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	Canadian Fertilizers Limited (a wholly owned subsidiary of CF Industries Holdings, Inc.) (Organization)
Decision number (file number)	P2020-ND-159 (File #017580)
Date notice received by OIPC	October 2, 2020
Date Organization last provided information	October 2, 2020
Date of decision	November 20, 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 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 incident involved all or some of the following information of employees, current employees and contractors: • name, • address, • telephone/cellphone number, and • position/title. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that telephone numbers of the affected individuals might include telephone numbers for contractors. As such, some of the information may qualify as "business contact information" which 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 email 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 disclosure of 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 to the business contact information. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On June 4, 2020, an unknown third party gained access to the Organization's data through a remote access server. • The Organization's investigation found the third party gained unauthorized access through a brute force attack of a single account. Files from two servers were removed from the network and stored (although not published publicly) on an online cloud storage website. • During the investigation, the files that had been stolen were deleted from the online cloud storage website. • The breach was discovered on June 5, 2020.
Affected individuals	The incident affected 214 individuals.
Steps taken to reduce risk of harm to individuals	• Investigated the cause and scope of the incident. • Required a password reset for all employees. • Notified all affected employees, retirees, former employees, and current contract workers. • Provided its contractor with a notice for contract workers who are no longer working on site. • Reminded employees to review IT security training about spotting a phishing attack. • Reminded employees to review its password policy. • Reminded employees to repot any suspicious activity to the local IT team. • Advised employees to review their account statements and to monitor credit reports.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 11, 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, *The primary type of harm that could occur to affected individuals as a result of the breach is that of being subject to a phishing attack and subsequently being subject to identity theft and/or fraud. In light of the type of information at issue, it is unlikely that affected individuals will be directly subject to identity theft and/or fraud without first being victim to some type of phishing attack.* I accept the Organization's assessment. A reasonable person would consider that cellphone numbers along with contact information could be used for the purposes of smishing (phishing), increasing the affected individuals' 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, *The likelihood that harm will occur to affected individuals is low. Affected individuals are at a risk of harm only in the event a third party commences a phishing attack and where affected individuals fall victim to such an attack and the attack succeeds in committing identify [sic] theft or fraud.* 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). The Organization reported that two servers were removed from its network and stored on an online cloud storage website, and later the stolen files were deleted from the website. It is not clear whether the unknown third party still possesses the stolen information.

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 cellphone numbers along with contact information could be used for the purposes of smishing (phishing), increasing the affected individuals' vulnerability to identity theft and fraud. These are 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). The Organization reported that two servers were removed from its network and stored on an online cloud storage website, and later the stolen files were deleted from the website. It is not clear whether the unknown third party still possesses the stolen information.

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 email on June 11, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner