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	Goodfellow Inc. (Organization)
Decision number (file number)	P2021-ND-252 (File #017714)
Date notice received by OIPC	October 8, 2020
Date Organization last provided information	November 8, 2021
Date of decision	December 9, 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 those 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 a distributor, manufacturer and importer of specialty wood products. Its head office is in Quebec, but it has offices across the country. 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: • name, • address, • banking information, and • government issued ID including social insurance numbers. 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 reported that its core systems were encrypted with ransomware on September 24, 2020. • A ransom demand indicated that sensitive information would be disclosed if a payment was not made. • There is evidence that some personal information was exfiltrated but the full scope of the exfiltration has not yet been determined. • As of the date of the Organization's report of the breach, there is not information indicating that any personal information that may have been taken has been published or distributed.
Affected individuals	The incident affected 1,200 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately retained security and forensic experts to assist with an investigation. • Provided credit-monitoring services to all employees. • Retained an IT security and forensics specialist to undertake a review of the system and remediate the attack vector. • Implementing further steps informed by the results of the forensic analysis
Steps taken to notify individuals of the incident	Affected individuals were notified verbally (live) on October 2, 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 possible harms that may result from the breach as "Identity theft, phishing, financial theft". In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 "… is proceeding on the basis that PII has been exfiltrated and will be used". In my view, 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, ransom demand). The Organization reported "there is no information indicating that any personal information that may have taken has been published or distributed by the threat actor although it is likely that the publication will occur if a payment is not made". The lack of reported incidents resulting from this

	breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

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 the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. 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, ransom demand). The Organization reported "there is no information indicating that any personal information that may have taken has been published or distributed by the threat actor although it is likely that the publication will occur if a payment is not made". The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

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 affected individuals verbally (live) on October 2, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner