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	Luxury Retreats (Organization)
Decision number (file number)	P2018-ND-076 (File #008752)
Date notice received by OIPC	May 24, 2018
Date Organization last provided information	May 24, 2018
Date of decision	July 9, 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 an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved certain customer personal information that was provided in connection with booking a villa. The information varied by customer but may have included: • name, • address, • date of birth, • payment card account number, • external verification code (CVV), • financial account number, • driver's license number, and • passport number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that six Alberta residents may have been affected; to the extent this information was collected in Alberta I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 22, 2018, the Organization learned that an unknown individual had gained access to an employee's corporate email account and used the employee's account to create and send spam emails. • The Organization did not identify any evidence that emails stored in the employee's account were viewed, but could not eliminate the possibility. • The Organization identified unauthorized access to the email account between September 7, 2017 and March 22, 2018.
Affected individuals	The incident affected 6 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately re-secured the account, initiated an investigation, and engaged a data forensics firm to assist. • Offered affected individuals one year of complimentary credit monitoring and identity theft protection services. • Taking additional measures to help prevent a similar occurrence from happening again.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent May 24, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 affected here includes payment card information which is generally used to make fraudulent purchases elsewhere online. However, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card. Five individuals had a passport number and/or driver's license affected, and none of those included Alberta residents". In my view, a reasonable person would consider that the identity (date of birth, if not driver's license or passport number) 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 "Given that in Canada there is zero liablity [sic] for fraudulent credit card purchases made on an individual's credit card, there is no risk of significant harm to the affected individual [sic] in Alberta arising from this incident. The affected individuals will be made whole by their credit card issuer. There may be some inconvenience associated with a replacement card, but that is not significant harm". Further, "Upon first learning of [the] suspected incident, [the Organization] immediately re-secured the account, initiated an investigation, and engaged a leading data forensics firm to assist. Although the investigation did not identify any evidence that emails stored in the employee's account were viewed, the investigation could not eliminate that possibility. To be clear, the company has no

	evidence that any of its customers' personal information was accessed, acquired, or misused in any way". In my view, the likelihood of harm resulting in this case is increased as the breach is the result of malicious intent (deliberate access by an unknown individual who used an employee's corporate email account to create and send spam emails) and the information may have been exposed for almost 6 months. The Organization is unable to eliminate the possibility that emails stored in the compromised employee account were viewed. 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 as a result of this incident.

A reasonable person would consider that the identity (date of birth, if not driver's license or passport number) and financial information at issue could be used to cause the significant harms of identity theft, and fraud. The likelihood of harm resulting in this case is increased as the breach is the result of malicious intent (deliberate access by an unknown individual who used an employee's corporate email account to create and send spam emails) and the information may have been exposed for almost 6 months. The Organization is unable to eliminate the possibility that emails stored in the compromised employee account were viewed. 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). I understand affected individuals in Alberta were notified by letter sent May 24, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner