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	Saputo Dairy Products Canada G.P. (Organization)
Decision number (file number)	P2021-ND-156 (File #018461)
Date notice received by OIPC	August 29, 2020
Date Organization last provided information	July 19, 2021
Date of decision	August 25, 2021
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 incident involved some or all of the following information: <u>Clients</u> • name, • date of birth, • civic address, • telephone number, and • credit card information, or banking information. <u>Employees</u> • annual salary, • medical records, • social security numbers, and • passport information. <u>Commercial clients</u> • name, and • credit card information.

	"Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies. The organization reported, **"**Not all the type of information listed above is available for every customer or employee whose information has been compromised." This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On May 12, 2020, a customer contacted an employee of the Organization to validate an email request the customer received from the employee regarding changes to a payment bank account. • The employee confirmed no such request was made. • The Organization investigated and determined that the employee's email account had been compromised since May 1, 2020. An unauthorized email forwarding rule was automatically transferring emails to an external address. • The employee's password was most likely compromised via phishing emails. • The unauthorized party did not gain access to the Organization's IT systems or infrastructure.
Affected individuals	The incident affected 122 individuals, including nine (9) Alberta residents.

Steps taken to reduce risk of harm to individuals	Some steps taken to reduce risk of harm to individuals include: • Reset the password and initiated an investigation, including interviewing the employee with the compromised account. • Deleted the email forwarding rules. • Terminated the unauthorized access and retained a forensic firm to assist in determining the scope of the breach, including potentially what personal information could have been accessed by the unauthorized user(s). • Performed scans on all IT assets and confirmed that no server, VPN or firewall was breached. • Improved the security around Outlook 365. • Provided a list of indicators to help customers identify potential fraudulent emails and a list of actions to take should they receive a suspicious email. • Performed extended monitoring of all new IT configurations.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email or letter between August 28 and September 15, 2020, and again between September 28, 2020 and October 5, 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, *Customers could be contacted to change their payment information and direct payments to a fraudulent account. Credit card information could be misused by the hackers. However it should be noted that the credit card security codes were not part of the credit card information compromised.* 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. It appears from the circumstances of the incident that email addresses were also compromised. This information 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, *A misuse of the information is unlikely to happen at this point as the breach occurred from May 1st, 2020 to May13th, 2020 and the hackers had access only to one e-mail account. Moreover, Customers were warned by a communication sent on May 28, 2020. To date, no customer has reported a misuse of their information, more than three months after the security breach.*

	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 (deliberate intrusion into an employee's email account). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately two (2) weeks.

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. It appears from the circumstances of the incident that email addresses were also compromised. This information 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 (deliberate intrusion into an employee's email account). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately two (2) weeks.

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 the affected individuals by letter and/or email sent between August 28 and September 15, 2020, and again between September 28, 2020 and October 5, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner