Case 202000583

Enforcement Order

GAIN GLOBAL MARKETS Inc.

2 August 2022

EXECUTIVE SUMMARY

A financial services company, Gain Global Markets Inc. (the data controller), suffered a cybersecurity incident when its systems were breached by a threat actor. Personal data of some 26,290 individuals representing distinct risk profiles, was accessed or exfiltrated. The breach was notified to the Ombudsman and the data subjects, as required under the Data Protection Act (2021 Revision) (DPA).

Based on the forensic investigations conducted by two IT firms hired by the data controller, the breach appears to have occurred as a result of a vulnerability in [redacted]. Apparently, adequate security standards to safeguard systems and data were not maintained; the latest security patches were not installed; regular vulnerability assessments or penetration testing were not undertaken; and staff awareness was lacking, contrary to established industry practices. Uncertainty surrounding the exfiltration of the personal data potentially continues to represent an ongoing risk for the affected data subjects.

The Ombudsman found that, on the balance of probabilities, these factors violated the seventh data protection principle of the DPA. However, they do not meet the threshold for causing substantial damage, as the categories of personal data involved are not sensitive. The Ombudsman also considered that the data controller, by means of its IT consultants, swiftly took initial and long-term technical and organizational measures to improve its infrastructure security posture.

Since appropriate protective technical and organizational measures were implemented by the data controller, the Ombudsman concluded that there are no further steps necessary to bring the data controller in compliance with the requirements of the DPA and ensure the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, of the personal data it processes, except the requirement that the data controller continue to carry out regular audits

and reviews of its security posture, at least on an annual basis,[1] to ensure that it remains up to date with current risks and development.

Contents

A. BACKGROUND

[redacted]

B. CONSIDERATION OF ISSUES

[redacted]

C. MITIGATING ACTIONS TAKEN BY THE DATA CONTROLLER

[redacted]

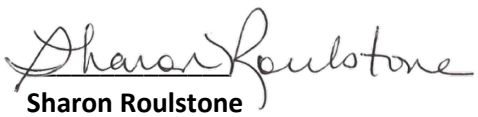
D. FINDINGS, RECOMMENDATIONS AND DECISIONS

Under section 45(1) of the DPA, for the reasons explained above, I make the following findings and decisions:

[1] BS ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements, paras 6-7.

- Under the seventh data protection principle a data controller is required to ensure that appropriate security and organisational controls are implemented throughout its processing activities, utilising best practices and a risk-based approach to identify, evaluate and mitigate threats to the organisation and its data. Such processing activities should be reviewed on a regular basis throughout the information lifecycle to ensure that appropriate safeguards and compliance with this principle are maintained.
- I find that Gain Global Markets, Inc. (the data controller) did not meet the requirements of the seventh data protection principle of the DPA, since adequate technical and organisational measures were not in place at the time of the breach. This led to the personal data of its clients not being processed in a manner that ensured their protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- Notwithstanding the above conclusion, the post-breach remediation steps taken by the data controller, as outlined above, were swiftly undertaken and satisfactorily implemented.
- In order for the data controller to remain compliant with the seventh data protection principle, I require that the data controller continues to carry out regular audits and reviews of its security posture, at least on an annual basis, in order to ensure that it remains up to date with current risks and developments.

Under section 47 of the Law, a person who receives an enforcement order under the DPA may, within 45 days of receipt and upon notice to the Ombudsman, seek judicial review of the Order to the Grand Court.



Sharon Roulstone
Ombudsman