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	Newcom Business Media Inc. (Organization)
Decision number (file number)	P2018-ND-073 (File #008894)
Date notice received by OIPC	June 5, 2018
Date Organization last provided information	June 5, 2018
Date of decision	July 6, 2018
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involves a compromised email account. The Organization reported that its investigation is ongoing and "it is not apparent which emails were accessed and therefore not apparent what information was and was not accessed". However, the Organization reported the following information may be at issue: • social insurance number, • banking information, • home address, • telephone number, • email address, • gender, • age, • family member names, • health benefit information.

	Further, "the emails may also contain the following information on employee's families": • name, • home address, • gender and health benefit account information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported "In Alberta, there are 4 individuals whose information may be subject to this unlawful access (1 employee and his family members)". To the extent this information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 28, 2018 the Organization became aware of an unauthorized access to the email account of the Chief Financial Officer (CFO). • It does not appear that any files of the Company were accessed and the unauthorized access is limited to strictly email communications. The email account contained email communication from approximately April 23, 2017 to early June 2018. • The cause of the unlawful access appears to have originated through a phishing scheme. • The incident was discovered by the CEO when an unauthorized email was sent to the accounting department requesting immediate transfer of a sum of money. That transaction was caught by the CEO and the accounting department and immediately halted. • The unauthorized access appears to have commenced the first week of April 2018.
Affected individuals	The incident affected a total of 84 employees and their family members, as well as 1 employee in Alberta and that employee's family members.
Steps taken to reduce risk of harm to individuals	The Organization took a number of steps, including: • Changed credentials for any targeted accounts, removed rules and forwards pertaining to breach. • Ran reports based on user account access, and compared locations to travel and known work locations to determine if valid. • Enabled full auditing on all user accounts.

	• Created new Data Loss Policy to retain deleted data from accounts during attacks. • Enhanced authentication and threat protection/safeguards. • Provided credit monitoring for affected individuals for one year. • Reported incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally and/or in writing between May 31 and June 4, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 that "Given the financial and other information that may have been accessed, harm to credit record, fraud, identity theft may result." I agree with the Organization's assessment. The comprehensive contact, identity, financial, family and medical information that may have been compromised could be used to cause the significant harms of identity theft and fraud, as well as phishing.
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 "We do not know yet whether the financial and other sensitive information on individuals was accessed; however, if it was, the potential for harm resulting from subsequent misuse, including credit record manipulation and identity theft could be significant. Given the evidence of hacking/phishing and the attempt at having money transferred using the information obtained, there is evidence of ill intent. …The likelihood that harm could have resulted is high; however, affected parties have been notified, measures have been put in place to monitor and prevent the harm and no harm has been reported to date, so at this point, the likely [sic] of harm is significantly reduced". I agree with the Organization. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion), and the information may have been exposed for approximately 2 months before the Organization became aware of the breach and took steps to mitigate potential harm.
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 as a result of this incident. The comprehensive contact, identity, financial, family and medical information that may have been compromised could be used to cause the significant harms of identity theft and fraud, as well as phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion), and the information may have been exposed for approximately 2 months before the Organization became aware of the breach and took steps to mitigate potential harm.	

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

I understand affected individuals were notified verbally and/or in writing between May 31 and June 4, 2018 in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner