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	Dawn Food Products (Canada) Ltd. (Organization)
Decision number (file number)	P2019-ND-184 (File #013634)
Date notice received by OIPC	October 11, 2019
Date Organization last provided information	October 11, 2019
Date of decision	December 10, 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"	The Organization reported the information at issue varies by individual but may have included: • name, • business and personal contact information, • email address, • employment-related information (date of birth, employee ID, salary/compensation details and financial account numbers), • Social Insurance Numbers, and • payment card number (in limited cases). For a single employee, additional information possibly indicated the individual's religious or philosophical beliefs and sexual preference or orientation. 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	• In or around September 2018, an outside individual sent emails to a few of the Organization's employees soliciting their login information to the Organization's email system. • The individual appears to have been able to use the login information to gain unauthorized access to the employees' mailboxes. • On approximately April 5, 2019, the Organization determined that these mailboxes contained certain information about a limited number of employees, customers and other individuals, and investigated further to confirm the scope of the information and identify contact details.
Affected individuals	The incident affected 37 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged an independent computer forensics firm to assist with an investigation and reset affected email account passwords. • Worked with a data review and e-discovery firm to determine what type of information could potentially have been affected. • Taking steps to enhance the security of email systems, including by implementing heightened authentication procedures for employees logging into the email system. • Offered complimentary identity and credit monitoring services and dark web monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about October 10, 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 possible harms that might result from this incident, but its notification to affected individuals provided advice "If you believe your identity is being used unlawfully/fraudulently" and for remediating against fraud. In my view, a reasonable person would consider that the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft and fraud. Information related to religious or philosophical beliefs and sexual preference or orientation could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing emails) and allowed an unauthorized party to gain access to email accounts.

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, financial and employment information at issue could be used to cause the harms of identity theft and fraud. Information related to religious or philosophical beliefs and sexual preference or orientation could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing emails) and allowed an unauthorized party to gain access to email accounts.

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 notified by letter on or about October 10, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner