The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

Swinburne Snowball and Jackson
2 Edith Street
Consett
County Durham
DH8 5DW

By email only to: [redacted]

9 August 2023

Dear [redacted]

Case Reference Number INV/0160/2021

I write to inform you that the ICO has now completed its investigation into the personal data breach reported by Swinburne Snowball and Jackson ('SSJ').

In summary, it is our understanding that:

- The threat actor compromised an employee Outlook email account via a spear phishing attack and interfered with payments to beneficiaries of a probate matter. Following contact from your bank on 14 January 2021, four fraudulent payments totalling [redacted] were identified.
- An independent cyber security firm identified the first malicious sign-in in occurred on 11 January 2021 until the account password was changed on 15 January 2021.
- SSJ reported the matter to its personal data insurers and the Solicitors Regulation Authority ('SRA') on 15 January 2021. SSJ later notified the ICO on 26 January 2021, 12 days after which SSJ confirmed it had a reasonable degree of certainty the security incident had led to a personal data breach.

Our consideration of this case

This case has been considered under the UK GDPR due to the nature of the processing involved, and that the incident occurred on or after 25 May 2018.

For more information about our powers under the data protection legislation please see the attached leaflet.

We have investigated whether SSJ has complied with the requirements of data protection legislation. During the course of the investigation, we have noted that:

- The personal data breach involved a large sum of money relating to a probate matter and resulted in a delay in the payments of the legacies to the beneficiaries by 21 days.
- SSJ did not have a suitable contract in place with its IT provider that defined security responsibilities or the level of security required. As a result, SSJ was unable to demonstrate if or how preventative, detective or auditing measures were implemented with regards to its email accounts.
- SSJ further did not have multi-factor authentication ('MFA') in place for the affected email account and advised the ICO it had not been suggested by its IT contractors beforehand. Extensive guidance was available via the National Cyber Security Centre ('NCSC'), Solicitors Regulation Authority and the Law Society, which promoted the use of strong or multi-factor authentication.[1] Additional means of authentication serve to make unauthorised access more difficult and help to protect particularly sensitive or private personal data.
- Given the nature of SSJ's business and the scope of information it processes and has access to, including financial transactions, it would be anticipated that appropriate security measures, such as MFA, or formal accreditations, such as the NCSC's Cyber Essentials, would be in place to protect this data. Post incident, SSJ has indicated it has implemented MFA.
- SSJ started but did not complete accreditation to the NCSC's Cyber Essentials, which is a government supported scheme designed to help businesses protect against basic cyber-attacks through self-assessment. Lexcel is the Law Society's legal practice quality mark

[1] Cyber-Essentials-Requirements-for-IT-infrastructure-2-2.pdf (ncsc.gov.uk), SRA | Technology and legal services | Solicitors Regulation Authority, Cybersecurity when working from home | The Law Society

and the March 2018 Lexcel Standards state that legal practices should be accredited against Cyber Essentials.

In view of the above, the ICO has determined that SSJ failed to comply with Article 5(1)(f), which requires personal data is processed securely, and Article 32(1)(b), which requires appropriate measures are in place to ensure a level of security appropriate to the risk and ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

We have also considered the remedial steps taken by SSJ in light of this incident, including SSJ's prompt notification to affected individuals. We further note SSJ commissioned a third party cyber security firm to investigate and report on this incident and liaised with its IT consultants for advice and assistance with remedial measures. We understand that all clients were repaid in full on 3 February 2021.

Based on the information provided and having taken into consideration your representations, the Commissioner has decided to issue SSJ with a reprimand in accordance with Article 58 of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the GDPR:

- Processing personal data in non-compliance of the requirements set out in Articles 5(1)(f) and 32(1)(b).

Recommendations

Accountability is one of the key data protection principles and makes a controller responsible for complying with the GDPR. A controller should therefore implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the GDPR. The ICO expects all organisations to demonstrate how they take personal data obligations seriously and process personal data in a manner that ensures appropriate security.

In line with Article 5(1)(f) and Article 32(1)(b) of the UK GDPR, The Commissioner routinely recommends the following steps concerning governance, identity and access controls, technical control selection, staff training and awareness and supply chain security:

1. Ensure senior management are accountable for the security of its personal data processing, and information security is regularly assessed in line with known threats.
2. Perform regular reviews of user privileges and enable strong authentication for any remote access into the network or internet facing services, such as cloud services. The NCSC's introduction to identity and access management guidance includes useful advice on privileged user management.
3. Consider the creation of a separate and formal password policy which directs users to appropriate levels of access controls. The NCSC's Password administrator for system owners guidance will provide support in implementing appropriate password strategies.
4. Implement measures to reduce the risk of social engineering attacks, such as anti-spoofing measures. The NCSC's Phishing Attacks: Defending your organisation guidance will provide support in implementing controls to prevent phishing attacks.
5. Deliver data protection training, with reference to cyber security, to all employees on a regular basis and evaluate the methods of control, delivery and monitoring of such training. Also regularly raise awareness of data protection, information governance and associated policies and procedures.
6. Determine and communicate security requirements to a supplier and formalise responsibilities within a contract. As part of this, establish how to seek assurances a supplier has implemented appropriate levels of security. The NCSC supply chain security guidance provides practical examples of how to manage security within a supply chain.
7. Conduct regular assessments of security controls to ensure they are achieving their intended outcomes.

It is important to note the above measures are suggestions and have been designed to support organisations in improving their security controls and overall protection against cyber-attacks; it is not a

regulatory requirement for SSJ to implement these recommendations. However, if further information relating to this matter comes to light, or if any further incidents or complaints are reported to us, further regulatory action may be considered.

The requirements of the UK GDPR

The UK GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

In the event of a personal data breach there is a requirement under Article 33 to notify the Information Commissioner's Office within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

Further guidance is also available on our website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

In this instance, we understand from SSJ's breach report that SSJ was initially unaware of the 72 hour deadline and focused primarily on identifying and containing the damage caused by the breach. SSJ further explained it was a small practice and had taken action to report to the SRA and insurers within 24 hours.

However, in line with Article 33, if a reportable personal data breach occurs, it must be reported to the competent supervisory authority (the Information Commissioner) without undue delay and no later than 72 hours of becoming aware of it. We would also like to stress that in instances where all of the information regarding a breach cannot be initially provided, Article 33(4) of the GDPR allows a data controller to report the breach and provide information in phases.

We are concerned to note that SSJ were not immediately aware of the reporting requirements under the GDPR. SSJ should therefore ensure all staff are appropriately trained in this area, especially those responsible for overseeing your organisation's data protection obligations.

Further information about overall compliance with the data protection legislation can also be found on our website: https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

We publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online here: https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely,

[redacted]
Lead Technical Investigations Officer
Information Commissioner's Office
[redacted]

Information Commissioner's Office

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice