Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	GAIN Capital-Forex.com Canada, Ltd. (Organization)
Decision number (file number)	P2020-ND-179 (File #015777)
Date notice received by OIPC	May 7, 2020
Date Organization last provided information	May 7, 2020
Date of decision	December 8, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization's head office is in New Jersey, USA. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information about clients and "demo" clients: • name, • date of birth, • gender, • email address, • passport number, • bank account number, and • sort code (in varying combinations depending on client), and • certain contact information of "demo clients" (telephone number, country of residence). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization is a subsidiary of GAIN Capital Holdings Inc.; the latter provides data processing and hosting services to the Organization. • On April 14, 2020, an external threat actor gained access to the service provider's network and created user accounts with administrative privileges. This enabled the threat actor to access servers which include customer personal information. • The threat actor ran several queries against client databases, and also extracted a zip file that may contain some or all of the results of the queries against client databases. • The breach was discovered on April 15, 2020 when daily system monitoring flagged suspicious activity. The breach was ended on April 18, 2020.
Affected individuals	The incident affected 2,888 individual clients, of which 29 have a connection to Alberta. Another 18,806 "demo clients" were affected; however, the Organization does not believe any of them were connected to Alberta.
Steps taken to reduce risk of harm to individuals	• Advised clients to monitor their accounts for suspicious activity and report suspicious activity to the Organization. • Provided clients with information regarding how they might engage in credit monitoring and similar guidance. • Identified and shut down the breached server. • Identified and patched the vulnerability that was used. • Set up a new communication to ensure that any patches released by the third party software are communicated directly to the product team. • Reset passwords on all affected administrative accounts and re-secured the domain from the top down. • Engaged two third party forensic firms.
Steps taken to notify individuals of the incident	Affected individuals were notified by email commencing May 7, 2020 and June 2, 2020.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported, *It is possible that phishing or spoofing could result. It (sic) limited cases, it is possible that some identity theft or fraud is possible (i.e. if, for a given individuals, the full range of information was accessed).* In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud and/or financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported it is "…still assessing this matter. Given the personal information that was potentially accessed, the harms are unlikely if individuals take some of the precautions identified in the notice letters." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party, personal information was exfiltrated, and significant numbers of clients were affected. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's network were to be used for fraudulent purposes, for example.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud and/or financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party, personal information was exfiltrated, and significant numbers of clients were affected. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's network were to be used for fraudulent purposes, for example.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email commencing May 7, 2020 and June 2, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner