Upholding information rights

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

Gain Capital UK Limited
Devon House,
58 St Katharine's Way,
London, United Kingdom,
E1W 1JP,

[redacted]

10 March 2023

Dear [redacted]

Case Reference Number INV/0093/2020

I write to inform you that the Information Commissioner's Office ('ICO') has now completed its investigation into the personal data breach reported by Gain Capital UK Limited ('GCUK') on 20 April 2020.

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

Case Summary

It is my understanding that on 14 April 2020, an unauthorised third party leveraged an unpatched SiteCore vulnerability to gain access to GCUK's systems and exfiltrate 17.92 GB of data to an external IP address. An investigation by GCUK was unable to determine the specific vulnerability exploited by the third party, but two vulnerabilities were identified as contributing to the incident. GCUK confirmed that a total of 72,361 UK Data Subjects were affected by the incident, with bank account numbers and sort codes, as well as names and email addresses being impacted.

Our consideration of this case

I have investigated whether GCUK has complied with the requirements of data protection legislation.

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

- ICO Enforcement Powers Leaflet – GDPR and DPA 2018

My investigation has found the following issues in relation to the security requirements of the GDPR:

- GCUK did not have a patch management programme in place at the time of the incident. ICO guidance recommends implementing programmes which ensure an organisation's approach to patch management.[1]

- [redacted]

After careful consideration and based on the information provided we have decided to issue GCUK with a reprimand in accordance with Article 58 (2) (b) of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the 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 the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

GCUK advised the ICO that with regards to the vulnerabilities, they were not notified by the third party with whom they had a support contract in place. However, the contract in question stipulated that the installation of security patches and upgrades was the responsibility of GCUK. GCUK were not applying security patches to their systems, as specified in their support contract, [redacted] as the NCSC's 'Ten Steps to Cyber

[1] Ransomware and Data Protection Compliance – ICO.org.uk
[redacted]

Security Guidance' makes clear, systems should be designed so that security updates can be applied as soon as they are made available.

Guidance was available which, had GCUK consulted, would have highlighted the steps to take to ensure the security of its systems. This includes the ICO's security checklist. The NCSC also provides guidance and recommendations for small businesses to follow to secure their systems, had GCUK consulted these guides, including following the Cyber Essentials, it is likely their systems would have been secured appropriately.

I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further Action Recommended

The Commissioner recommends that Gain Capital UK Limited should take steps to ensure it is compliant with the GDPR. The information above details the compliance issues relevant to this investigation. The guidance provided in this reprimand should be considered by Gain Capital UK Limited.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

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.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and powers under the GDPR. We will 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-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

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
[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