Pensions fraud: time to act

2018

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Pensions fraud: time to act

The role of a trustee and those who work in the pensions industry continues to evolve as fraud threats and cybercrime risks increase and the tools used become more sophisticated.

RSM's survey shows encouraging signs that the sector has started to recognise that fraud and IT systems breaches are areas of increasing risk. But there is still work to be done.

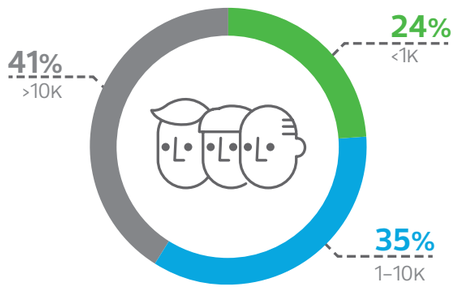
While fraud awareness is growing, the actions needed to mitigate risks are lacking. As fraudsters wake up to the value of scheme assets and member data, a strong internal control environment is a critical line of defence. Without this, scammers will always be one step ahead.

Today, pensioner existence fraud is still an ever-present threat. At the same time, the Pensions Freedoms continue to result in a marked increase in the number of withdrawals from UK schemes. But the internal controls needed to make sure money is paid to the right people or to a valid receiving scheme are not always as robust as they should be and millions of pounds continue to be lost to fraudulent transfers.

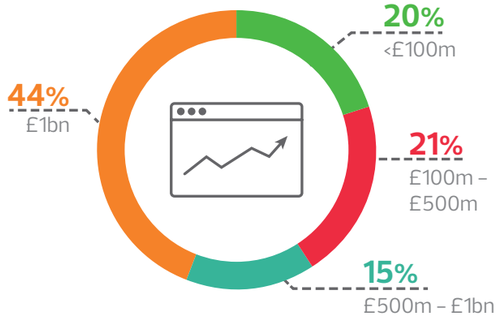
Alongside these perennial threats the risk from cybercrime is more apparent. With the impending roll out of the General Data Protection Regulation (GDPR) in May 2018, the need to protect members and their data must be prioritised. Failure to act could have devastating consequences.

Ian Bell
Head of Pensions, RSM

Total membership

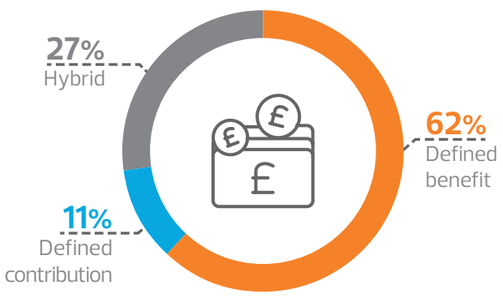


Scheme size



Scheme administration

Benefit structure



Respondent profile
We ran an online survey from October to December 2017. Here is a breakdown of the respondents' profiles.

PENSIONSAge AWARDS 2017 WINNER
PENSIONS ACCOUNTANCY FIRM OF THE YEAR

Part 1: Fraud awareness

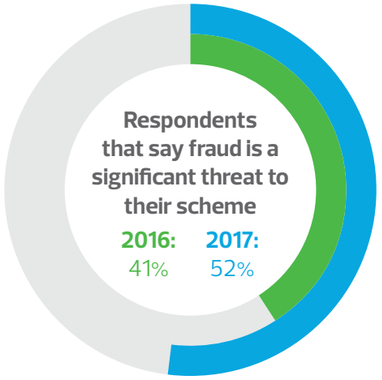
Fraud continues to create pressures across the sector, with one in six respondents reporting that they have experienced a scam in the past two years. With fraudsters often dodging detection for years, it is likely that incident rates are even higher. Unless schemes have the proper controls and reporting processes in place, many victims remain unprotected.

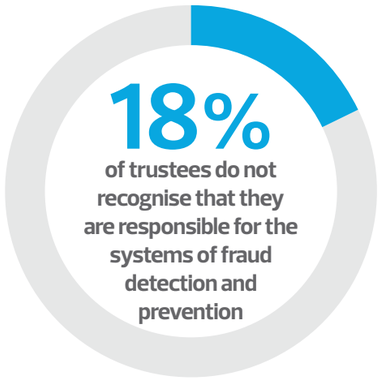
Over the past 12 months, the sector has become more alert to the risk – 52 per cent now say fraud is a significant threat to their scheme. Against this backdrop, fraud has shot up the agenda. Boards are actively considering the threat, adding fraud to their risk registers, rolling out trustee training and asking questions of their service providers.

It is good news that attitudes are changing and trustees are moving in the right direction. But there is still a long way to go before the pensions industry is as vigilant to fraud risks as it needs to be. Despite the progress made over the past year, defences must be bolstered further.

The Pensions Regulator expects schemes to test their internal controls each year. This helps to identify whether mitigation and prevention processes are still fit for purpose and will continue to protect schemes from the latest threats. Worryingly, a third of respondents are not carrying out these checks.

At the same time, there is confusion about lines of responsibility. While everyone has a role to play in the detection and prevention of fraud – pension managers, auditors, sponsoring employers and administrators – trustees remain ultimately responsible. Yet 18 per cent of trustees do not recognise this fact. The majority of those who did not recognise this responsibility were from larger schemes with more than 10,000 members.



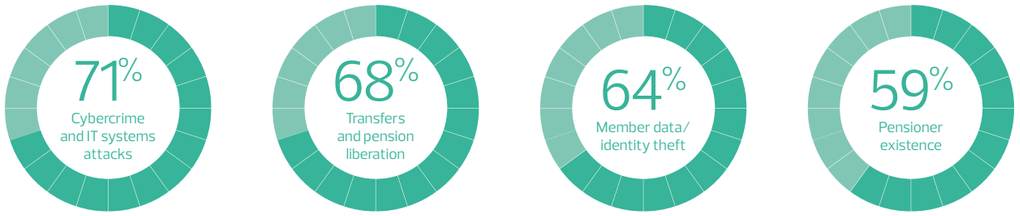


Schemes are significantly exposed where trustees do not understand their role. If a fraud event occurs, those that have failed to fulfil their duties 'are potentially liable. The repercussions – personal, professional and organisational – could be substantial.

There is little doubt that trustees' workloads are growing. With limited time, it can be tempting to focus energy and attention on funding risks and other pressing day-to-day challenges. While these activities are undoubtedly important, trustees cannot afford to overlook the need to maintain robust risk management processes. Fraud awareness, as well as detection and prevention, must become priorities in the year ahead.

Part 2: Key threats

Perceived areas of vulnerability



Top areas of fraudulent activity

1. Pensioner existence

2. Transfers and pension liberation

3. Theft of member data and internal dishonesty

This year's survey shows a marked gap between perceived areas of vulnerability and experience on the ground. Most think cybercrime and IT breaches pose the greatest threat of fraud to their scheme. Yet the reality is that perennial risks, such as pensioner existence frauds and transfers/liberation scams, are still the most commonly detected frauds.

The increasing prevalence of IT hacks, in the wider economy coupled with the impending arrival of the GDPR, has undoubtedly brought cybersecurity concerns into sharp focus. Schemes must do all they can to guard against the threat of unauthorised data access. But this activity should not jeopardise other fraud risk management action. All threats must stay on the radar.

2.1: Pensioner existence

Schemes continue to lose the fight against fraudulent pension claims. Pensioner existence frauds – those that continue to draw the benefits of deceased members – are still the top fraud event experienced across the sector.

In 2016, the Cabinet Office published statistics that showed pensioner existence scams led to an £11.4m overpayment of public sector pensions between 2014 and 2016.[1] With pensioner existence scams still so rife, it is likely that losses of this scale continue today – it will be interesting to see the results of the next NFI publication.

What can schemes do to tackle the threat of fraudulent pension payments? Existence tests, which crosscheck member details against official death register data, can go some way to help, but success is not guaranteed. Despite widespread adoption of these checks, it is clear that many fraudsters are still able to escape detection.

Schemes that use third party administrators to carry out existence checks must seek assurance about the level of testing carried out. It is critical trustees ask the right questions. What proportion of the database is crosschecked? How often are checks carried out? Is more rigorous testing in place for older pensioners or members living overseas?

Our survey reveals that many are not doing this. Just 32 per cent of respondents have asked their administrators to amend or extend their processes for pensioner existence tests. And only 24 per cent of respondents have asked their administrators to enhance their tests for members known to be living overseas. Without these improved controls, schemes will be hamstrung in their attempts to crack down on fraudulent claims.

[1] Cabinet Office. National Fraud Initiative. November 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/565216/nfi_national_report_2016.pdf

Whether through deliberate action by a fraudster or neglect by family members who have more pressing matters on their minds, benefits continue to be paid to those who are no longer entitled to them. Unfortunately, there are still some pension schemes that only perform existence checks once a year, if at all. Others do not carry out extra checks on pensioners who now live overseas. All trustees should ask themselves whether they are doing enough to protect the assets of the scheme.

Elisabeth Storey, Audit Director, RSM

2.2: Transfers and liberations

It has been three years since the Pension Freedoms were introduced, but the legislative shakeup is still creating shockwaves across the sector. With so many over-55s continuing to accelerate withdrawals, trustees have had their work cut out to separate valid claims from fraudulent ones.

The Pensions Regulator estimates that 80,000 transfers were made from DB schemes between April 2016 and March 2017.[2] Recent HMRC statistics also reveal that individuals accessed pensions with a value of £6.5 billion during 2017.[3] While the majority of these transfers will be legitimate, many others will be scams – figures show fraudsters secured nearly £5m from pension pots in the first five months of 2017 alone.[4]

Trustees are in a difficult position. We are aware that the Pensions Ombudsman has investigated instances where trustees have refused suspicious requests as well as those where trustees have approved transfers that later turned out to be scams. Schemes are increasingly relying on a growing database of known fraudsters to reach more confident decisions, but this approach will not catch all fraudulent transfers.

Importantly, trustees and their administrators need to be aware that they can, and should, distinguish between statutory and non-statutory transfers. However, schemes do not routinely distinguish between the two, nor do administrators always recognise the important difference.

What are statutory transfers?
Under statutory transfer rules, members have certain rights. This means trustees can warn members if they are suspicious about a transfer request. But if basic checks are passed, the member can insist that the transfer is made, and ultimately the trustees will have to release the funds.

What are non-statutory transfers?
These transfers are typically discretionary. When making these transfers, trustees must make sure they protect all scheme members, not just those who ask for a transfer (and might make a claim against the trustees if things don't turn out as they expect). This includes current and future members who may be affected if a fraud event causes significant costs to the employer. Trustees must ensure that there is a written record as to how discretion has been exercised in the case of non-statutory transfers, and may also wish to consider obtaining a signed discharge from the member to protect against any potential future claims.

Scamming is likely to be grossly underestimated by official reports and its full scale may not be apparent for many years. For the victims, the loss of a lifetime's saving can be devastating. It is a problem that warrants urgent action.

Work and Pensions Committee, December 2017

Trustees must understand their responsibilities in this area and, most importantly, keep a written record to show they have exercised discretion themselves or have delegated authority to someone else who, in turn has, kept a written record. Failure to do this could provide grounds for a claim as it could be seen as a fundamental breach of trust.

There has been significant activity within the pensions industry to educate members about transfers out, particularly with the release of TPR's scorpion campaign. But it is also critical that trustees treat statutory and non-statutory transfers differently – this will be a key step to combat any potential claims against them.

In February 2018, the government reinforced its commitment to a cold calling ban, with a proposed timetable to achieve this by June 2018. Increased public awareness of the issue will clearly be one more weapon in the armoury to prevent the looting of members' pension pots. But with the government likely unable to stop calls from outside the UK, the ban will not stamp out all fraudulent transfers and liberation scams. The sector must keep a careful watch on the proposals that come forward. If a cold calling ban is not introduced at the earliest opportunity, members' pension pots will unfortunately remain a lucrative option for con artists at home and abroad.

[2] The Pensions Regulator. Number of people who transferred out of their DB schemes last year. FOI response: FOI 2017-05-22. May 2017
http://www.thepensionsregulator.gov.uk/foi/number-of-people-who-transferred-out-of-their-db-schemes-last-year-may-2017.aspx
[3] HM Revenue and Customs. Flexible Payments from Pensions. Official statistics. January 2018.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675350/Pensions_Flexibility_Jan_2018.pdf
[4] Gov.uk. Tough new measures to protect savers from pension scams. August 2017.
https://www.gov.uk/government/news/tough-new-measures-to-protect-savers-from-pension-scams

2.3: Cybercrime

As cybercrime risks are increasing dramatically, complacency leaves schemes exposed.

89%
say cybercrime is a significant threat to the industry

72%
say cybercrime is a significant threat to their scheme

88%
say cybersecurity is on the risk register

48%
have received formal cyber risk training in the last year

21%
have asked their administrator to review or enhance identity theft controls

20%
have a 24-hour incident response plan to react to a breach

The 2017 WannaCry attack on the NHS was a clear signal that it is not just global corporates that are targets. Organisations of all sizes and purpose are at risk from the growing threat.

Cyberattacks do not just disrupt day-to-day operations. They also dent reputations and erode trust. Pension schemes hold a huge amount of sensitive data, which makes them an attractive target for cyber criminals. Trustees must do all they can to meet members' expectations that their data will be kept safe.

However, our survey shows many have failed to adopt basic security measures. While most schemes have put cybersecurity on their risk registers, many have stopped short of other key prevention and mitigation actions. In a climate where cybercrime risks are increasing dramatically, complacency leaves schemes significantly exposed.

Critically, less than half of trustees have received formal cyber risk training in the past year. If boards are to effectively guard against the latest threats, they must be up to speed about which IT resources will help them do this. With cybercrime threats evolving rapidly, training must not be seen as a one-off event.

Equally, trustees must ensure their administrators have the right safeguards in place to protect member data. Yet we know that only 57 per cent have asked their service providers for details of their cyber risk policies. And only 21 per cent have asked their administrator to review or enhance their controls against identity theft.

It is critical that supplier contracts specify which cybersecurity measures are in place, as well as how and when attacks should be reported to the trustees. This will ensure trustees get the assurance they need that their scheme is protected.

The arrival of the GDPR on 25 May 2018 will significantly increase the financial ramifications if a data breach occurs. Under the new data protection rules, schemes could face fines of up to €20m or 4 per cent of global turnover, whichever is higher. It is not yet clear how this will be applied to pension schemes. The costs of doing nothing should not be underestimated.

Worryingly, many are struggling to prepare for the new rules – 13 per cent say they are yet to take any action to get ready for GDPR. Key problem areas include reviewing all contracts with data processors, complying with individuals' rights to personal data deletion and dealing with tightening consent requirements.

Beyond this, the GDPR will mean organisations must report data breaches to the relevant authority, as well as the affected individuals, within 72 hours. With just 20 per cent of schemes having a 24-hour response plan in place, it is likely that many will struggle to meet this new legislative requirement if the worst happens.

With less than three months to go before the new rules come into effect, schemes must work to ensure their internal processes are fit for purpose. Trustees must be equipped to report and manage communications with affected individuals quickly and accurately. Those that don't must be ready to answer tough questions if things go wrong.

Part 3: Critical actions in the next 12 months

Put fraud on the agenda
The board must discuss fraud and cyber risks at least annually and put these issues on the risk register. The right tone at the top will ensure that risk management is not overlooked and the right resources are put behind mitigating threats.

- Are fraud and cybersecurity risks included in your trustees' meeting agenda at least once a year?
- Are fraud and cybersecurity risks on your risk register?
- Have you allocated enough resource to mitigate the risks of fraud and cybersecurity?
- Do you have a robust fraud response plan that supports a 'no tolerance' approach? Does it incorporate the anti-bribery and anti-corruption requirements of the Bribery Act 2010?

Test your internal controls
The right controls can last a lifetime. But it is important that you regularly check they are still fit for purpose against the latest threats. The Pensions Regulator is clear that this should be done at least annually.

- Are you satisfied that the trustee board has enough knowledge of the internal control environment and the oversight role it must play?
- Has the trustee board considered nominating a trustee with the right skills to obtain and review the internal control reports prepared for service providers?
- Have the internal controls recorded in the risk register been formally tested in the last 12 months, in compliance with Code of Practice number 9?

Develop a cyber strategy
A cyber strategy should set out your approach to dealing with an IT systems breach. It must be approved by the board, and should be underpinned by a formal assessment of cyber risks.

- Have the trustees carried out a formal assessment of the cyber risks facing the pension scheme?
- Does it cover the whole of your cyber footprint where an IT systems breach could occur?
- Does the trustee board have a cyber strategy that sets out the response to an IT systems breach?
- Has the cyber strategy been formally considered and approved by the board? Does it cover all areas where an IT systems breach could occur?

Embed a 24-hour breach response plan
Under the new GDPR, schemes will have 72 hours to inform the Information Commissioner and their members about a data breach. Those that prepare will stand the best chance of avoiding financial and reputational damage if things go wrong.

- Do you have formal, written agreements with all your advisers that set out when they must report data breaches to the trustee board?
- Do you have a 24-hour breach response plan that sets out who is responsible for key actions (and a deputy in case of absence) if a data breach occurs?
- Do you have the processes in place to deal with and mitigate the reputational damage, for example to the sponsoring employer, if a significant data breach occurs?

Get assurance from third party suppliers
It is critical you ask the right questions of your administrators and third-party suppliers. Assumptions can leave your scheme and members significantly exposed. Make sure their actions match your expectations.

- Do you know the circumstances in which the administrator would report a data breach to you? Would it alert you to any breach or only those that directly affect your scheme?
- If a data breach occurs, are protocols in place to deal with the impact — for example, recorded messages at the administrator to deal with the extra volume of calls from concerned members?
- In the case of a DC or hybrid arrangement, does the incident response plan make clear when an investment transaction blackout is needed to mitigate fraudulent access to member pots?

rsmuk.com