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	Helly Hansen AS (Organization)
Decision number (file number)	P2018-ND-096 (File #009246)
Date notice received by OIPC	July 19, 2018
Date Organization last provided information	July 19, 2018
Date of decision	August 2, 2018
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 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 registered in Norway and 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: • first and last name, • address (street, city, region, country, postal code), • telephone number, • payment card information, expiry date, and CVV number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• During a scan by the Organization's e-commerce service provider of its client sites, it was discovered that malware had been embedded on the hellyhansen.com e-commerce website.

	• As a result of this malware, payment card information collected from April 20 - 26, 2018 and May 2 - 14, 2018 may have been compromised. • The incident was discovered through monitoring conducted by the third party vendor (Magenta Inc.), who services the platform. • The malware was identified on May 14, 2018, and confirmed by independent forensic investigation on July 16, 2018.
Affected individuals	The incident may have affected 3,817 users globally, including 83 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately contained and remediated the incident. • Working closely with the platform provider and a forensics firm to further safeguard the e-commerce platform. • Deleted and reset administrator account credentials and installed additional security scans for malware on the e-commerce platform. • Advising all affected individuals of the incident and the steps they may take to safeguard their financial information. • Notified data protection authorities in Norway, Canada and in the process of notifying US authorities.
Steps taken to notify individuals of the incident	The Organization reported that it is "in the process of notifying impacted individuals" and "Emails are being deployed by region".
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 potential harm(s) that might result from this incident as "Potential unauthorized charges on existing credit card account." In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft 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.	In assessing the likelihood that significant harm would result from this incident, the Organization reported "At this time [the Organization] has no evidence that any payment card information has been misused. As stated above, if the incident is reported timely to banks and credit card companies, consumers should not be liable for any unauthorized purchases. [The Organization] is taking all reasonable measures to ensure potentially affected customers are notified and informed so that they can take steps to protect their information."

	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 and installation of malware). Further, the information may have been exposed for over 2 weeks. The Organization can only speculate that affected individuals may not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. 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 and installation of malware). Further, the information may have been exposed for over 2 weeks. The Organization can only speculate that affected individuals may not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to my office in writing within ten (10) days of this decision that it has done so.

Jill Clayton
Information and Privacy Commissioner