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	Arrow Truck Sales, Inc. (Organization)
Decision number (file number)	P2022-ND-047 (File #021079)
Date notice received by OIPC	March 5, 2021
Date Organization last provided information	March 5, 2021
Date of decision	August 29, 2022
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 retailer of pre-owned medium and heavy duty trucks operating primarily in the United States and Canada. Arrow is incorporated in Missouri and has its headquarters in Kansas City, MO. 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 some or all of the following information: • name, • phone number, • date of birth, • passport number, • bank account number, • routing number, • partial and/or expired credit card number and expiry date, and • social insurance number. 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	• Personnel reported being unable to access the servers and that login credentials had been changed. • The Organization determined that on or about November 16, 2020, an unauthorized third party gained access to its network and subsequently acquired some of its internal company information from a server before installing a ransomware program. • The unauthorized party posted certain of the Organization's information on a publicly accessible website. • The Organization learned that certain of its customers' personal information was affected after completing a detailed search and a manual review of thousands of files. • The Organization reported, "We are not aware of any cases of identity theft or fraud connected to this incident and do not believe the unauthorized third party was targeting personal information in the incident."
Affected individuals	The incident affected 35 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Began an investigation with the support of outside cybersecurity experts and took steps to prevent further unauthorized access. • Offered 24 months of complimentary identity theft and credit monitoring services. • Established a call center to respond to questions. • Took measures to ensure the unauthorized third party did not have access to its systems. • Continuing to monitor and improve its capabilities to detect any further threats and avoid any future unauthorized activity. • Reported the incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 5, 2021.
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	The Organization did not specifically identify any harm that might result from this incident. However, the Organization's notification to affected individuals stated, *We took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of*

non-trivial consequences or effects.	*our systems...We have arranged with Trans Union to provide you with a two-year subscription to myTrueIdentity, an online monitoring service, at no cost to you...Remain vigilant and carefully review your accounts for any suspicious activity...If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained.* 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, fraud, and financial loss. 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... *We are not aware of any cases of identity theft or fraud connected to this incident and do not believe the unauthorized third party was targeting personal information in the incident.* 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party 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.

The contact, identity, and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. 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, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. Further, the information may have been available to the unauthorized third party 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 affected individuals by letter on March 5, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance.