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 Forest Products Ltd. (Organization)
Decision number (file number)	P2021-ND-140 (File #017465)
Date notice received by OIPC	April 17, 2020
Date Organization last provided information	April 17, 2020
Date of decision	May 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 incident involved all or some of the following information: • name, • salary, • social insurance number, • pension information, • address, • date of birth, • scholarship amount, • photographs of 2 passports • photograph of 1 birth certificate, and • Canadian confirmation of permanent residence form (containing date of birth and a travel document number) for one minor age individual. 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	• An employee's laptop bag and laptop were stolen in Edmonton, Alberta on or about March 1, 2020. • The laptop's local storage drive does not contain documents or files containing personal information. However, several months of emails are stored locally on the laptop. • The Organization determined that some of the emails or their attachments contained personal information. • On or about March 28, 2020, the software the Organization uses when a device connects to the internet, contacted the Organization to provide an update on the laptop activities. The Organization "isolated" the laptop, blocking all network activity and making the laptop useless. The laptop remained online until March 29, 2020. • The Organization reported that when the laptop was online, its activity was directed towards removing or disabling the software. The Organization believes the software was successfully removed or disabled. • The software logs indicate that the laptop has been powered up several times since it was stolen and that the laptop's local administrator account has been compromised. • The laptop has not been recovered.
Affected individuals	The incident affected 536 individuals, including 202 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement. • Offered all affected individuals credit monitoring services for one year. • Encrypting all corporate laptops. • Will to employees setting out best security practices when travelling with corporate laptops outside of the office.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter during the period from March 25, 2020 to April 6, 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 information could be used for identity theft or financial fraud." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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: *This appears to have been a random theft of opportunity. The more recent developments described on or around March 29 above suggest attempts to access content on the laptop. In these circumstancs [sic], the risk may be more than conjectural; however, it is difficult to assess the likelihood that the harm identified under Section 12 will actually result.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the laptop in question was only password protected and not encrypted. There were attempts to access the contents of the laptop, and to date, the laptop has not been recovered.

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 financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the laptop in question was only password protected and not encrypted. There were attempts to access the contents of the laptop, and to date, the laptop has not been recovered.

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 affected individuals were notified by letter during the period from March 25, 2020 to April 6, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner