PENSIONS FRAUD: SLEEPWALKING INTO A CRISIS

January 2017
Today, the pensions sector faces more challenges than ever before. Continued economic and political uncertainty over the past 12 months has amplified funding risks and created fresh concerns over sponsors’ long-term durability. In an already difficult operating environment, ever-more sophisticated fraud events present trustees with yet more challenges.

Since we published our first fraud risk report in 2011, the frequency and scope of scams has increased dramatically. But the threat shows no signs of abating in the year ahead. Alongside perennial challenges, such as pensioner existence fraud, cybercrime has emerged as a major new risk area. Online fraudsters are proving indiscriminate in their approach—no scheme is immune.

Over the past year, legislation has also magnified challenges. Our prediction that the Pension Freedoms introduced in April 2015 would create a scammers charter has unfortunately rung true, with respondents highlighting a significant increase in suspicious member transfer requests since the rules came into effect.

The government’s recent commitment to tackle these scams should be welcomed, but it must not be considered a silver bullet. Fraud will remain a major risk to pension schemes throughout 2017 and beyond, with new General Data Protection Regulation (GDPR) rules due to come into force in 2018 adding further pressure. Under the planned changes, those responsible for data breaches could incur fines of up to €20m. Whether fines are levied on schemes, trustees or third party administrators will depend on individual scheme arrangements and the assurances in place, but the new rules clearly demonstrate that data protection is being taken far more seriously.

Despite the growing threat, there continues to be a worrying degree of complacency across the sector. Few have put in place the necessary controls to properly identify and manage risks. As fraud becomes increasingly common and penalties grow markedly, many are in danger of sleepwalking into a crisis. The costs of doing nothing should not be underestimated.

Ian Bell
Head of pensions, RSM.
The online survey ran between October and November 2016.
Fraud has the potential to have a devastating impact on pension schemes. The loss of assets, reputational damage and fines that could result from fraud may, at best, be a major distraction for trustees. At worst, they will be a real threat to members’ benefits. While the right insurance plan can help when things go wrong, it is not a guarantee. Trustees and their administrators must remain alert to the risk.

Our survey revealed a significant increase in scam activity over the past 12 months. Paying benefits to deceased pensioners continues to be the top threat, but incidents of liberation fraud and cybercrime have also grown significantly over the last year.
Of those that have experienced fraud:

- **51%** were victims in the last **12 months**
- **17%** were scammed **12 to 24 months ago**
- **32%** were scammed **more than 24 months ago**

Despite the growing risk, a worrying proportion of respondents continue to see fraud as a low-level threat. For many, funding concerns and sponsor viability will be considered more pressing challenges. While these are critical issues to contend with, they must not come at the expense of robust fraud prevention and mitigation controls.

A lack of fraud awareness is likely a key driver of the widespread complacency. Trustees are ultimately responsible for the overarching strategies and structures that inform day-to-day fraud controls. The tone they set at the top is critical, but our survey shows that nearly a quarter are unaware of their responsibilities. Education must be a key priority in the year ahead.

Looking forward, changing pension benefit structures are likely to intensify risks. Defined contribution schemes have become ever-more popular, with employers in recent years giving members greater autonomy over how funds are invested. But allowing individuals to access sensitive pension information online could leave them vulnerable to cybercriminals, and increase their exposure to potential data losses.

If handled incorrectly, the outsourcing of scheme administration to third parties could create further challenges. Working with external providers does not assuage trustees of their personal liability in the event of fraudulent activity — instead, trustees must assure themselves that their partners have the right controls in place to identify and mitigate risks. Ongoing monitoring remains essential.
Part two: Risk areas

2.1 PENSIONER EXISTENCE REMAINS A MAJOR THREAT

Continuing to pay benefits to relatives of deceased pensioners, referred to here as pensioner existence fraud, has long been a major challenge for the sector, but the threat shows no signs of abating. Recent figures from the National Fraud Initiative (published in November 2016 by the Cabinet Office) show that failure to report the death of pensioners resulted in an £11.4m overpayment of public sector pensions between April 2014 and March 2016. By identifying the problem and ceasing further payments, a potential future loss of more than £85m has been prevented.

In our survey, pensioner existence fraud continues to be the top fraud event experienced by respondents. The growing ability and willingness of over-55s to retire overseas is a key driver. Once a member leaves the UK it becomes more challenging for schemes and their administrators to keep up with any changes to circumstances. While families have a responsibility to report a pensioner death, experience shows this is not always carried out.

As schemes mature and more members relocate overseas, it is more important than ever that trustees and pension providers keep pensioner existence fraud on their radar. While it is easier to track UK-based pensioners, trustees and their administrators must remember that domestic fraud still occurs. Member databases should be cross-checked with official death records held by the government at least annually. Additional testing should also be considered for older demographics.

Today, many schemes outsource data matching activity to external providers. To mitigate risks, trustees must be assured about the level of testing that is carried out: as databases grow in complexity, administrators do not always cross-check the entire member list. With sampling becoming increasingly common, simply asking an administrator whether it carries out data matches is no longer enough.

In order to safeguard the scheme’s assets and protect the interests of the entire member population, trustees must challenge the administrator to ensure rigorous testing is performed.

Of those that have experienced fraud:

- 39% say it occurred in pensioner existence

31% say pensioner existence is most vulnerable to fraud.
Simply asking an administrator whether it carries out data matches is no longer enough.
2.2 MEMBER TRANSFERS AND LIBERATION FRAUD INCREASES

The introduction of Pension Freedoms in April 2015, arguably the biggest shake-up to pensions legislation in recent years, has so far proved popular with over-55s. Many have taken advantage of new opportunities to accelerate fund withdrawals: HMRC figures reveal that 232,000 people accessed £4.35bn from their pension pots in the first year alone, with a further 243,000 retrieving £3.3bn in the first two quarters of 2016¹.

Of those that have experienced fraud:

- 56% say suspicious requests have increased since April 2015.
- 29% say transfers/pensions liberation is most vulnerable to fraud.
- 58% have had to consider suspicious member transfer requests.

The new rules have created challenges for the sector. Since April 2015, schemes and administrators have experienced a worrying increase in suspicious member transfer requests, while cases of over-55s receiving unexpected tax bills for early withdrawals have regularly hit headlines. Although awareness has gradually increased, fraudsters continue to dupe more vulnerable members.

To date, the sector’s hands have been tied. Legally, trustees cannot block transfer requests. Even if fraudulent activity is suspected, their only option is to ensure members have the necessary guidance and information to reach a confident and appropriate decision.

However, figures reported in the recent Autumn Statement show almost 11 million pensioners are targeted annually by cold callers, with savers reporting estimated losses of almost £19m to pensions scams between April 2015 and March 2016. There will undoubtedly be more cases that have gone unreported. With many schemes unable to prevent their members from making the wrong decision, sector-wide frustration has continued to reign.

Looking forward, there are signs that the sector will be better placed to tackle the challenge head-on. The government has launched a consultation on plans to ban cold callers that target members and clarify the law so schemes and administrators are able to block member transfer requests if certain criteria are met.

While the proposed changes are to be welcomed, they must not be considered a silver bullet. It is difficult to see, for example, how the planned safeguards will protect the public from overseas callers that fall outside UK jurisdiction. Member transfer scams will not disappear overnight and could even increase in the short term if fraudsters sense that their window of opportunity is closing. Trustees and administrators must remain vigilant.
2.3 EMERGING THREATS

Cybercrime is a growing risk

In a digital world, data has become a commodity to be bought, sold and traded online. As personal information becomes more valuable, hackers are increasingly exploiting vulnerabilities in organisations’ IT infrastructure. Cybercrime has grown from a rare phenomenon just a few years ago to one of the biggest threats facing the modern world.

For hackers, schemes and their administrators hold a treasure trove of information that can facilitate identity thefts or be used to divert pension payments. Bank account details, addresses, dates of birth and National Insurance numbers are hugely valuable to cybercriminals. Raids on the sector will undoubtedly increase.

Today, the tools needed to identify weaknesses in an IT system are readily accessible, allowing hackers to breach systems with relative ease. Across the sector, however, there is widespread complacency – few have the proper controls to effectively assess and manage cyber risks. Without these assurances, it is likely that many breaches will have gone undetected.

Against this backdrop, schemes should enhance their identity checks on members to ensure that they are dealing with and paying benefits to the correct claimant. Our survey showed that many had still not considered this area.

Do your internal controls cover cyber security?

YES 52%

NO 29%

UNSURE 19%

Have your processes been amended to guard against identity theft?

YES 58%

NO 21%

UNSURE 21%
How do cybercriminals attack?

**Ransomware attacks**
A hacker gains access to a system and takes it over. It holds the organisation to ransom by blocking system access until a substantial payment is made.

**Insider attacks**
Employees download sensitive or confidential data and sell it on.

**Phishing activity**
Multiple individuals are targeted by a single scam. Typically, a blanket email is sent in the hope that some will reply with sensitive information, transfer funds or open rogue links or attachments.

**Whaling attacks**
A small group of individuals with significant data access are targeted. Typically, a hacker poses as a senior official and requests personal information, bank detail changes or a large funds transfer.

As the public becomes increasingly sensitive to how companies use their personal data, it is more important than ever that the sector protects member information. Forthcoming legislative changes will add further pressure: GDPR rules are expected to come into force in 2018 that could lead to fines of up to €20m if data is lost, compromised, handled incorrectly or stolen and adequate checks and procedures are not in place to protect it.

Trustees have a clear responsibility to protect members' data from cybercriminals. Even though they are not directly involved in the day-to-day handling of information, they are defined as data controllers under the Data Protection Act. As such, they could be exposed to public and legal scrutiny if things go wrong. Indemnity insurance must not be relied upon as a form of defence; it rarely covers cyber breaches.

To avoid individual liability claims, trustees must put in place robust strategies and systems to protect member data, and hold sponsoring employers and service providers to account. With human error the weakest link in most cybercrime cases, effective prevention and mitigation measures must focus as much on behavioural controls as infrastructure vulnerabilities.
Preventing cybercrime

Key questions trustees must ask themselves, their sponsoring employer and their administrators:

- Is cyber security on our risk register and in what guise?
- Has the risk been appropriately assessed and has it been rigorously tested?
- Do trustees use portable devices to access board papers?
- Do trustees use home computers? How secure are they?
- Have trustees been given sufficient training in order to understand and assess risks?
- Does the administrator have an internal controls report and does it sufficiently detail IT risk?
- If a breach occurs, would the administrator have to tell the trustees? What is covered in the contractual arrangements and when were they last reviewed?
- What controls are in place to check a member’s identity when benefits are being claimed?
Part three: Mitigating risks

3.1 PREVENTING FRAUD

Fraud prevention starts at the top: trustees are ultimately responsible for developing the counter-fraud strategies and controls that inform the day-to-day activities of pension managers, administrators and service providers. Without a robust framework in place, risks cannot be properly understood or properly mitigated.

But how well equipped are trustees to undertake this role? With our survey revealing a worrying level of complacency, training must become a key priority in the year ahead. If trustees are to make confident judgements about a scheme’s vulnerability and whether controls are fit for purpose, they must first understand common risk areas, as well as evolving threats.

Trustee boards should actively consider fraud risk on at least an annual basis. An up-to-date risk register is an important output of these discussions. It should outline the potential risks faced by the scheme as well as the controls that have been put in place to mitigate them, and whether these are working effectively. To remain fit for purpose, it must be reviewed at least once a year. Elements that cover high-impact or high-likelihood risks should be reviewed more frequently.

An up-to-date risk register can help inform a robust fraud risk policy by ensuring control measures are appropriate and proportionate. The risk register should also clearly allocate responsibility to ensure key individuals understand their obligations and how and when to take action.

Once fraud prevention controls have been introduced, they must be regularly tested. New threats are continually emerging and scam techniques constantly evolving. Our survey shows that the sector is falling short of the need to check controls at least annually or to respond to new frauds when they arise. Without this, many will have an inaccurate view of their scheme’s vulnerability.

Action taken in last 12 months to mitigate fraud risk:

- On the risk register 36%
- We improved internal controls 24%
- Trustee training 22%
- Asked service provider to detail its fraud risk policy 14%
- We did nothing 4%
Has the trustee board actively considered fraud risk?

YES, IN THE LAST 12 MONTHS: 68%

NO: 14%

YES, BUT NOT RECENTLY: 18%

Today, a lack of awareness or human error is the weakest link in many fraud cases, particularly with newly emerging threats like cybercrime. Experience shows that the wrong click of a button can expose organisations to severely damaging and costly fraud events. Education has a key role to play.

Employees must be trained to recognise externally initiated fraud risks, such as suspicious email activity. But staff education must also extend to the warning signs of internally initiated fraud. While less common, the risk that staff members could be implicit in major fraud activity must not be overlooked.
3.2 CYBER SECURITY: WHEN THINGS GO WRONG

Do not have a formal fraud response policy

Took no action after experiencing fraud

75% 11%

Once significant cyber security breaches have been detected, trustees and pension providers have a 24-hour window to successfully minimise impacts. Every hour counts: any delays to remedial action or errors in internal and external communications have the potential to magnify challenges and reduce the chance of a successful outcome.

Typically, the fraud event itself has little bearing on the long-term impacts on the scheme. Instead, the consequences are largely dictated by the actions of trustees, administrators, managers and providers in the months before the fraud takes place. In most cases, pre-adopted strategies and training are the difference between damage limitation and a crisis.

A formal fraud response plan should be in place to provide a framework for effective and swift action. It should allocate clear roles of responsibility and set out a policy for how fraudulent events will be handled internally and externally. Who will be told, and how? Will the press be informed? Has the appointed spokesperson received appropriate crisis training to effectively handle public scrutiny or backlash?

In the wake of a cyber fraud event, the worse thing a scheme can do is nothing. Trustees must regroup and consider how future attacks can be prevented. Controls will likely need to be updated and, in some cases, the service provider changed. Many will be tempted to make a quick adviser appointment to minimise disruption, but a rushed selection process will likely cause further problems.
Is your scheme at risk?
Fraud warning signs

• Internal or external audit have raised concerns about the quality of financial or management reporting.

• Low-quality information disclosure.

• Out-dated and legacy systems are run in isolation and not subject to governance scrutiny.

• Inadequate segregation between risk takers and record makers.

• Frequent changes of adviser.

• Lack of policies on values and behavioural standards and no published code of conduct.

• Separate office locations that are not accessible to members of staff in accounting, compliance or governance functions.

• No enforcement of holidays for key administration staff.
What should trustees be doing now?

- Ensure that fraud is on the trustee board agenda and consider if there are any training needs.
- Update the risk register and make sure measures are in place to regularly test internal controls.
- Define a fraud risk policy and a fraud response plan.
- Identify any areas of concern and action required.
The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm, each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Consulting LLP, RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.

© 2017 RSM UK Group LLP, all rights reserved. 4003. Expires 1217