Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Chartered Institute for Securities & Investment
20 Fenchurch Street
London
EC3M 3BY

By email only to: [redacted]

21 February 2023

Dear [redacted]

**Case Reference Number INV/0158/2020**

I write to inform you that the Information Commissioner's Office ('ICO') has now completed its investigation into the personal data breach reported by the Chartered Institute for Securities & Investment ('CISI') on 16 April 2020.

The case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

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

- ICO Enforcement Powers Leaflet – GDPR and DPA 2018

**Case Summary**

It is my understanding that on 17 February 2020, an unauthorised third party exploited a known vulnerability in the Sitefinity software to leverage a bruteforce attack to upload a malicious code to CISI's website checkout page. The code captured payment details of an estimated 3,883 UK Data Subjects, as well as other personal data including names and email addresses.

CISI instructed a third party to conduct a forensic investigation which found that CISI were running unsupported software which had a number of vulnerabilities, one of which was a critical vulnerability for which a security patch had been available since 2017. CISI also advised that no penetration tests had been conducted prior to the incident, and that 654 Data Subjects had reported fraudulent activities on the payment cards affected by the incident.

It is also my understanding that CISI may have missed opportunities to identify the data breach earlier, as a number of individuals had reported card fraud prior to a group notification 14 April 2020, at which point CISI conducted a full investigation.

## Our consideration of this case

The ICO has investigated whether CISI has complied with the requirements of the data protection legislation.

After careful consideration and based on the information obtained during the investigation, we intend to issue CISI with a reprimand in accordance with Article 58 (2) (b) of the GDPR for the reasons set out in this letter.

In the course of our investigation we have noted that CISI notified affected Data Subjects and offered access to credit monitoring. CISI also offered financial compensation to Data Subjects who expressed severe detriment, and covered expenses for items such as new bank cards or banks not refunding costs incurred.

We have also considered and welcome the remedial steps taken by CISI in the light of this incident. In particular, CISI:

- Installed additional security measures in the form of a web application firewall
- Updating impacted software to the latest version

## The proposed reprimand

We have provisionally decided to issue a reprimand to CISI in respect of the following alleged infringements of the UK GDPR:

- Article 32 (1) which states taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

- Article 32 (1) (b) which states that a Data Controller should have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- Article 32 (1) (d) which states that a Data Controller should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In particular, we have provisionally found that:

- CISI did not implement appropriate organisational measures to ensure their systems were secure. CISI did not implement timely security upgrades to the website, which itself had reached the end of enterprise support at the time of the incident. NCSC guidance highlights the importance of an effective vulnerability management process.[1]

- CISI were not conducting regular security testing prior to the incident. No penetration testing or web application scanning had been conducted. NCSC guidance sets out the need to conduct regular scanning, and identifies the different scans available to businesses.[2]

In conclusion, we have provisionally decided to issue a reprimand to CISI in relation to the alleged infringements of Article 32 of the UK GDPR.

**Further Action Recommended**

The Commissioner recommends that the Chartered Institute for Securities & Investment should take steps to ensure it is compliant with UK GDPR. The information above details the compliance issues relevant to this investigation.

With particular reference to Article 32 of the UK GDPR, the following steps are recommended:

- Implement a testing procedure which sets out the timings and nature of testing to be conducted.
- Implement a patching policy to ensure that vulnerabilities are identified and managed accordingly.
- Identify who is responsible for managing the patching policy, ensuring responsible staff are aware of their obligations.

The guidance provided in this reprimand should be closely considered by the Chartered Institute for Securities & Investment.

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

[1] NCSC Vulnerability Management – NCSC.GOV.UK
[2] Vulnerability Scanning Tools and Services – NCSC.GOV.UK

Further information about compliance with the data protection legislation can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

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

We look forward to hearing from you

Yours sincerely

[redacted]

[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

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