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	Discovery Communications, LLC (Organization)
Decision number (file number)	P2019-ND-179 (File #013601)
Date notice received by OIPC	July 26, 2019
Date Organization last provided information	July 26, 2019
Date of decision	November 27, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Information involved in the breach may have included: • email address, • name, • address, • telephone number, • age, • gender, • date of birth, • marketing preferences, and • limited account activity information. For one Alberta resident, the information also included demographic information such as marital status and household income range. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The Organization uses a cloud-based platform to store and exchange certain corporate information. • On March 9, 2019, it learned from a third party that certain folders stored in the platform had been shared by staff with external business partners in such a way that the folders and the files within the folders could potentially be accessed by other parties. The next morning, the Organization reconfigured the access settings to these folders to remediate the issue. • The Organization investigated and identified a small number of customer marketing lists that were potentially accessible. The files in question were accessed and downloaded between two and four times by IP addresses not associated with the Organization between February 15 and March 10, 2019, most likely by a security researcher who was investigating the issue and through whom the Organization indirectly learned of the issue.
Affected individuals	The Organization reported that it "…identified approximately 13,000 unique email addresses associated with information that indicates the records belong to Alberta residents."
Steps taken to reduce risk of harm to individuals	• Disabled public access to the folders and initiated an internal investigation. • Implemented new procedures relating to the use of this cloud-sharing platform, and changing the default settings to employee sharing only. • Reviewing additional security measures that can be implemented.
Steps taken to notify individuals of the incident	Affected individuals were provided with written notice beginning on July 25, 2019.
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 did not specifically identify the potential harm(s) that might result from this incident, but its notice to affected individuals said "…it is always a good idea to exercise caution when responding to unsolicited emails requesting your personal information or account credentials. Be alert to any requests for personal information, in particular financial information, account numbers or passwords." In my view, a reasonable person would consider that the contact, identity and profile information at issue could be used to cause the

	harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are 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 that it "… has no evidence of these folders being accessed by any IP address not associated with [the Organization] prior to this time period. Under these circumstances, we do not believe there is a real risk of significant harm to the affected individuals." Further, the Organization's notice to affected individuals said it "…has not received any reports of suspicious emails being received by customers in its database and has no evidence of any misuse of your personal information." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent but rather internal error (misconfigured access). However, I am concerned that the Organization reported the files were "accessed and downloaded between two and four times by IP addresses not associated with the Organization" and said this was "most likely by a security researcher" but did not provide any confirmation. Further, the Organization said it "has no evidence of these folders being accessed by any IP address … prior to this time period", but does not say whether this is based on a review of audit logs. It is also not clear from the Organization's report how long the information was exposed.

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 profile information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is decreased as the breach did not result from malicious intent but rather internal error (misconfigured access). However, I am concerned that the Organization reported the files were "accessed and downloaded between two and four times by IP addresses not associated with the Organization" and said this was "most likely by a security researcher" but did not provide any confirmation. Further, the Organization said it "has no evidence of these folders being accessed by any IP address … prior to this time period", but does not say whether this is based on a review of audit logs. It is also not clear from the Organization's report how long the information was exposed.

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 affected individuals were provided with written notice beginning on July 25, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner