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	Gray Monk Estate Winery (Organization)
Decision number (file number)	P2021-ND-091 (File #013326)
Date notice received by OIPC	June 3, 2019
Date Organization last provided information	June 3, 2019
Date of decision	March 30, 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 operates in British Columbia, 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: • name, • mailing address, • telephone number, • email address, • credit card number, cardholder name and expiry date, • notes respecting customer preferences, • start date of membership, • name of the employee that signed up the member. 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	• On May 22, 2019, the Organization sent an email to some of its members and inadvertently attached a document containing the information at issue of other members. • The email was received by 63 members and included the personal information of 1,232 individuals. • The breach was discovered the same day, when one of the recipients reported the error to the Organization.
Affected individuals	The incident affected 1,232 individuals, including 374 located in Alberta.
Steps taken to reduce risk of harm to individuals	• Followed up with the unintended recipients, via multiple avenues, requesting they delete the attachment without reading it and provide confirmation of having done so. • Reviewing practices and procedures to avoid future incidents. • Reported the incident to data protection authorities. • Provided affected individuals with a one year credit monitoring service.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and telephone beginning May 22, 2019.
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 that "Privacy commissioners in Canada have previously noted that a breach of an individual's name and credit card number could result in identity theft and financial fraud, with potential negative effects on an individual's credit record". In addition, the Organization's notice to affected individuals "... recommended that each wine club member contact his or her credit card provider immediately and follow its recommended next steps to guard against any potential misuse of any compromised credit card information." In my view, a reasonable person would consider that the contact, financial and transaction information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 it considered a number of factors in determining the likelihood that significant harm would result from this incident, including, but not limited to: • The scope of the breach, which was limited to disclosure to a small number of members who are also affected by the breach. As a result, these recipients "... may be less likely to misuse or exploit the disclosed information".

	• All but 18 of the unintended recipients confirmed they deleted the information without reading it. • The recipients are well-known to the Organization and would be "much less likely to misuse or exploit the disclosed information, as any misuse might be traceable back to them". Overall, the Organization reported that it "...considers that the circumstances of the breach, the immediate mitigation steps taken ... the multi-channel and repeated notification to members and the offer of a credit watch and insurance service has significantly reduced any risk of significant harm to any individuals affected by the breach. As noted above, the [Organization] is currently unaware of any improper use of any member's credit card or other personal information...". I generally agree with the Organization's assessment. A reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach did not result from malicious action, the unintended recipients are known to the Organization, and the Organization has been able to contact many of the recipients to confirm they deleted the information. However there are still a number of recipients who have not been contacted (18) and therefore the Organization has not been able to confirm the information was not used, forwarded, etc.

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, financial and transaction information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is decreased as the breach did not result from malicious action, the unintended recipients are known to the Organization, and the Organization has been able to contact many of the recipients to confirm they deleted the information. However there are still a number of recipients who have not been contacted (18) and therefore the Organization has not been able to confirm the information was not used, forwarded, etc.

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 email and telephone beginning May 22, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner