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	Matson Navigation Company and Horizon Lines (Organization)
Decision number (file number)	P2017-ND-28 (File #002219)
Date notice received by OIPC	January 5, 2016
Date Organization last provided information	February 25, 2016
Date of decision	February 1, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • date of birth, • address, • telephone number, • emergency contact information, • Social Security Number, • bank account and routing number, • photocopy of passport, • credential documents, and • fit for duty medical documents. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected from an individual residing in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	

Description of incident	• An external removable hard drive was last backed up on November 9, 2015 and was on a ship that was in dry dock in China during November 2015. • After a subsequent journey involving rough seas, the device was discovered to be missing on December 7, 2015, after the ship returned to port in Tacoma, Washington. • The personal information at issue was stored on the device, which was password protected but not encrypted. • It is not known if the device was lost or stolen, but it has not been recovered.
Affected individuals	A total of 14,074 individuals were affected, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals. • Offered no-cost credit protection and monitoring services. • Reviewing information technology and data security policies and practices and evaluating potential enhancements.
Steps taken to notify individuals of the incident	The affected resident of Alberta was notified by letter sent December 23, 2015.
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 "While the potential exists for harm such as fraud, identity theft, effects on credit ratings and financial loss if an unauthorized person were to gain access to and improperly use information stored on the device … there is no evidence of any individual actually having gained access to the database on the missing device." In my view, the contact, identity, health and financial information at issue could be used to cause the harms of identity theft and fraud, financial loss, negative effect on credit rating, and possibly hurt, humiliation and embarrassment. 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 that "…there is no evidence of any individual actually having gained access to the database on the missing device." Further, the "database on the device was accessible only with a valid user ID and password" which "provides a layer of protection in the event the device were to be obtained by an unauthorized individual." The Organization's "investigation has revealed no evidence of malicious intent or unauthorized use of the information to date. Moreover, given that there have been no reports of misuse of the information contained on the device over the past two months, it would appear that the risk of any potential harm at this point is low and continues to decline over time."

	In my view, there is a real risk of harm resulting from this incident. The Organization does not know the cause of the breach (human error vs. deliberate action with malicious intent), the device was not encrypted, and has not been recovered. I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen 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, I have decided that there is a real risk of significant harm resulting from this incident.

The contact, identity, health and financial information at issue could be used to cause the harms of identity theft and fraud, financial loss, negative effect on credit rating, and possibly hurt, humiliation and embarrassment. These are significant harms. The Organization does not know the cause of the breach (human error vs. deliberate action with malicious intent), the device was not encrypted, and has not been recovered. I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by letter sent December 23, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner