The Pensions Regulator
Making workplace pensions work

Napier House
Trafalgar Place
Brighton
BN1 4DW

0345 600 0707

www.tpr.gov.uk
www.trusteetoolkit.com

mpcorrespondence@tpr.gov.uk

12 May 2023

Dear Ms Kitchen

You will be aware of the cyber incident that has affected Capita. TPR is working closely with Capita, other regulators and trustees as the situation evolves.

Administrators play a key role in the safety and security of pension scheme members' data, and we are writing to you as a leading administrator to urge you to ensure that you have robust cyber security controls in place.

Prevention

The cyber threat is constantly evolving. This means that your prevention mechanisms should be equally dynamic:

- Make sure that you have technical controls in place (eg firewalls, anti-virus and anti-malware) and keep these up to date.
- Use penetration testing to identify potential weaknesses in your systems
- Provide regular training to your staff and consider testing levels of awareness eg through phishing tests
- Keep informed of developments in cyber threats through the National Cyber Security Centre's (NCSC) advisories or by joining their Cyber Security Information Sharing Partnership

Detection

Early detection of cyber incidents is critical to minimising the risk to members' data and scheme assets:

- Monitor system activity so you know what normal looks like, and can therefore identify abnormal activity more easily
- Monitor endpoints (eg mobile phones, laptops) for suspicious behaviour or activity
- Log digital processing activity. An automatic audit trail of operations is useful as a source of investigation in case of a cyber incident

Response

Cyber incidents are inevitable so you must make sure that you are prepared to respond when one arises, to minimise the impact on your organisation and on scheme members:

- Have a robust cyber incident response plan which sets out:
  - Clear roles and responsibilities
  - Backup and recovery procedures for scheme records
  - Prioritised scheme services covering at a minimum, pensioner payments, retirement processing and bereavement services
  - Internal and external communication plans
  - Reporting mechanisms to trustees, regulators and members.
- Have procedures in place for shutting down elements of your infrastructure to prevent malware and viruses from spreading
- Know what data you hold and where it is held, so that you can swiftly determine which data has been compromised and who might be affected
- Make sure you have access to an NCSC approved incident response provider to support you in the event of a breach
- Be aware of, and comply with your duties to report breaches to us and the Information Commissioner
- Consider what support services you can offer members in the event of a data breach
- Only bring systems and data back online when you are confident that they are secure
- Review systems, operations and approval processes that may have been compromised by loss of data or material

The cyber threat is constantly evolving, and we must work together to protect savers – we urge you to contact us in the event of an incident.

Kind regards,

Nicola Parish
Executive Director of Frontline Regulation