyone seeking to better their financial, physical, or emotional state can be susceptible (NCPQSW, 2020). Our pension professionals (2023) gave examples including individuals with small pension pots who are desperate for cash; individuals distracted by other responsibilities in life, such as parenthood; and individuals looking for new ways to make their money grow. This is consistent with FCA guidance (2021b) which says firms should view vulnerability as a range of potential risks and recognise that any customer can become vulnerable, giving four drivers of vulnerability: capability, life events, resilience and health.

Capability

"[It] tends to be somebody who's between the ages of about .. 60 and 75. So they're just old enough to have. . not .. a massive familiarity with technology, but also young enough to .. use online banking …or have a smartphone. So, that's the sort of demographic, I think they are targeted perhaps more than any other now, and are the ones who give the scammers dollar signs in their eyes" - Pension professional

Lacking pension knowledge. Many people exhibit low levels of financial literacy, and consequently lack confidence in managing their finances effectively (FCA, 2021b). This is particularly true when it comes to pensions, which are widely regarded as being complex and

difficult to understand, with individuals frequently having minimal contact with their pension provider or scheme until they wish to access their pension savings at retirement (TPR, 2021). The legislative changes that have been made to allow greater pension freedom have not been accompanied by a corresponding increase in public understanding of the risks associated with scams, nor of the personal responsibilities that come with managing one's finances (Skidmore, 2020). According to a recent FCA (2022) survey, over 50% of the population feel uncertain about growing their pension savings; 38% are unsure about pensions in general; and 24% take 24 hours or less to decide on a pension offer - with some consumers focusing on the immediate benefits rather than considering the long-term value (Skidmore, 2020). Our interviews with pension professionals (2023) described how some clients were not aware what their pension was invested in; thought their pensions were safe like bank deposits; or thought if there was a problem the state would step in. Despite a lack of understanding, the uptake of regulated financial advice which may warn of scams remains low (TPR, 2021), and the advice that is given may not always be of the highest quality (Skidmore, 2020). Some interviewees affected by scams (2023) had been proactively seeking advice when they were targeted because they did not feel confident in making decisions about their pension. Unfortunately, scammers are able to exploit people's misunderstandings about how pensions work (TPR, 2021).

Being highly educated. People who are highly educated are more susceptible to pension scams, shown by research that individuals with a university degree are 40% more inclined to agree to a free pension review from an unfamiliar company, and 21% more likely to accept an offer for early access to their pension, both common pension scams tactics (FCA, 2019b). It is important to note that these statistics are correlations and don’t imply a causal relationship between education and the risk of being affected - it might simply be that those with higher levels of education tend to have larger pension pots or are more likely to look for financial advice in general.

Being overconfident. Overconfidence in one's financial knowledge increases the risk of becoming affected by a scam (Gamble et al., 2013). A 2005 Organisation for Economic Co-operation and Development (OECD) report analysing financial literacy survey results across 11 countries found that many consumers believe they have a greater understanding of financial concepts than they actually do. In the UK, nearly 63% of survey respondents said they were confident about making pension decisions, but the same percentage would trust someone offering pensions advice 'out of the blue' – a major scam warning sign (FCA, 2022). Research by Citizen’s Advice was even more concerning: 88% consumers selected a pension offer which contained one of three pension scam warning signs, and of these 87% had identified themselves as being confident at spotting scams (Citizens Advice, 2016). In Australia, ASIC's (2002b) investigation into those exploited by an international cold-calling scam found investors not only underestimated the likelihood of an 'out-of-the-blue' investment offer being 'too good to be true' but also disregarded the recommendations of others, such as family, friends, and experts, believing that they knew better or were willing to take a gamble. Snyder (1986), studying those who lost money through gambling swindles found that excessive confidence regarding one's knowledge can increase susceptibility to scams. In Snyder's analysis, people typically fall prey to such scams because they extrapolate success from one area of their life, like their occupation, and apply it to the context of gambling. The persona of ‘Daniel’ presented below provides an illustration of this

group.[15]

Daniel, 58

Lives in Derby with his wife and two children.

Successful small business.

- Daniel is the owner of a small business. He's confident about his knowledge on financial matters as he has successfully run his business for many years.
- He's in a good pension scheme but he wants to make the most of his money. He's sure he can beat the market, so he has decided to take out some of his money and reinvest it.
- Daniel doesn't want to pay for a financial advisor since he thinks he's aware of the risks and has a clear understanding of where he can put his money. He finds dealing with "pettifogging bureaucracy" and "the nanny state" extremely frustrating.
- An acquaintance from Daniel's golf club recommended he invest in storage units. He was told by buying them he will receive a high guaranteed rent. The units are based abroad which helps him diversify his portfolio. His wife is not so sure about that decision but he dismisses her concerns as she has never really cared about investments anyway.

Life events

Being distracted. Pension savers affected by scams often lack the motivation or ability to thoroughly process information, leading them to disregard specific attributes that could help distinguish scam messages from legitimate offers. This results in errors of judgement (Langenderfer and Shimp, 2001). Reduced motivation can stem from the content of scam messages, which as described earlier can provoke visceral responses or create a sense of urgency that puts the target under time pressure. Alternatively, external events may distract individuals and impede their ability to focus. Those who are successfully exploited are often experiencing significant distractions, acute stress, or emotional strain when they are targeted. This leads to a 'scarcity mindset' and tunnelling, with a disproportionate focus on the problem at hand and a higher risk of missing the warning signs of a scam (Mullainathan and Shafir, 2013). The persona of 'Jenny' below illustrates this.

[15] We created the personas in this report by combining evidence from the literature and insights from our interviews into 'typical' cases. The personas do not represent specific individuals.

Jenny, 48

Lives in London with her two children, aged 13 & 15 and her mother, aged 78.

She's a single mum and has to take care of her children and mother, meaning she has to work part-time.

- Jenny works part-time as a secretary in local government for a disorganised boss. There are redundancy rumours. Due to her caring responsibilities, she cannot work additional hours and is limited to 15 hours per week.
- Jenny is too busy dealing with her job and family to look into how her pension exactly works or risks such as pension scams. She thinks pensions are safe.
- She has heard a lot in the news about the cost of living crisis Money concerns take up a lot of headspace for Jenny as she worries she won't be able to pay her rent or rising energy bills, when she retires.
- She's thinking about searching through Google for options to increase the size of her pension pot, even if that involves transferring it from the local government scheme.

Experiencing financial dissatisfaction. Although pension liberation scammers, for example, often prey on desperate individuals in need of quick cash (Spalek, 1999), household income is not a significant factor in determining susceptibility to financial scams. Instead, it is the level of financial dissatisfaction that is most strongly associated with falling for a fraud, suggesting financially dissatisfied individuals, of whatever income group, are more likely to engage in risky investment projects in the hope of increasing their income (Kadoya, Khan and Yamane, 2020). One interviewee who had been affected by a scam (2023) said they needed more money to support a relative moving from overseas to the UK. They thus had a perceived, and arguably legitimate, need for more money, even if they were able to meet basic needs. Our pension professional interviewees also found those affected were often not satisfied with the returns they received on their current pension schemes. Many middle-aged adults are unsure about their retirement income and employment prospects, even if they have received tertiary education. As a result, they may be more likely to take risks with their finances (Lichtenberg et al., 2016).

"I was going through court cases [...] regarding access and custody of my son. I was quite desperate for money." - Person affected by a scam

Resilience

Experiencing social isolation or loneliness. Lack of social support is associated with scam

susceptibility (James, Boyle and Bennett, 2014). Social isolation and loneliness have been identified as contributing factors to susceptibility to scams and fraud, with socially isolated older adults being particularly vulnerable (Ganzini, McFarland and Bloom, 1990). Social isolation describes a lack of contact with friends, family, and the community, while loneliness describes how a person perceives their level of social interaction (Lubben et al., 2015). People who are socially isolated are at a higher risk of falling for scams because they have fewer opportunities to discuss their financial decisions with others (Age UK, 2015). For example, childless individuals are more likely to become victims of fraud, as the perpetrators take advantage of those lacking trustworthy relatives to safeguard their assets (DeLiema, 2018). Other pension professional interviewees found that those affected were often isolated; and that older individuals often have limited knowledge of technology. This situation makes them an easier target since they will trust the requests of the scammers. Depression and social needs-fulfilment are also factors associated with falling for financial scams, since depressed individuals may be more susceptible to influence by socially skilled scammers to curb their loneliness (Lichtenberg, Stickney and Paulson, 2013; Lichtenberg et al., 2016). According to Olivier, Burls, Fenge, and Brown (2015), participating in scams may give individuals a feeling of usefulness by engaging them in a significant activity and providing them with a sense of purpose and so they are reluctant to discontinue their involvement.

Age-related social reasons. Older adults tend to be more trusting of unfamiliar faces, which can increase their susceptibility to fraudsters (Kieffer and Mottola, 2017; Shao et al., 2019). Carstensen and colleagues (2005) have found that older adults exhibit a 'positivity effect' whereby they tend to prefer positive information over negative information during decision-making, compared to younger adults. This preference for positive information may make older adults more vulnerable to consumer fraud, as they may focus on the potential rewards (positive cue) and overlook the associated costs or fees (negative cue). Older people are also less likely to acknowledge fraud (AARP, 2011).

Health

Suffering cognitive decline or impairment. As people age, their 'fluid' cognitive abilities, such as processing speed, working memory, and episodic memory - crucial for making consumer decisions - tend to decline, starting from their early twenties and continuing throughout their adult years (Salthouse and Ferrer-Caja, 2003). This cognitive decline may reduce older people's ability to comprehend scam messages. A decline in cognition is also linked to a decline in financial literacy, but not a decrease in self-confidence regarding managing personal finances. As discussed above, overconfidence is a risk factor. 'Cognitive impairment associated with conditions like dementia can have severe implications on individuals' daily lives including increasing vulnerability to financial abuse and financial scams' (Fenge, 2017, p. 66). Common symptoms of dementia include memory loss, communication difficulties, and issues with problem-solving and reasoning. Those with dementia and financial resources may attract those keen to exploit them. Individuals with dementia may also not be considered credible, making the detection of financial abuse and scams difficult (Alzheimer's Society, 2011; NCPQSW, 2018b). Six out of ten people living with dementia are undiagnosed (DHSC, 2011) and are particularly vulnerable as they have no care plan and are not being monitored or protected.

5.2 Repeat targeting

"So they [the scammers] weren't content with just taking the money from the sale of his house, they took his pension as well" - Pension professional

Those who have lost money already are often repeatedly targeted. As a pension professional interviewee (2023) described, individuals may be targeted until they have nothing left to give. Some individuals are targeted by other scammers for a secondary scam e.g. an investment scam followed by recovery fraud (see Section 4.1), while others are groomed by their initial scammer who continuously makes demands on them.

Scale

About 13% of those affected by scams have been hurt more than once, according to the Crime Survey for England and Wales, and 10% of reports to Action Fraud come from individuals who have been previously impacted (Poppleton, Lymperopoulou and Molina, 2021). The likelihood that a repeat crime occurs increases with each subsequent incident (Ellingworth, Farrell and Pease, 1995), with the general typology of those affected resembling an iceberg with a small number of so-called 'chronic victims' or 'super targets' at its peak (Button, Lewis and Tapley, 2009).

Risk factors for repeat targeting

"[...] there's something to understand about the world of scammers, which is that if you get scammed, once you are 'numero uno' on their list of people who they're going to pass on to the next [scamming] call centre [for payment]. Basically the way scammer data works is [that] if you scam one person, they then get put on your what's called the suckers list [...] And there's nothing more valuable in the world of scams than a suckers list" - Investigative journalist.

There are two main explanations as to why so-called 'repeat victimisation' occurs. The first explanation for repeat victimisation is 'event dependence' or 'boost.' This occurs when offenders who have successfully targeted someone learn from their experience and identify targets most likely to fall prey to their tactics. The second is called 'state heterogeneity' or 'flag.' This occurs when some targets or individuals appear more attractive to offenders, either because of their vulnerability, wealth, or other characteristics that make them more likely to fall for a scam. Examples include being too polite to hang up the phone and disengage from the fraud (Harvey et al., 2014); experiencing high levels of stress and therefore being in an emotionally vulnerable state (HTBSC, 2021); or appearing on a 'suckers list' (Grove et al., 2012). We discuss 3 other characteristics: enjoyment of risk

taking, over optimism and needs fulfilment below.

Enjoyment of risk taking. Survey respondents who reported experiencing repeat victimisation said they felt that their adventurous and addictive personalities, as well as their desire for financial success, had made them more vulnerable to fraud. These individuals were more open to possibilities and willing to take risks, which made them more likely to fall prey to scams. They contrasted their approach to life with that of their more cautious friends and family members, who were less likely to fall for scams (Harvey et al., 2014). Lyng (1990) argues that some individuals participate in active risk-taking because the experience of taking a risk provides benefits in and of itself. This draws them towards what he calls 'edgework activities', which he characterised as having an intensely seductive character. For such individuals, the personal, non-financial benefits of engaging in this 'edgework' draws them into the fraud.

Over optimism. According to research by the consultancy Heart+Mind Strategies, chronic targets often hold onto hope that the scam will eventually work out in their favour, and if not, they hope that the next opportunity will succeed (FINRA, 2021).

Needs fulfilment. Individuals who do not usually display impulsive behaviour may still take risks due to their need for emotional or financial fulfilment. Although they may take pride in their ability to carefully evaluate risks, they may feel unfulfilled by following traditional rules throughout their lives. Consequently, they take calculated risks to find the fulfilment they crave (FINRA, 2021). Fraudsters may use tactics such as grooming to create an emotional connection with the individuals they targeted (Harvey et al., 2014). While those who fall for a scam once may also experience such emotions, those who fall repeatedly may feel them more intensely. Although they may initially experience temporary feelings of fulfilment, these emotions are replaced by despair when the fraud is exposed, amplifying the original void and making them more vulnerable to future scams (FINRA, 2021).

Chronic victimisation

"[The person affected by the scam] was being told that he had become a millionaire in a very short space of time, and basically because he could see it on this platform in front of him nobody could convince him that it wasn't real" - Pension professional

Chronic targets may not even be aware that they are involved in a scam, and may not view themselves as victims. Unlike addicts, chronic targets are often unaware of their behaviour and their behaviour's outcomes, but like addicts, those individuals may be driven by unmet needs. Many of those affected develop a stronger trust in the scammer than in their own family members. As the individual becomes more deeply involved in the scam, it becomes increasingly difficult to escape. All this can make it challenging to intervene successfully (FINRA, 2021). The persona of 'Simon' illustrates a persona of the repeatedly affected.

Simon, 71

Lives in Birchwood, near Warrington, alone.

He's a widower and has two daughters that live in London with their own families.

- ➔ Simon worked his whole life as a electricity technician for a small company that helped him build a pension. He retired 5 years ago. Animal-loving Simon has always been rather shy and since his wife passed away from cancer does not socialise much.
- ➔ A year ago, he started to have memory loss problems and he struggles organising his thoughts.
- ➔ Six months ago, Simon received an email to invest his pension in an alpaca farm. He received a glossy brochure and had several phone calls with the sellers. They really seemed to care about him and about supporting him in having a good life. He thought that it was a good opportunity and agreed to transfer the money.
- ➔ He was recently contacted by the sellers who told him to send more money because the farm is having some problems and he might be lose his investment. They are now calling him daily, and its sounds very serious.
- ➔ Simon wants to contact an estate agency to sell his house and raise money to help save the alpacas. He doesn't want to get his daughters involved, because he's afraid that they will think that he cannot live by himself any longer.

6. What works - evidence and proposed solutions

6.1 Objective 1: Preventing Scams *While effective awareness campaigns can provide a first layer of protection, successful prevention will rely on impactful interventions at critical points when pension savers are about to make a decision related to their pension. We propose (1) introducing an additional point of reflection after the Pension Safeguarding Appointment and before the reference number required to make the transfer is issued, (2) increasing the salience of the risk of a transfer, (3) supporting pension savers to take alternative safer steps to make progress towards the goal they are seeking to achieve, (4) involving the pension savers' social network either when the transfer request is made or when the individual comes closer to retirement age, (5) creating teachable moments through spoof campaigns, and (6) consider introducing government-backed independent advice.*

6.2 Objective 2: Encouraging those affected to seek support *In addition to mitigating the negative impact on individuals' wellbeing and offering opportunities for recovery of (some of) the funds, encouraging uptake of support services can help with the detection of ongoing scams. We propose (1) simplifying access to support to lower the burden placed on those who want to seek redress, for example by assigning a dedicated caseworker; (2) reducing stigma by avoiding terms such as 'victim' and involving people with lived experience in support provision; (3) encouraging the social network to refer those affected for support.*

6.3 Objective 3: Lower the risk of being affected by a pension scam more than once *To lower the risk of secondary scams, we propose (1) making the risk more salient at touchpoints such as the 'Pension loss appointment' form and (2) implementing ideas such as the dedicated caseworker to reduce the risk of individuals of seeking help from illegitimate claims management companies. Supporting people at risk of 'super targeting' would likely require involving the social support network. Finally, check-ins after completion of an amber-flag transfer may help individuals spot a scam early, potentially limiting the damage.*

Organisations across the UK, including MaPS, use approaches from awareness campaigns to the amber flag system with its Pension Safeguarding Appointments to prevent pension scams. In this section, we present evidence in support of different approaches and propose additional solutions for MaPS to strengthen their prevention and support work. In line with the scope of this study, our ideas focus on MaPS' remit, rather than providing recommendations for other stakeholders or regulation. However, these ideas could be adapted to support the work of other organisations in the sector, such as pension providers or those operating helplines and supporting pension savers seeking redress.

We believe that it's important to keep three things in mind:

1. **Most people don't fall for scams most of the time**[16] - partly because awareness campaigns have made people more vigilant, partly because human instincts do work.
2. **No approach is perfect.** Each intervention provides an additional protective layer in a Swiss cheese: with holes if taken on its own, but creating a strong barrier if layered on other approaches. This means, on the one hand, that different approaches should be combined and that, on the other hand, it will be difficult to eliminate (pension) scams completely. We therefore suggest combining several of the ideas below.
3. **As scammers develop new tactics and exploit loopholes in regulation and supervision, even the most diligent and careful individuals might be affected by a scam**. One of the pension savers we interviewed told us that they had checked that both the advisor and the scheme they were transferring to were regulated and protected by the FCA and FSCS at the time when making the transfer. More than a year later, and after spotting some warning signs, they found out that the scheme had been shut down by the regulators in the meantime (Pension savers interviews, 2023). While an expert might have been able to spot the warning signs earlier, this level of expertise and diligence cannot be expected from the average pension saver. This is why, in addition to recommendations for prevention, this section also provides suggestions for how MaPS and other stakeholders can better support those who have been affected by scams.

6.1 Objective 1: Preventing Scams

Successful prevention will rely on interventions that reach pension savers at the right time, that is, ideally, when they are about to make a decision related to their pension. This might be when an individual is seeking to reinvest (part of) their pension savings to boost their pension pot, when they are trying to access the money held in a pension pot to meet immediate needs, or when they are making decisions about accessing their pension at the age of 55 or above. Indeed, we found in our interviews that many of those affected by a scam had initially looked proactively for options to reinvest or access their pension, rather than being targeted by a cold-call.

While general awareness campaigns on the MoneyHelper website and social media can provide a first layer in the Swiss cheese, other touchpoints available to MaPS provide

[16] For example, while 9.3m adults in the UK received at least one unsolicited approach which could have been a scam in the 12 months to February 2020, 8.3 of them did not respond, and 9.2 did not pay out any money (FCA, 2021a)

opportunities for more targeted interventions. These include: (1) Pension Wise appointments which are offered to all individuals over the age of 50 who have defined contribution pension savings; (2) calls to the various helplines, such as pensions and money guidance; and (3) Pension Safeguarding (PSG) Appointments, which pension savers whose transfer request has triggered an amber flag, have to attend.

In addition to general awareness campaigns, we make suggestions in particular for Pension Safeguarding Appointments and the follow-up communication, as they are the most targeted and timely opportunities for intervention. We acknowledge that these will only capture requests for transfers, rather than withdrawal and reinvestment of funds. However, similar ideas could be implemented by pension providers who have touch points with pension savers who are planning to withdraw pension savings.

Evidence on the effectiveness of awareness campaigns

The evidence base

The effectiveness of fraud prevention education initiatives is not well established, and it is challenging to obtain evidence on their efficacy (OECD, 2005; OICV-IOSCO, 2015; Kieffer and Mottola, 2017). Campaigns aiming to raise awareness of the existence of scams and providing advice on how to spot scams are a well-trodden strategy. These campaigns, such as the FCA's ScamSmart campaign or the Singapore Government's 6S Anti-Scam self-protection principles, normally explain what scams look like, what warning signs are and what steps individuals should take to protect themselves (ScamSmart, 2017; HTBSC, 2021). However, most anti-scam campaigns lack robust and formal evaluations and often rely on anecdotal information. Limited budgets are a significant contributing factor (OECD, 2005). This absence of a strong evidence base makes it difficult to determine what works or does not work to protect pension savers from harm. Additionally, the lack of accurate and dependable estimates of fraud presents a significant challenge in identifying effective strategies (OICV-IOSCO, 2015).

Factors limiting effectiveness

That said, the fact that the timing of general campaigns is, by definition, not targeted to an individual's circumstances will likely limit their effectiveness: firstly, people might have forgotten the content of the campaign when they are targeted or they might have not absorbed the content in the first place because, at the time, the campaign did not seem relevant to them. Secondly, in many instances, individuals will be successfully exploited by a scam when they are in a 'hot' state, either because of personal circumstances (such as an urgent need for money leading to severe tunnelling) or because the scammer uses tactics to move their target to this state. Even if they see a campaign at the right moment, general campaigns might, in many cases, not be sufficient to prompt individuals out of this 'hot' state.

Suggestions for strengthening awareness campaigns

However, while rigorous evidence on their effectiveness is scarce, common traits of those who evade scammers are an awareness of scam tactics and daily vigilance in dealing with financial matters. This suggests that, when done right, they are a promising first layer of

protection against scams in general. They may also contribute to a degree of 'herd immunity': the greater public awareness and discussion of scams, the more likely people will be able to protect their family and friends from being affected by them. We propose that MaPS applies the following evidence-based principles across it's various communication channels (for more detail, see Appendix 4):

Do's

- Engage the audience - This can be done by creating teachable moments (see below), appealing to emotions or using case studies to bring the challenge to life.
- Convey expertise and authority - The message should come from an authoritative source and convey expertise.
- Appeal to an individual's positive self-image - Recipients of a message are unlikely to react to it if it contradicts the image they have of themselves
- Focus the message on a clear target market - Understanding the unique motivations and needs of groups, messaging can be tailored more effectively.
- Improve skills - Focus on helping individuals identify scams, providing knowledge on tactics (rather than specific scams) and specific strategies that people can take to protect themselves against all types of scams.

Don'ts

- Avoid creating fear - While a potent motivator, it is believed to be ineffective in campaigns aimed at modifying behaviour.
- Avoid reactive behaviour - Campaigns reacting against currently prevalent scams leave consumers vulnerable as scams evolve.

Idea 1: Introduce a point of reflection

Introduce a point of reflection or additional friction to help individuals to move from a 'hot' to a 'cold' state. In the context of the PSG Appointment, implement by[17]:

- Requiring the pension saver to actively request - through an online form - that they wish to receive the unique reference number after the PSG appointment;
- Including reflection questions in the PSG Appointment notification that informs the pension saver of the requirement to attend an appointment.

Evidence in support of idea

Studies have shown that an effective way to reduce susceptibility to misinformation is to ask people to slow down for a moment and engage with the content before sharing it (Pennycook

[17] Additional friction and reflection points could also be introduced by pension providers, to further strengthen MaPS work.

and Rand, 2022). For example, a BIT study conducted in Ukraine in 2019 showed that asking both Ukrainian and Russian speakers to stop for just seven seconds before deciding if a misleading news headline was truthful or not was effective in reducing beliefs in fake news. Similarly, evidence from Korea found that introducing a period of reflection reduced the number of finalised divorces by approximately 9 percent (Wie and Kim, 2015).

Similarly, small frictions can have a disproportionate impact on people's behaviour. BIT showed that removing one click in a taxpayer's journey to file a tax return significantly increased response rates (BIT, 2015). Conversely, introducing additional frictions can help discourage undesirable behaviours. In fact, the 'friction' of a PSG appointment may already reduce scams: many pension savers whose transfer request gets an amber flag do not actually attend the PSG appointment with MaPS and instead decide to not go ahead with the transfer (Pension professionals interviews, 2023). Similarly, the FCA (2023) recently showed that introducing positive friction in the form of checkboxes and manual fields in a high-risk investment journey encourages individuals to reflect, improves their understanding of the risks and makes it less likely that they will recommend the investment to others.

Idea 2: Make the risks more salient

Use simple, direct messages to ensure that people understand that they have limited right to redress if they lose their money. Implement by:

- Clearly communicating the specific risks, including examples and relevant numbers of damage done by scams in the PSG Appointment summary;
- Combining messages on risk with requiring an active choice, e.g. by asking pension savers to confirm that they have understood the risk during the PSG Appointment.

Evidence in support of idea

Feedback from our interviews with the pension professionals shows that many people do not realise that their pension is not always protected by the government and that the circumstances where people can successfully claim compensation if they are scammed are limited (Pension professionals interviews, 2023). Additionally, people are subject to availability bias (Tversky and Kahneman, 1973), which leads to underestimating the risk if they cannot think of an example of someone like them who has lost money because of a scam. Conversely, by making the risk of a transfer more prominent through clearer and direct messages, we can exploit the so-called salience bias: people's tendency to focus on information that is particularly remarkable (Taylor and Fiske, 1975).

Idea 3: Enable substitution behaviour

Enable substitution behaviour to (1) address the perception of the 'nanny state' telling people what to do; (2) help people invest in (save) funds that are more aligned with their interests/ help meet immediate needs for money. Implement by systematically covering alternatives to taking money out of the pension during PSG appointment, such as:

- Transfers to different investments with the same provider, which (1) meet their investment objectives e.g. investing abroad; (2) aligns with their values e.g. environmental concerns;
- Money management or debt advice to provide alternative, short-term sources of funds.

Evidence in support of idea

Feedback from our interviews with the pension professionals shows that one tactic scammers use, particularly with pension savers living abroad, is persuading savers to transfer their pension to an overseas scheme, promising an escape from what they refer to as the 'nanny state' (Pension professionals interviews, 2023). Other domestic savers are encouraged to diversify their portfolio and enter lucrative markets by investing directly overseas (ASIC, 2002a).

Rather than expecting consumers to give up on a specific behaviour, it is much easier to substitute one behaviour for another, which requires little effort and which solves the same problem. Evidence suggests that this is why switching from cigarettes to e-cigarettes is much easier than quitting entirely (Brown et al., 2014). Swapping risky investments with external providers for transfers to a different account with the same provider is a similarly pragmatic first step.

We also know that some savers request access to their pensions due to an immediate need for money. For example, one pension saver interviewed stated that they needed money to support a family member's move to the UK during a period when their own earnings had decreased (Pension savers interviews, 2023). In such instances, MaPS could offer alternatives to taking money out of the pension, such as debt advice or options for loans.

Idea 4: Involve the social network

Involve family and friends as trusted advisors to support pension savers in considering different options around their pensions. Implement by:

- Prompting pension savers to speak to a number of trusted friends and family members to challenge their decision ahead of them making the investment;
- Prompting pension savers to nominate a 'retirement planning buddy' during a Pension Wise appointment or any other MoneyHelper guidance appointment This 'buddy' provides more long-term support and helps protect pension savers later on, when they might be otherwise more isolated and experience cognitive decline.

Evidence in support of idea

As outlined in Section 4.4, fraudsters use urgency in their stories and explanations to invoke 'hot states' in their targets, leading them to make snap, risky choices. We also know that those who have been affected by pension scams often do not speak to their network about this because they are embarrassed, suggesting that pension transfer choices are often made alone. At the same time, we are more likely to trust not only experts, but also those we can relate to (Durantini, Albarracin, Mitchell, Earl & Gillette, 2006). Involving friends and family members as trusted messengers could therefore help prompt pension savers out of their 'hot' state.

Idea 5: Create teachable moments

Create teachable moments where people are informed that they have interacted with a simulated scam to help to raise awareness about scams and one's own vulnerability. Implement by:

- Running social media campaigns with mock-ads similar to those used by scammers with information on how to spot scams displayed if individuals click on the link;
- Highlighting rules of thumb through an online game or during a pension appointment.

Evidence in support of idea

This is based on the idea that people might be more open to learning just after being informed of a potentially harmful mistake. One example is the spoof campaign targeting Facebook users above. Another BIT trial found that sending mock phishing emails (closely resembling actual phishing emails from past attacks) to police officers reduced the number of

officers who clicked on the link and the number of officers who submitted their login credentials (BIT, 2019).

Finally, in a study by Scheibe et al. (2014), participants were targeted by a telemarketing mock scam two to four weeks after they had received a warning either about the same or a different scam. Both types of warnings decreased participants' unconditional acceptance of the fake scam. While rejections (as opposed to expressions of doubt) were more common among those who received the same scam warning, its effectiveness, but not that of the different scam warning, decreased over time.

Idea 6: Consider providing easy access to government-backed advice and personalised guidance

Provide access to government-backed advice and/ or personalised guidance as a trusted source, to (1) reduce pension savers' vulnerability to relying on advice from private sector providers who might be involved in scams; (2) offer an option to double-check advice received elsewhere for enhanced consumer protection. Implement by:

- Relevant public/ regulatory bodies enabling the introduction of a government-backed financial advisor;[18]
- MaPS building on the MoneyHelper website's tools to bring together different sources of guidance to help individuals make a better choice if they have either been approached by a (potential) scammer or are actively looking to manage their pension.

Evidence in support of idea

Several of the individuals affected by a scam that we interviewed had indeed sought out financial advice, sometimes even checking that the advisor was regulated. However, this ultimately did not protect them from the scam. One of the pension savers interviewed by us (Pension savers interviews, 2023) said that they would have trusted advice from a government backed financial adviser and would have been prepared to pay for that advice.

"Because [Google] Chrome cannot give you financial advice, you know, you gotta be careful. But surely it's got to be some sort of Government department that [does the job of giving advice and] could override [the scam] a little bit and say, 'We are looking at this. We think you are correct [in thinking this is a scam]. I think you should go back to your financial advisor, and we [will] address it in its early stages'. [In sum, there should

[18] We acknowledge that MaPS being able to provide/ commission this advice would necessitate a change in legislation since MaPS is currently not authorised to offer financial advice. We are also aware of other legal and organisational factors, such as the distinction between advice and guidance, that would need careful consideration when deciding whether and how to implement this idea.

> *be] that sort of Government backed financial, independent financial advice" - P*erson affected by a scam

6.2 Objective 2: Encouraging those affected to seek support

MaPS is one of several public-sector organisations offering support to those who have lost money to pension scams. It operates a reporting helpline, which directs individuals to the Financial Crimes and Scams Unit operated by Money Helper, as well as pension loss appointments. However, those affected by scams often do not seek support and the current support and redress journey in the UK is fragmented. As an added benefit, encouraging uptake of support services, ideally as early as possible, could help with the detection of ongoing scams.

Idea 7: Make it easy to seek support

Simplify access to support across different public organisations, to lower the burden placed on pension savers who want to see redress. Implement by:

- Assigning pension savers affected by scams to a dedicated caseworker.
- Providing tailored guidance and information on processes to reduce 'the unknown' of what will happen during a redress process and to help pension savers navigate the support system.

Evidence in support of idea

One of the most important lessons from the behavioural science literature is that even when people want to do something, they can become deterred if it's not easy. It's important to recognise that often very small, seemingly irrelevant details can make a task feel more effortful, such as having to read unnecessary information or repeating the same steps several times. Removing these frictions makes it more likely an individual will perform the target behaviour. Similarly, communications and instructions should clearly highlight what you want people to do (or what they are required to do).

The existing system is highly fragmented and may involve several entities such as financial intermediaries, pension providers, regulators, ombudsman services, MaPS, FSCS, claims management services, and law enforcement. However, research has indicated that people often fail to engage with these services due to a lack of awareness about where to turn for help (Button, Lewis and Tapley, 2009). During our interviews, we found that some individuals, despite being highly organised and resourceful, were still struggling to navigate the system, When one interviewee was asked if they had reported the incident to the police, they

appeared surprised that no one had suggested that course of action before (Pension saver interviews, 2023). Those who are less organised, whose mental health has suffered significantly as a result of the scam, or who experience cognitive decline may face even greater difficulties in seeking redress.

"[...] sadly, quite often with us, it's usually long after the horse has bolted and it's too late to do anything, and a lot of these people are already resigned to having a frugal life in the future. Whereas prior to that, they had some quite worthwhile pension investments" - Pension professional

Idea 8: Reduce stigma

Avoid terms that could increase stigma and put people off reporting, such as 'victim'. Conversely, depict scammers consistently as resourceful, enterprising and manipulative. Implement by:

- Involving people who have been affected in the past to provide practical and emotional support as 'lived experience counsellors'
- Avoiding referring to people who have been scammed as 'victims' and countering narratives that indicate that pension savers who call in see themselves as 'victims'
- Normalising the experience of being scammed by highlighting that it can happen to anyone, and featuring testimonies of a diverse group of people who have been through a similar experience.

Evidence in support of idea

Just as consumers dismiss awareness campaigns that they do not see as applying directly to themselves (see above), evidence on bullying and harassment suggests that one reason people do not seek support is that they do not identify with the vulnerable and frightened image of a victim, for example because they may want to maintain a positive self image (Vijayasiri, 2008). Furthermore, 'anticipated stigma', that is, concerns about how others will see you once you disclose what happened to you (Overstreet and Quinn, 2013) might reduce help-seeking behaviour and the likelihood that those affected by a scam will tell their social network about it. In a study by the Money Advice Service and Revealing Reality (2017), the idea of peer-support programmes received positive feedback from over-indebted people and were seen to potentially lower the stigma associated with seeking debt advice.

Idea 9: Encourage people to refer friends and family for support

Embolden people to protect their loved ones' retirement savings (or their own inheritance). Implement by using touchpoints such as Pension Wise appointments and follow-up communication or campaigns to provide simple checklists for how to spot scams in others and how to support them.

Evidence in support of idea

We often fail to see our own vulnerability because of cognitive biases (such as overconfidence), but find it easier to spot them in others (Pronin et al, 2002). This can be exploited by shifting the responsibility for spotting warning signs from the person affected to people in their social network. Similarly, the stigma associated with being a 'victim' of a scam might prevent pension savers from identifying a scam due to cognitive dissonance (Festinger, 1957), because their self-image does not align with the mental model they hold of an individual affected by a pension scam. Beyond addressing these biases, involving the wider network may also work as a channel to boost awareness in general, contributing to 'herd immunity' at the societal level.

6.3 Objective 3: Lower the risk of being affected by a pension scam more than once

Instances of re-victimisation fall broadly into two categories (see Section 5.2): secondary scams and 'super targeting', which have different underlying causes and thus solutions.

Lower the risk of secondary scams

Individuals at risk of secondary scams such as recovery fraud may not differ in terms of their characteristics from those targeted only once. It may be more a question of (1) whether they have identified the first instance as a scam by the time they are re-targeted; (2) what support they are able to access. While it is difficult to address the timing of spotting the scam, MaPS can use their support touchpoints to apply some of the ideas from above, in particular:

Make the risk more salient (see Idea 2). Touchpoints such as the Money Helper scam helpline, the 'Pension loss appointment' form, or the 'Potential loss of pension benefits' document provide 'teachable moments', as individuals will have already identified a (potential) scam. MaPS can use these to make the risk of recovery fraud more salient by stating it upfront and help people spot the warning signs.

Make it easy to seek/ receive support (see Idea 7). Dedicated case workers and tailored guidance to accessing government support and redress will lower the risk of individuals seeking help from, for example, illegitimate claims management companies.

Support people at risk of becoming a ‘super target’

Individuals at risk of becoming ‘super targets’ often have certain characteristics that scammers can exploit, such as a larger risk appetite, a need for fulfilment or a desire for meaningful relationships (see Section 5.2).

Involve the social network (see Idea 4). Due to certain characteristics making ‘super targets’ more vulnerable and less likely to recognise or acknowledge a scam, the most promising strategy might be to bring in outside support from their social network or, in certain cases, institutions dedicated to the support of individuals with certain vulnerabilities (see Idea 9).

Idea 10: Check in after completion of an amber-flag transfer

Check in proactively at regular intervals with pension savers who have transferred despite amber flags. Implement by re-contacting pension savers to inform of risk of two-part or secondary scams.[19]

Evidence in support of idea

Scammers might re-target individuals who have previously gone ahead with an amber flag transfer, to access a different pension pot/ savings, to set up a recovery scam or as part of a two-part scam, where pension savers are convinced to transfer their pension to a different regulated investments and subsequently in high-risk, unregulated investments.

6.4 Additional recommendations

In addition to the specific ideas presented in this section, we have three more general recommendations to support the fight against pension scams. We understand that MaPS and its partners are already in the process of implementing some of them, independently of this review:

Recommendation 1: Work with PSAG to address data gaps.

As outlined in Section 3.1, a combination of underreporting and fragmented data collection make it impossible to reliably estimate the scale of scams in the UK. Due to the nature of scams as being a covert activity, this will always remain a problem. However, certain steps could help reduce the data gap:

1. Adopt a common definition across all institutions for concepts that data is reported against, including scam, problematic transfers, and attempted scams;

[19] We understand that MaPS currently does not have access to information on whether a transfer goes ahead after a PSG appointment. However, this idea could be implemented in collaboration with the relevant pension provider.

2. Consider expanding a flag system to withdrawal and reinvestment of funds, in particular for individuals under the age of 55;
3. Streamline reporting of scams by capturing all occurrences in one database and consider unique identifiers to avoid double counting;
4. Create incentives for pension providers to report suspected scams.

Recommendation 2: Systematically consult frontline staff to identify new trends.

One of the challenges with preventing scams from happening is that scammers' tactics are constantly evolving. In our interviews, we found that call handlers and scam teams working at pension providers have a good sense of the latest trends. However, these are currently not compiled in a systematic way. We recommend that MaPS develops a systematic approach to collecting and compiling qualitative data on new trends. Due to its qualitative nature, this data would not aim to capture frequency, but rather the range of tactics. While we would advise against basing awareness campaigns around specific current tactics, making these insights available as a resource would provide vigilant pension savers who want to protect themselves with the means to identify specific scams. In addition, the information could be shared with law enforcement and other agencies to support them in addressing illegal scams. For example, communications about the increase in retirement age and the new pension dashboard (see Section 4.2) provide obvious opportunities and touchpoints to warn pension savers about the dangers of related scams, using similar interventions to those outlined in Section 6.1.

Recommendation 3: Test the ideas rigorously

The ideas presented in this section are based on the evidence from the research conducted for this project. However, we know that human behaviour is highly context dependent and the impact of particular interventions is difficult to predict. We therefore recommend that MaPS tests any ideas carefully before rolling them out permanently and at scale. This will ensure that those ideas that have a cost associated with them provide good value for money and that those that do not cost anything do not backfire. While randomised control trials are generally considered the gold standard for testing impact, they might not be feasible or appropriate for assessing some of the ideas. Alternatives could include user testing to gather feedback from the target group, online experiments to test communications or carefully designed piloting phases that systematically collect data. This will allow MaPS to not only improve its own services, but also help fill the evidence gap on what works to prevent scams.

7. Conclusion

In this report, we present the evidence-base on pension scams, drawing both on the existing literature, and on the insights from speaking to those affected and professionals in the sector.

Key findings

Significant methodological challenges remain in the estimation of the scale of the problem in the UK. This is due to a mix of underreporting and a lack of systematic data collection, as well as the covert nature of scams. What is clear, though, is that the impact on those affected is often severe - ranging from having to work for longer to make up for lost pension income to severe damage to trust in financial institutions and disrupted relationships with family and friends.

The types of scams and the tactics are often very similar to investment scams more generally - something which is implicitly acknowledged by the FCA's Scam Smart campaign, which covers *all* types of scams. Scams evolve as legislation tries to catch up and external events - such as Covid or the cost of living crisis - offer new ways to exploit pension savers' fears and needs. A behavioural science lens can help us understand the tactics used: they are not dissimilar to those used in marketing and take advantage of humans' innate biases and individual vulnerabilities. That said, those affected by scams do not fall into a few easily identifiable categories - ultimately, anyone can be scammed.

The professionals we spoke to mentioned four potential future trends: (1) a renewed surge in pension liberation scams when the minimum age to access pension savings rises from 55 to 57; (2) two-part scams where pension savers are first convinced to transfer their savings to another regulated investment; (3) scams targeting smaller pots which might (re-) appear on the pension savers' radar through the new pension dashboard; (4) a continued rise in phishing, where scammers seek direct control over individuals' pensions by accessing, for example, their online accounts. It will be important for MaPS and other actors in the sector to anticipate risks and plan their response to these and other emergent threats. For example, communications about the increase in retirement age and the new pension dashboard provide obvious opportunities to warn pension savers about the dangers of related scams. While any research into trends is invariably subject to being overtaken by events, we recommend developing a structured approach to collating information on trends from those 'on the frontline' and disseminating this information to pension savers who are seeking to protect their savings.

In our interviews we found that some of those affected by scams had tried to do all the 'due diligence' before making a decision about their pension: they had sought advice and tried to research the legitimacy of the advisor and the scheme to the best of their ability, sometimes even checking whether these were registered with the FCA and covered by the compensation schemes. While these steps allowed individuals to claim compensation, it does not take away the stress associated with being exposed to the scam and the skills and

tenacity necessary to navigate the fragmented support and compensation system. MaPS's efforts should therefore focus on helping individuals to better evade scams, while at the same time making it easy for those who are affected to access support.

Proposed solutions

This review has allowed us to develop evidence-based ideas and recommendations to strengthen MaPS' and other stakeholders' existing work in preventing scams and supporting those affected. These are based on what we know about human behaviour and decision-making from the behavioural science literature. Importantly, they also draw on what we heard in our interviews with professionals and affected individuals.

The Pension Safeguarding Appointment, which pension savers have to attend who have requested a transfer that has led their current provider to trigger an 'amber flag', together with the accompanying documentation, provides the most timely opportunity for intervention. The appointment itself introduces a positive friction, that is, a little additional hoop to jump through that puts some people off pursuing a transfer any further. It could be made more effective by introducing additional friction, such as requiring individuals to confirm after the appointment that they want to take the next steps, rather than automatically receiving the reference number they will need to complete the transfer. It is also the moment where harder hitting messages alerting the individual to the risk could be made more prominent. Involving the individual's social network early on - for example at the point of receiving guidance from MoneyHelper, such as through a Pension Wise appointment - can help protect individuals early who, once targeted, might withdraw from their network, either because they are groomed by a scammer to do so or because they feel shame. Finally, while not possible under the current regulatory scheme, the introduction of government-backed independent financial advice could help address a critical market gap in the provision of sound pensions advice, as many of those affected had been cautious but ultimately did not have the skills or headspace to spot the warning signs early enough.

While introducing additional friction will prevent some scams from occurring, once an individual has been affected, it will be important to minimise the impact by removing friction in the support process. Individuals we interviewed, while appreciative of the availability of support lines such as MoneyHelper, described a confusing situation where they were sent from one place to the next in their search for redress. Navigating this system requires resourcefulness and tenacity and might therefore let down most. We therefore propose further simplifying access to support to lower the burden placed on those who want to seek redress, for example by assigning a dedicated caseworker. Avoiding stigmatising terms such as 'victim' and involving people previously affected in scams in the support provision can help normalise the experience for those affected.

Finally, in light of the paucity of evidence on what works to reduce the risk of re-targeting, additional research into the factors that make individuals more vulnerable to 'chronic' targeting is required. In the meantime, many of the ideas above will provide a certain level of protection also for those at risk of being affected by secondary scams.

Next steps

Many of our proposed solutions can be implemented within MaPS' existing offer, strengthening services such as the Pension Safeguarding of Pension Wise appointments. We encourage MaPS to further develop and test these high-level ideas in collaboration with its partners, to make sure they meet the needs of those (at risk of) being affected by pension scams.

For the ideas that would push MaPS' current remit - such as a government-backed financial advisor - this review provides evidence to be considered by sector stakeholders. While our ideas focused on MaPS' services and touchpoints with pension savers, we believe that some of them can be adopted by pension providers, reporting lines and other actors in the sector.

Finally, it is important to acknowledge that it will be impossible to fully eliminate pension scams. Instead, it's about adding as much defence capability as possible to protect citizens, putting systems in place to spot new trends and providing the best support possible to those affected. This will require a multi-agency approach, combining the forces of MaPS, regulators, law enforcement and support charities.

Bibliography

AARP (2011) AARP Foundation National Fraud Victim Survey. Washington, DC: AARP.

ABS (2023) Personal Fraud, 2021-22 financial year | Australian Bureau of Statistics. Available at: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release (Accessed: 7 March 2023).

ACCC (2022) Targeting scams. Report of the ACCC on scams activity 2021.

Action Fraud (2021) Warning from Action Fraud to #ProtectYourPension as £1.8 million lost to pension fraud so far this year. Available at: https://www.actionfraud.police.uk/protectyourpension (Accessed: 21 February 2023).

Aegon (2021) Small pots, big problem: More than a quarter of adults have at least one small pension pot. Available at https://www.aegon.co.uk/news/small_pots_big_problemmorethanaquarterofadultshaveatleastonesmal.html

Age UK (2015) Only the tip of the iceberg: Fraud against older people Evidence review. Available at: https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf.

Age UK (2016) Scamming and its effect on vulnerable individuals. Available at: https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/age_uk_briefing_fraud_and_scams_sept_2016.pdf (Accessed: 14 February 2023).

Age UK (2022) Pensions scams and fraud. Available at: https://www.ageuk.org.uk/information-advice/money-legal/pensions/pension-scams/ (Accessed: 22 February 2023).

AgeUK (2018) Applying the brakes: Slowing and stopping fraud against older people. Available at: https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf.

Alzheimer's Society (2011) Short changed: Protecting people with dementia from financial abuse. Available at: https://www.alzheimers.org.uk/sites/default/files/migrate/downloads/short_changed_-_protecting_people_with_dementia_from_financial_abuse.pdf.

Andersen, S., Hanspal, T. and Nielsen, K.M. (2019) 'Once bitten, twice shy: The power of personal experiences in risk taking', Journal of Financial Economics, 132(3), pp. 97–117.

Anderson, A., Baker, F. and Robinson, D.T. (2017) 'Precautionary savings, retirement planning and misperceptions of financial literacy', Journal of Financial Economics, 126(2), pp. 383–398. Available at: https://doi.org/10.1016/j.jfineco.2017.07.008.

Ariely, D. et al. (2009) 'Large stakes and big mistakes', The Review of Economic Studies, 76(2), pp. 451–469.
Asch, S.E. (1956) 'Studies of independence and conformity: I. A minority of one against a unanimous majority.', Psychological monographs: General and applied, 70(9), p. 1.
ASIC (2002a) Hook, line & sinker: Who takes the bait in cold calling scams? 15. Sydney: Australian Securities and Investments Commission,.
ASIC (2002b) International cold calling investment scams. 14. Australian Securities & Investments Commission. Available at: https://download.asic.gov.au/media/1339370/International_Cold_Calling_report.pdf.
BBC (2020) 'German property company collapses with my pension', BBC News, 26 November. Available at: https://www.bbc.com/news/business-55077709 (Accessed: 7 March 2023).
BIT (2015) EAST Four simple ways to apply behavioural insights. Available at: EAST Four simple ways to apply behavioural insights.
BIT (2016) Applying behavioural insights to tackle social engineering fraud. An evidence review.
BIT (2017) Helping everyone reach their potential: new education results. Available at: https://www.bi.team/blogs/helping-everyone-reach-their-potential-new-education-results / (Accessed: 27 March 2023).
BIT (2019) The Behavioural Insights Team Annual Report 2017-18. Available at: https://www.bi.team/wp-content/uploads/2019/01/Annual-update-report-BIT-2017-2018.pdf.
BIT (2022) Economy. BIT Review. Available at: https://www.bi.team/wp-content/uploads/2023/01/BIT-Review-2021-22-Economy.pdf.
Blanton, K. (2012) 'The rise of financial fraud: Scams never change but disguises do', Center for Retirement Research working paper [Preprint].
Brehm, S.S. and Brehm, J.W. (2013) Psychological reactance: A theory of freedom and control. Academic Press.
Brenner, L. et al. (2020) 'Consumer fraud victimization and financial well-being', Journal of Economic Psychology, 76, p. 102243.
Brown, J. et al. (2014) 'Real-world effectiveness of e-cigarettes when used to aid smoking cessation: a cross-sectional population study', Addiction, 109(9), pp. 1531–1540.
Button, M., Lewis, C. and Tapley, J. (2009) 'Fraud typologies and the victims of fraud: Literature review'.
Button, M., Lewis, C. and Tapley, J. (2014) 'Not a victimless crime: The impact of fraud on individual victims and their families', Security Journal, 27, pp. 36–54.
CAFC (2021) Fraud: Recognize Reject Report Canadian Anti-Fraud Centre Annual Report 2021. Available at: https://publications.gc.ca/collections/collection_2022/grc-rcmp/PS61-46-2021-eng.pdf.
Carstensen, L.L. and Mikels, J.A. (2005) 'At the intersection of emotion and cognition: Aging and the positivity effect', Current directions in psychological science, 14(3), pp. 117–121.
Cho, J.-H., Cam, H. and Oltramari, A. (2016) 'Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis', in 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE, pp. 7–13.
Cialdini, R.B. (2007) Influence: The psychology of persuasion. Collins New York.

cifas (2020) Avoiding pension & investment fraud in a pandemic | Cifas. Available at: https://www.cifas.org.uk/insight/fraud-risk-focus-blog/coronavirus-pension-fraud-advice (Accessed: 20 February 2023).

Citizens Advice (2016) Too good to be true? Available at: https://www.citizensadvice.org.uk/Global/CitizensAdvice/welfare%20publications/Too%20good%20to%20be%20true%20-%20Understanding%20consumer%20experience%20of%20pension%20scams%20a%20year%20on%20from%20pension%20freedoms.pdf

Comet, C. (2011) 'Anatomy of a fraud: Trust and social networks', Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique, 110(1), pp. 45–57.

Cressey, D.R. (1953) 'Other people's money; a study of the social psychology of embezzlement.'

Cross, C. et al. (2016) Improving responses to online fraud victims: An examination of reporting and support. Criminology Research Advisory Council.

DBS (2022) 'Dear Victim'. Understanding the psychology behind scams. Available at: https://www.dbs.com/livemore/money/understanding-the-psychology-behind-scams.html (Accessed: 27 February 2023).

Deevy, M., Lucich, S. and Beals, M. (2012) 'Scams, schemes, & swindles: A review of consumer financial fraud research. Financial Fraud Research Center'. Stanford Center on Longevity. Retrieved from http://longevity3. stanford.

DeLiema, M. (2018) 'Elder fraud and financial exploitation: Application of routine activity theory', The Gerontologist, 58(4), pp. 706–718.

DHSC (2011) Six out of ten people with dementia go undiagnosed – £2 million campaign launched to tackle dementia. Available at https://www.gov.uk/government/news/six-out-of-ten-people-with-dementia-go-undiagnosed-2-million-campaign-launched-to-tackle-dementia (Accessed 16 May 2023)

Dolan, P. et al. (2010) MINDSPACE: influencing behaviour for public policy. London, UK: Institute of Government. Available at: http://www.instituteforgovernment.org.uk/publications/ (Accessed: 23 February 2023).

Donelly, W. (2022) Pensions Scams and Fraud - How to Stay Alert | Lottie. Available at: https://lottie.org/news/pension-scams-and-fraud/ (Accessed: 23 March 2023).

Duffield, G. and Grabosky, P. (2001) 'The psychology of fraud. Australian Institute of Criminology [homepage on the Internet]. 2001. C2013'.

Durantini, M. R., Albarracin, D., Mitchell, A. L., Earl, A. N., & Gillette, J. C. (2006). Conceptualizing the Influence of Social Agents of Behavior Change: A Meta-Analysis of the Effectiveness of HIV-Prevention Interventionists for Different Groups. Psychological Bulletin, 132(2), 212–248. https://doi.org/10.1037/0033-2909.132.2.212

DWP (2021) Minister calls for schemes scam support. Available at: https://www.gov.uk/government/news/minister-calls-for-schemes-scam-support (Accessed: 14 February 2023).

DWP (2023) 'Review of the Occupational and Personal Pension Schemes (Conditions for Transfers) Regulations 2021 (SI 2021/1237)' Available at: https://www.gov.uk/government/publications/conditions-for-transfers-regulations-2021-review-report/review-of-the-occupational-and-personal-pension-schemes-conditions-for-transfers-regulations-2021-si-20211237 (Accessed: 7 July 2023).

Ellingworth, D., Farrell, G. and Pease, K. (1995) 'A victim is a victim is a victim-chronic victimization in four sweeps of the British Crime Survey', Brit. J. Criminology, 35, p. 360.

Farber, D.B. (2005) 'Restoring trust after fraud: Does corporate governance matter?', The accounting review, 80(2), pp. 539–561.

Farghly, F., Hayes, L., Ng, C., & Spohn, M. (2022). Pausing, reading, and reflecting: decision points in high-risk investment consumer journeys. FCA Research Note. Available at: https://www.fca.org.uk/publication/research/decision-points-consumer-journeys.pdf#page=12 (Accessed: 25 April 2023).

FCA (2017a) Inside the mind of a scammer: FCA reveals the tactics investment fraudsters use to deceive over 55s. Available at: https://www.fca.org.uk/news/press-releases/inside-mind-scammer-tactics-investment-fraudsters (Accessed: 23 February 2023).

FCA (2017b) Types of investment and pension scams. Available at: https://www.fca.org.uk/scamsmart/types-investment-and-pension-scams (Accessed: 14 February 2023).

FCA (2018a) FCA warns of increased risk of online investment fraud, as investors lose £87k a day to binary options scams, FCA. Available at: https://www.fca.org.uk/news/press-releases/fca-warns-increased-risk-online-investment-fraud-investors-scamsmart (Accessed: 24 February 2023).

FCA (2018b) How to avoid pension scams. Available at: https://www.fca.org.uk/scamsmart/how-avoid-pension-scams (Accessed: 20 February 2023).

FCA (2018c) ScamSmart prompts tens of thousands of pension holders to seek information. Available at: https://www.fca.org.uk/news/press-releases/scamsmart-prompts-tens-thousands-pension-holders-seek-information (Accessed: 14 February 2023).

FCA (2019a) 5 million pension savers could put their retirement savings at risk to scammers, 201. Available at: https://www.fca.org.uk/news/press-releases/5m-pension-savers-could-put-retirement-savings-risk-scammers (Accessed: 14 February 2023).

FCA (2019b) 22 years of pension savings gone in 24 hours. Available at: https://www.fca.org.uk/news/press-releases/22-years-pension-savings-gone-24-hours (Accessed: 14 February 2023).

FCA (2020) Aviva Plc / Aviva Bonds Plc / Aviva Investors / Aviva Investors & Pensions Ltd / Aviva Life & Pensions UK Limited (clone of FCA authorised firm), FCA. Available at: https://www.fca.org.uk/news/warnings/aviva-plc-aviva-bonds-plc-clone-fca-authorised-firm (Accessed: 7 March 2023).

FCA (2021). Scammers target over £2 million in pension pots in the last five months. Available at: https://www.fca.org.uk/news/press-releases/scammers-target-pension-pots. (Accessed: 29 March 2023).

FCA (2021a) Financial Lives 2020 survey: the impact of coronavirus. Available at: https://www.fca.org.uk/publication/research/financial-lives-survey-2020.pdf.

FCA (2021b) Guidance for firms on the fair treatment of vulnerable customers. Finalised guidance FG21/1. Available at: https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf.

FCA (2022) FCA research: A quarter of consumers would withdraw pension savings earlier to cover cost of living – making them vulnerable to scammer 'misdirection', FCA. Available at: https://www.fca.org.uk/news/press-releases/fca-research-quarter-consumers-would-withdraw-pension-savings-earlier-cover-cost-living (Accessed: 23 February 2023).

Fenge, L.-A. (2017) 'Dementia, safeguarding and scam involvement', Safeguarding Adults: Scamming and Mental Capacity, p. 65.

Festinger, L. (1957) A theory of cognitive dissonance. Stanford, 58-63: Stanford University Press.

FINRA (2021) Addressing the Challenge of Chronic Fraud Victimization. Available at: https://www.finrafoundation.org/sites/finrafoundation/files/addressing-the-challenge-of-chronic-fraud-victimization.pdf.

Fontinelle, A. (2022). The Most Common Types of Consumer Fraud. Available at: https://www.investopedia.com/financial-edge/0512/the-most-common-types-of-consumer-fraud.aspx (Accessed: 29 March 2023).

Freedman, J.L. and Fraser, S.C. (1966) 'Compliance without pressure: the foot-in-the-door technique.', Journal of personality and social psychology, 4(2), p. 195.

FTC (2022) Protecting Older Consumers 2021-2022. A report by the Federal Trade Commission. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/P144400OlderConsumersReportFY22.pdf.

Gamble, K.J. et al. (2013) 'Aging, Financial Literacy, and Fraud'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.2361151.

Ganzini, L., McFarland, B. and Bloom, J. (1990) 'Victims of fraud: Comparing victims of white collar and violent crime', Journal of the American Academy of Psychiatry and the Law Online, 18(1), pp. 55–63.

Gouldner, A.W. (1960) 'The Norm of Reciprocity: A Preliminary Statement', American Sociological Review, 25(2), pp. 161–178. Available at: https://doi.org/10.2307/2092623.

Grabosky, P.N. and Duffield, G.M. (2001) Red flags of fraud. Citeseer.

Graham, W. (2014) A quantitative analysis of victims of investment crime. London: Financial Conduct Authority. Available at: https://www.fca.org.uk/publication/research/quan-study-understanding-victims-investment-fraud.pdf.

Griggs, D. et al. (2013) 'Sustainable development goals for people and planet', Nature, 495(7441), pp. 305–307.

Grimes, G.A., Hough, M.G. and Signorella, M.L. (2007) 'Email end users and spam: relations of gender and age group to attitudes and actions', Computers in Human Behavior, 23(1), pp. 318–332.

Grove, L.E. et al. (2012) Preventing repeat victimization: A systematic review. Brottsförebyggande rådet/The Swedish National Council for Crime Prevention.

Gurun, U.G., Stoffman, N. and Yonker, S.E. (2018) 'Trust busting: The effect of fraud on investor behavior', The Review of Financial Studies, 31(4), pp. 1341–1376.

Harding, N. and Sales, T. (2022) #Clickers: Buy now, pay never. Whitepaper. We Fight Fraud. Available at: https://www.wefightfraud.org/wp-content/plugins/pdf-viewer-for-elementor/assets/pdfjs/web/viewer.html?file=https://www.wefightfraud.org/wp-content/uploads/2022/05/Whitepaper-Clickers-Buy-Now-Pay-Never-We-Fight-Fraud-2022.pdf&embedded=true.

Harford, T. (2019) ‘Richard Thaler: 'If you want people to do something, make it easy'', FInancial Times, 2 August. Available at: https://www.ft.com/content/a317c302-aa2b-11e9-984c-fac8325aaa04 (Accessed: 28 March 2023).

Harvey, S. et al. (2014) ‘Understanding victims of financial crime’, Vol [Preprint].

HMT and DWP (2017) Pension scams: consultation response. London: HM Treasury. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/638844/Pension_Scams_consultation_response.pdf.

HoC Work and Pensions Committee (2021) What is it like to be the victim of a pension scam? Available at: https://houseofcommons.shorthandstories.com/work-and-pensions-scam-victims/ (Accessed: 16 February 2023).

Home Office (2021) Economic crime research strategy: Home Office research priorities. Available at: https://www.gov.uk/government/publications/economic-crime-research-strategy-home-office-research-priorities/economic-crime-research-strategy-home-office-research-priorities (Accessed: 16 February 2023).

HTBSC (2021) Scammer, Beware: Building Societal Resilience To Scams A Behavioural Sciences Perspective. Singapore: Ministry of Home Affairs and Ministry of Sustainability and the Environment.

IFS (2023) ‘Challenges for the UK pension system: the case for a pensions review’ Available at: https://ifs.org.uk/publications/challenges-uk-pension-system-case-pensions-review

Individual affected by scam (2023) ‘Interview by BIT’.

Investigative journalist (2023) ‘Interview by BIT’.

IOSCO and OECD (2018) The Application of Behavioural Insights to Financial Literacy and Investor Education Programmes and Initiatives.

Ipsos (2020) Survey on ‘Scams and Fraud experienced by Consumers’. EU Commission. Available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

Jakubowski, Z. (2020) ‘Pension scammers hide behind QROPS verification’, Accountancy Daily, 2 January. Available at: https://www.accountancydaily.co/pension-scammers-hide-behind-qrops-verification (Accessed: 16 February 2023).

James, B.D., Boyle, P.A. and Bennett, D.A. (2014) ‘Correlates of susceptibility to scams in older adults without dementia’, Journal of elder abuse & neglect, 26(2), pp. 107–122.

Janoff-Bulman, R. (1985) ‘Criminal vs. non-criminal victimization: Victims’ reactions’, Victimology, 10(1–4), pp. 498–511.

Jones, R. (2022) ‘Thousands of UK steelworkers victims of pension regulation scandal, says NAO’, The Guardian, 18 March. Available at: https://www.theguardian.com/business/2022/mar/18/thousands-of-uk-steelworkers-victims-of-pension-regulation-scandal-says-nao (Accessed: 7 March 2023).

Judges, R.A. et al. (2017) ‘The role of cognition, personality, and trust in fraud victimization in older adults’, Frontiers in psychology, 8, p. 588.

Kadoya, Y., Khan, M.S.R. and Yamane, T. (2020) 'The rising phenomenon of financial scams: evidence from Japan', Journal of Financial Crime, 27(2), pp. 387–396. Available at: https://doi.org/10.1108/JFC-05-2019-0057.

Kahneman, D. and Tversky, A. (1979) 'Prospect Theory: An Analysis of Decision under Risk', Econometrica, 47(2), pp. 263–291. Available at: https://doi.org/10.2307/1914185.

Kaplan, S. and Reckers, P.M. (1995) 'Auditors′ reporting decisions for accounting estimates: the effect of assessments of the risk of fraudulent financial reporting', Managerial Auditing Journal [Preprint].

Katz, S. and Mazur, M.A. (1979) Understanding the rape victim: A synthesis of research findings. Wiley New York.

Keller, P.A. et al. (2011) 'Enhanced active choice: A new method to motivate behavior change', Journal of Consumer psychology, 21(4), pp. 376–383.

Kieffer, C. and Mottola, G. (2017) 'Understanding and combating investment fraud', Financial decision making and retirement security in an aging world, 185.

Langenderfer, J. and Shimp, T.A. (2001) 'Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion', Psychology & Marketing, 18(7), pp. 763–783.

Levi, M. (1988) The prevention of fraud. Citeseer.

Levi, M. and Pithouse, A. (1992) The victims of fraud. Springer.

Lichtenberg, P.A. et al. (2016) 'Psychological and Functional Vulnerability Predicts Fraud Cases in Older Adults: Results of a Longitudinal Study', Clinical Gerontologist, 39(1), pp. 48–63. Available at: https://doi.org/10.1080/07317115.2015.1101632.

Lichtenberg, P.A., Stickney, L. and Paulson, D. (2013) 'Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults?', Clinical Gerontologist, 36(2), pp. 132–146. Available at: https://doi.org/10.1080/07317115.2012.749323.

Loewenstein, G. (2005) 'Hot-cold empathy gaps and medical decision making', Health Psychology, 24, pp. S49–S56. Available at: https://doi.org/10.1037/0278-6133.24.4.S49.

Loewenstein, G.F. et al. (2001) 'Risk as feelings', Psychological Bulletin, 127(2), pp. 267–286. Available at: https://doi.org/10.1037/0033-2909.127.2.267.

Lubben, J. et al. (2015) Social Isolation Presents a Grand Challenge for Social Work, American Academy of Social Work and Social Welfare Working Paper No. 7. Available at: https://aaswsw.org/wp-content/uploads/2015/03/Social-Isolation-3.24.15.pdf.

Lyng, S. (1990) 'Edgework: A Social Psychological Analysis of Voluntary Risk Taking', American Journal of Sociology, 95(4), pp. 851–886.

Maguire, M. and Bennett, T. (1982) Burglary in a dwelling: the offence, the offender and the victim. Heinemann London.

Malmendier, U. and Nagel, S. (2011) 'Depression babies: Do macroeconomic experiences affect risk taking?', The quarterly journal of economics, 126(1), pp. 373–416.

MaPS (2021) How MaPS can help those who have been scammed on their pensions | The Money and Pensions Service. Available at: https://maps.org.uk/2021/06/21/how-maps-can-help-those-who-have-been-scammed-on-their-pensions/ (Accessed: 14 February 2023).

MaPS (2021) TPR and MaPS key messages on pension safeguarding. | The Money and Pensions Service. Available at: https://moneyandpensionsservice.org.uk/wp-content/uploads/2021/12/the-pensions-regulator-and-money-and-pensions-service-pension-safeguarding-key-messages-nov21.pdf (Accessed: 29 March 2023).

Mason, K.A. and Benson, M.L. (1996) 'The effect of social support on fraud victims' reporting behavior: A research note', Justice Quarterly, 13(3), pp. 511–524.
Milgram, S. (1963) 'Behavioral study of obedience.', The Journal of abnormal and social psychology, 67(4), p. 371.
MMMI, National Committee for the Prevention of Elder Abuse, and Center for Gerontology at Virginia Polytechnic Institute and State University (2009) Broken Trust: Elders, Family, and Finances. MetLife Mature Market Institute.
Mohamed, Y.K., Khair, K.A.H. and Jon, S. (2015) 'Fraudulent financial reporting: an application of fraud models to Malaysian public listed companies', The Macrotheme Review, 4(3), pp. 126–145.
Money Advice Service & Revealing Reality (2017). Moving forward together: peer support for people with problem debt.
MoneyHelper (n.d.) How to spot a pension scam, MaPS. Available at: https://www.moneyhelper.org.uk/en/money-troubles/scams/how-to-spot-a-pension-scam (Accessed: 20 February 2023).
Mullainathan, S. and Shafir, E. (2013) Scarcity: Why having too little means so much. Macmillan.
Murphy, P.R. and Free, C. (2016) 'Broadening the fraud triangle: Instrumental climate and fraud', Behavioral Research in Accounting, 28(1), pp. 41–56.
NCA (n.d.) Our mission. Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/our-mission (Accessed: 15 February 2023).
NCPQSW (2018a) Cyber Fraud and Scamming. Bournemouth University. Available at: https://ncpqsw.com/publications/cyber-fraud-and-scamming/ (Accessed: 4 January 2023).
NCPQSW (2018b) 'Financial Scamming and Fraud'. Bournemouth University. Available at: https://ncpqsw.com/publications/financial-scamming-and-fraud/ (Accessed: 4 January 2023).
NCPQSW (2020) 'Scams: the power of persuasive language'. Bournemouth University. Available at: https://www.bournemouth.ac.uk/sites/default/files/asset/document/Scams%20-%20the%20power%20of%20persuasive%20language.pdf (Accessed: 4 January 2023).
Nickerson, R.S. (1998) 'Confirmation bias: A ubiquitous phenomenon in many guises', Review of general psychology, 2(2), pp. 175–220.
Norris, G., Brookes, A. and Dowell, D. (2019) 'The Psychology of Internet Fraud Victimisation: a Systematic Review', Journal of Police and Criminal Psychology, 34(3), pp. 231–245. Available at: https://doi.org/10.1007/s11896-019-09334-5.
OECD (2005) Examining Consumer Policy: A Report on Consumer Information Campaigns Concerning Scams. OECD Digital Economy Papers, No. 103. Paris: OECD Publishing. Available at: https://doi.org/10.1787/231767418167.
OICV-IOSCO (2015) Survey on Anti-Fraud Messaging. FR06/2015. The Board of the International Organization of Securities Commissions. Available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD485.pdf.
Olivier, S. et al. (2015) ''Winning and losing': vulnerability to mass marketing fraud', The Journal of Adult Protection, 17(6), pp. 360–370.

ONS (2018) Pensions, savings and investments. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/personalandhouseholdfinances/pensionssavingsandinvestments (Accessed: 14 February 2023).

ONS (2022a) Nature of fraud and computer misuse in England and Wales - Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 (Accessed: 24 March 2023).

ONS (2022b) Saving for retirement in Great Britain - Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/personalandhouseholdfinances/incomeandwealth/bulletins/pensionwealthingreatbritain/april2018tomarch2020 (Accessed: 14 February 2023).

Overstreet, N. M., Earnshaw, V. A., Kalichman, S. C., & Quinn, D. M. (2013). Internalized stigma and HIV status disclosure among HIV-positive black men who have sex with men. AIDS care, 25(4), 466-471.

Parker, A.M. et al. (2012) 'Inappropriate confidence and retirement planning: Four studies with a national sample', Journal of Behavioral Decision Making, 25, pp. 382–389. Available at: https://doi.org/10.1002/bdm.745.

Pattinson, M.R. et al. (2011) 'Managing Phishing Emails: A Scenario-Based Experiment.', in HAISA, pp. 74–85.

Pennycook, G. and Rand, D.G. (2022) 'Accuracy prompts are a replicable and generalizable approach for reducing the spread of misinformation', Nature Communications, 13(1), p. 2333. Available at: https://doi.org/10.1038/s41467-022-30073-5.

Pension Professionals (2023) 'Interview by BIT'.

Pension Scams Industry Group (PSIG) (2018). The PSIG Scams Survey Pilot 2018. Available at: https://docs.wixstatic.com/ugd/ca2947_529582a813cb457a80ba48cb1e20c8b0.pdf

Perloff, L.S. (1983) 'Perceptions of vulnerability to victimization', Journal of Social Issues, 39(2), pp. 41–61.

Perri, F.S. and Brody, R.G. (2012) 'The optics of fraud: Affiliations that enhance offender credibility', Journal of Financial Crime [Preprint].

Petty, R.E. et al. (1986) The elaboration likelihood model of persuasion. Springer.

Poppleton, S., Lymperopoulou, K. and Molina, J. (2021) 'Who suffers fraud? Understanding the fraud victim landscape'. The Victims' Commissioner.

Pratkanis, A.R. (2011) The science of social influence: Advances and future progress. Psychology Press.

Pratkanis, A.R. and Farquhar, P.H. (1992) 'A brief history of research on phantom alternatives: Evidence for seven empirical generalizations about phantoms', Basic and applied social psychology, 13(1), pp. 103–122.

Pronin, E., Lin, D. Y., & Ross, L. (2002). The Bias Blind Spot: Perceptions of Bias in Self Versus Others. Personality and Social Psychology Bulletin, 28(3), 369–381. https://doi.org/10.1177/0146167202286008

Rehman, S.U. et al. (2005) 'What to wear today? Effect of doctor's attire on the trust and confidence of patients', The American journal of medicine, 118(11), pp. 1279–1286.

Reisig, M.D. and Holtfreter, K. (2013) 'Shopping fraud victimization among the elderly', Journal of Financial Crime [Preprint].

Ross, M., Grossmann, I. and Schryer, E. (2014) 'Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud', Perspectives on Psychological Science, 9(4), pp. 427–442.

Rusch, J. (2008) The 'Social Engineering' of Internet Fraud. Available at: https://web.archive.org/web/20080617150031/http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm (Accessed: 23 February 2023).

Sacks, D.W., Stevenson, B. and Wolfers, J. (2012) 'The new stylized facts about income and subjective well-being.', Emotion, 12(6), p. 1181.

Salthouse, T.A. and Ferrer-Caja, E. (2003) 'What needs to be explained to account for age-related effects on multiple cognitive variables?', Psychology and aging, 18(1), p. 91.

Sandhu, N. (2020) 'Behavioral red flags of fraud: a gender-based ex post analysis', Journal of Financial Crime, 27(4), pp. 1307–1322.

ScamSmart (2017) FCA. Available at: https://www.fca.org.uk/scamsmart (Accessed: 27 March 2023).

Scheibe, S. et al. (2014) 'Forewarning reduces fraud susceptibility in vulnerable consumers', Basic and applied social psychology, 36(3), pp. 272–279. Available at: https://doi.org/10.1080/01973533.2014.903844.

Segal, M., Doron, I. and Mor, S. (2021) 'Consumer fraud: Older people's perceptions and experiences', Journal of Aging & Social Policy, 33(1), pp. 1–21.

Shadel, D., Pak, K. and Gannon, J. (2010) 'The Effects of Investment Fraud Workshops on Future Investor Resistance', in Presentation at National Academy of Sciences meeting on Elder Mistreatment and Abuse and Financial Fraud, Washington, DC, June.

Shao, J. et al. (2019) 'Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud', Journal of Elder Abuse & Neglect, 31(3), pp. 225–243. Available at: https://doi.org/10.1080/08946566.2019.1625842.

Shapiro, S.P. (1990) 'Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime', American Sociological Review, pp. 346–365.

Sharot, T. (2011) 'The optimism bias', Current Biology, 21(23), pp. R941–R945. Available at: https://doi.org/10.1016/j.cub.2011.10.030.

Shover, N., Coffey, G.S. and Hobbs, D. (2003) 'Crime on the line. Telemarketing and the changing nature of professional crime', British Journal of Criminology, 43(3), pp. 489–505.

Silvani, C. (2021) What you can learn from three high-profile pension scams, Raconteur. Available at: https://www.raconteur.net/legal/fraud/three-high-profile-pension-scams/ (Accessed: 7 March 2023).

Skidmore, M. (2020) Protecting people's pensions: Understanding and preventing scams. The Police Foundation.

Skurnik, I. et al. (2005) 'How warnings about false claims become recommendations', Journal of Consumer Research, 31(4), pp. 713–724.

Smart Pension (2021) How to spot a pension scam. Available at: https://www.smartpension.co.uk/news-and-media/how-to-spot-a-pension-scam (Accessed: 20 February 2023).

Snyder, R.J. (1986) 'Gambling swindles and victims.', Journal of gambling behavior [Preprint].

Soames Job, R.F. (1988) 'Effective and ineffective use of fear in health promotion campaigns.', American journal of public health, 78(2), pp. 163–167.
Spalek, B. (1999) 'Exploring the impact of financial crime: A study looking into the effects of the Maxwell scandal upon the Maxwell pensioners', International Review of Victimology, 6(3), pp. 213–230.
SRA (2016) Solicitors and investment fraud. Available at: https://www.sra.org.uk/globalassets/documents/sra/research/investment-fraud.pdf.
Stevenson, R.J. (1998) The boiler room and other telephone sales scams. University of Illinois Press.
Sutherland, E.H. (1983) White collar crime: The uncut version. Yale University Press.
Taylor, S.E. and Fiske, S.T. (1975) 'Point of view and perceptions of causality.', Journal of Personality and Social Psychology, 32(3), p. 439.
The Insolvency Service (2018) Court shuts down companies behind £9m truffle scam, GOV.UK. Available at: https://www.gov.uk/government/news/court-shuts-down-companies-behind-9m-truffle-scam (Accessed: 7 March 2023).
Titus, R.M. and Gover, A.R. (2001) 'Personal fraud: The victims and the scams', Crime prevention studies, 12, pp. 133–152.
TPR (2021) Our strategy to combat pension scams. Available at: https://www.thepensionsregulator.gov.uk/en/document-library/corporate-information/our-strategy-to-combat-pension-scams (Accessed: 14 February 2023).
TPR (2022) Pension scams threat assessment summary, The Pensions Regulator. Available at: https://www.thepensionsregulator.gov.uk/en/document-library/research-and-analysis/pension-scams-threat-assessment-summary (Accessed: 14 February 2023).
TPR (n.d.) Avoid or report pension scams, The Pensions Regulator. Available at: https://www.thepensionsregulator.gov.uk/en/pension-scams (Accessed: 16 February 2023).
Tversky, A. and Kahneman, D. (1973) 'Availability: A heuristic for judging frequency and probability', Cognitive psychology, 5(2), pp. 207–232.
Vijayasiri, G. (2008) 'Reporting sexual harassment: The importance of organizational culture and trust', Gender Issues, 25, pp. 43–61.
Volant, M. (2022) How to avoid a pension scam, PensionBee. Available at: https://www.pensionbee.com/blog/2022/june/how-to-spot-a-pension-scam (Accessed: 16 February 2023).
Which? (2022) The psychology of scams: Understanding why consumers fall for APP scams. Available at: https://www.which.co.uk/policy/money/9245/the-psychology-of-scams-understanding-why-consumers-fall-for-app-scams.
Wie, D. and Kim, H. (2015) 'Between Calm and Passion: The Cooling-Off Period and Divorce Decisions in Korea', Feminist Economics, 21(2), pp. 187–214. Available at: https://doi.org/10.1080/13545701.2014.999008.
Wilkinson, L. (2020) How have scams evolved since the introduction of pension freedoms? Briefing Note 121. Pensions Policy Institute.
Wolfe, D.T. and Hermanson, D.R. (2004) 'The fraud diamond: Considering the four elements of fraud', The CPA Journal, 74(12), pp. 20–25.

Wood, H. et al. (2021) ‘The silent threat: The impact of fraud on UK national security’. RUSI. Occasional Paper.

Worchel, S., Lee, J. and Adewole, A. (1975) ‘Effects of supply and demand on ratings of object value.’, Journal of personality and social psychology, 32(5), p. 906.

Appendix 1: Research method

A1.1 Research questions

This report seeks to explore the following research questions:

Understanding pension scams:

- What is the current scale and nature of pension scams in the UK?
- What are the underlying causes of pension scams? Who are the offenders, how do they offend and what regulatory gaps are they exploiting?
- What are the key types of pension scams and channels used? How do pension scams work/ interact with each other? What are the current trends/ how is the landscape of pension scams changing?
- Which individuals are at risk of pension scamming, for what reason and at what stage in their life? What are the key characteristics of those affected repeatedly?
- What is the impact of pension scams on those affected and the wider UK economy?

Preventing pension scams:

- What works in preventing pension scams? In particular,
    - What are the key characteristics of a successful communication aimed at preventing pension scams?
    - What are the most common pitfalls and what are the most effective ways of tackling them?
    - What can MAPS learn about how to best communicate the risk of pension scams to its customers, identify vulnerable groups early, and address their needs effectively? What can MAPS do to reduce instances of repeat scamming?
- What are the key evidence gaps in understanding pension scams and how to best prevent them?

A1.2 Approach

We combined a review of the academic and grey literature, with interviews with people affected by scams and professionals working for pension providers and government bodies.

Evidence review. We searched for and included evidence which seeks to explore the above research questions with a preference for recent publications, and, in the case of evaluations, Randomised Controlled Trials (RCT) and high-quality qualitative evaluations.[20] This included

[20] By ‘high quality qualitative evaluations’, we mean evidence (1) where the research questions are clearly linked to the research purpose, and evidence which (2) includes triangulation or uses multiple methods, and (3) is transparent about how design decisions (e.g., sample design, assumptions) and conclusions are reached. These markers for high quality are based on recommendations from published literature on this topic such as 'A Review of the Quality Indicators of Rigor in Qualitative Research' and 'Quality in Qualitative Evaluation: A framework for assessing research evidence' as well as input from BIT’s qualitative researchers.

sources from both the academic literature - such as articles published in peer-reviewed journals - as well as evidence from the grey literature, such as government policy and research reports. Initial sources were identified by keyword searches based on the research questions, with subsequent sources identified by snowballing or recommended by interview subjects. We complemented the findings from the literature review with discussions with a US pension expert to improve our understanding of the scale of pension scams in the US. It confirmed that, though impacts vary between regions and pension systems, pension scams are prevalent worldwide, and that the global scale of pension scams is undoubtedly increasing. This suggests that evidence from the US presented in this report could equally be applied to the UK.

Interviews. We interviewed professionals working for pension providers and government agencies, an investigative journalist who has extensive knowledge of scams, and people affected by pension scams in February and March 2023. We conducted semi-structured interviews with ten staff working for pension providers or MaPS helplines and spoke to relevant teams at the Department of Work and Pensions (DWP), The Pensions Regulator (TPR) and the Financial Conduct Authority's (FCA) ScamSmart campaign.

We also conducted six semi-structured interviews with people affected by pension scams. We reached out to people from MaPS' database who (1) were scammed after Pension Freedoms was introduced in 2015, and (2) were not marked as vulnerable cases.

Note:

- *The personas presented in this review are based on the evidence review and the interviews with pension professionals and those individuals affected. They do not represent specific individuals.*
- *We cite evidence from our interviews as 'Pension professionals interviews, 2023' or 'Pension savers interviews, 2023'. To protect the privacy of those interviewed, we do not provide any further information such as age or employer.*

A1.3 Limitations

Evidence gaps

While conducting this review, we identified three evidence gaps also acknowledged in the related literature:

- **Economic crime:** There is currently a lack of extensive research on the pathways through which individuals get involved in economic crime and their associations with organised and serious crime.
- **Risk factors:** While there is increasingly an understanding that vulnerability cannot simply be predicted using demographic characteristics (e.g. age), the understanding of what makes some people more likely to lose money to scams and others more resilient is still limited (Norris et al., 2019; Home Office, 2021). This gap in understanding limits the ability to design targeted and effective interventions to overcome the psychological factors that make people more vulnerable.

- **What works:** Evidence on the effectiveness of scam interventions, and indeed fraud more generally, is limited (Kieffer and Mottola, 2017; OICV-IOSCO, 2015). We therefore know little about what specifically is key to successful communication and other interventions to prevent scams specifically. There is a particular need for further research into the prevention of repeat victimisation.

Lack of quantitative data

We had initially intended to carry out quantitative analysis to better assess the scale of the problem. However, it became clear that although data on pension scams in the UK is available from many different sources including pension providers, regulators and the police, it is not complete. We describe these gaps in more detail in Section 3.1. This has implications also for our ability to quantify the impact on the UK economy.

Universal applicability of findings

Pension scams encompass a wide range of activities, varying from unethical practices and violations of financial regulations to outright criminal fraud. Scammers may tailor their scams and tactics to specific demographics and personality types. Therefore, not all findings on tactics will be universally applicable to all forms of scams and target groups. However, there is little robust evidence on differences across types of scams and demographics and we therefore do not systematically explore these in this report.

Appendix 2: Case study of a scam

This case describes international investment scams as an illustration of how different types of scams are layered and how scam has been industrialised. It is taken from a review by ASIC, the Australian Securities & Investments Commission (2002).

Boiler rooms are rooms filled with salespeople who make unsolicited calls to potential investors with the aim of convincing them to invest their money in bogus financial schemes. These salespeople use elaborate scripts and a variety of sales tactics to come across as trustworthy and knowledgeable. However, they often use fake names, titles, and business addresses, and their operations have been linked to countries such as Thailand and the Philippines, not the financial centres they claim to be located in. It is believed that some sales staff, often international tourists, are lured by the promise of high commissions to work in these boiler rooms. Investors have reported receiving calls from individuals with various accents, including English, American, Australian, New Zealand, South African, Scottish, and Irish.

During the calls, the salesperson will ask questions about the potential investor's financial situation and habits to build rapport. They will then make a seemingly attractive investment offer. To add an air of legitimacy, the salesperson will often courier impressive brochures, misleadingly referred to as 'prospectuses,' to the potential investor, which showcase both the broker and the companies they are being urged to invest in.

Some individuals have been provided with phone numbers of fake referees in an attempt to make them feel more comfortable. Potential investors are also encouraged to visit websites that broadcast stock trading data. These misleading charts display fluctuations in share prices are used to convince the potential investor to make an investment.

The cold caller's attempt at appearing legitimate does not end after securing an investment. Instead, their detailed paperwork and frequent communication often give investors a false sense of security, leading them to make multiple investments. The tactics used by the cold callers depend on the personality of the pension saver targeted. (We describe this later in section 4).

To conceal their true identity, location, and size, scammers use telephone and mail technology to create virtual offices. These offices allow them to run the scam for a limited time and collect profits without being easily traced. Once discovered, scammers simply start a new company with a different name, set of numbers, and bank accounts, and continue the cycle. Unfortunately, the investors who invested with the previous company are left stranded and unable to reach their 'brokers,' realising too late that they have fallen for the scam (ASIC, 2002b).

Appendix 3: Other approaches for considering susceptibility

Character traits

Studies that identify the behavioural characteristics which make people particularly susceptible to fraud are very limited. Instead most evidence and resulting beliefs are anecdotal (Button, Lewis and Tapley, 2009; BIT, 2016). Similarly personality theories tell us very little about why people are more likely to respond to fraudulent communications. For example, extroverts are found to take more risks and so may be expected to be more susceptible to fraud, but there is no clear mechanism which links extraversion to fraud susceptibility (Pattinson et al., 2011). Neuroticism is linked to an increased susceptibility to fraud (Cho, Cam and Oltramari, 2016), while conscientiousness is associated with a reduced likelihood of falling for fraud (Judges et al., 2017) and time-limited messages might appeal to those with lower levels of social control (Reisig and Holtfreter, 2013). However, these observations only align loosely with plausible individual-level explanations (Norris, Brookes and Dowell, 2019).

Appendix 4: Suggestions for improving effectiveness of awareness campaigns

These principles could be applied by MaPS across their various communication channels, but may also be useful to other stakeholders aiming to prevent scams.

Engage the audience. Purely information-led 'warning' campaigns may not connect with the audience (OECD, 2005), change attitudes without changing behaviour or change behaviour in a way that does not prevent the crime (Grove et al., 2012). Conversely, France's Autorité des marchés financiers (AMF) created an online campaign that aimed to capture the interest of potential investors through a witty and unorthodox approach and Nigeria SEC worked on a weekly TV soap opera which focused on scam investment schemes (OICV-IOSCO, 2015). BIT used a similar approach, creating a spoof campaign targeting Facebook users to sell them coffee machines through a fake online scam to help teach people how to avoid the actual ones. Those who received a message alerting them that this was a scam were less likely to fall for a subsequent scam (BIT, 2022). Additionally, successful social marketing campaigns aim to identify and communicate consumer benefits, rather than focusing on benefits for society at large (OECD, 2005). These campaigns often employ case studies or narratives to engage consumers and make their messages personal. For example, Spain and Hong Kong produced videos based on real-life cases to deliver anti-fraud messages on their websites in a lively and engaging manner (OICV-IOSCO, 2015).

Convey expertise and authority. A campaign's tone should reflect a level of technical understanding of the issue at hand, as well as come from an authoritative source, such as government departments. The Australian Little Black Book of Scams campaign is an example of this, as it addresses the psychology behind scams in an authoritative manner (OECD, 2005).

Appeal to an individual's positive self-image. Because of an illusion of invulnerability, consumers may dismiss campaigns that they do not see as applying directly to them (Kieffer and Mottola, 2017). Negative depictions of 'victims' are unlikely to match an individual's self image (OECD, 2005). In 2014, the US Commodity Futures Trading Commission (CFTC) conducted a survey targeting investors who were nearing retirement to identify which fraud prevention messages would resonate with them. The survey found that in order to effectively communicate with investors, it was important to first validate their sense of responsibility, competence, and independence. The messaging should focus on positive aspects, such as how to evaluate investment opportunities more effectively, rather than negative ones such as the risk of losing money due to fraud. Additionally, the study showed that investors were more likely to engage with resources and websites that were perceived as tools to help them become more knowledgeable about investment research and stay informed about new trends and scams. The CFTC incorporated these insights into the SmartCheck campaign, which leveraged the audience's overconfidence bias and emphasised social norms to encourage them to conduct

registration checks, similar to savvy investors (OICV-IOSCO, 2015; IOSCO and OECD, 2018).

Focus the message on a clear target market. Although the issues being addressed may be relevant to a broad audience, successful campaigns have identified a specific group to focus on. By understanding the unique motivations and needs of these groups, the messaging can be tailored to effectively resonate with them, which has been a critical factor in campaign success (OECD, 2005). ASIC's MoneySmart website in Australia employs search engine optimization to analyse the search terms that consumers and investors are using to search for information about scams online. By doing so, ASIC can ensure that the content and keywords on their website are relevant to these search terms, which increases the likelihood of their web pages appearing in search results (OICV-IOSCO, 2015). This approach is helpful for directing the information at those who might already be searching for information on pension investment opportunities.

Improve skills. To change behaviour, it is important to focus on improving skills to identify scams; to increase knowledge of the tactics used by scammers and to specify specific strategies that people can take to protect themselves - ideally that can be applied to all financial transactions, not just pension scams, to normalise vigilance (OECD, 2005), and are applicable regardless of the type of scam. Outsmarting Investment Fraud (OIF) is a program developed by the FINRA Investor Education Foundation and AARP, with a strong emphasis on building skills to combat investment fraud. According to research conducted by Shadel et al. (2010), individuals who received the OIF training were significantly less likely to respond to a fraud appeal than those who did not receive the training.

Avoid fear. Early investment fraud prevention campaigns emphasised cautioning investors about the risks involved in investing. However, a potential drawback of warning campaigns is that they could generate fear in the intended audience. Although fear is recognized as a potent motivator, as illustrated by the scarcity tactic, it is generally believed to be ineffective in campaigns aimed at modifying behaviour (Soames Job, 1988; Kieffer and Mottola, 2017).

Avoid reactive behaviour. Retail Investors experts counselled against reacting against currently prevalent scams (OECD, 2005). While such campaigns may be effective in combating specific scams, the constant emergence of new scams means that consumers continue to be vulnerable. Furthermore, naming specific scams can inadvertently increase their success by giving them name recognition (Skurnik et al., 2005). Additionally, warning campaigns are reactive, responding to a situation that has already occurred and leaving those who have already lost money without recourse. These campaigns are generally short-term, as creating awareness may deter people from falling for a scam at the time, but unless communication is continuous, awareness fades quickly. As an alternative, general campaigns aiming at building resilience can refer people to additional, up-to-date resources that help individuals identify current scam tactics.