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	Peter Michael Winery (Organization)
Decision number (file number)	P2017-ND-19 (File #001072)
Date notice received by OIPC	June 22, 2015
Date Organization last provided information	June 22, 2015
Date of decision	January 30, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is located in California, U.S.A. and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • payment card number, • related payment address, and • date of birth. 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	• On May 27, 2015, the Organization was notified by its e-commerce vendor that an unauthorized third party breached the vendor's systems on April 12, 2015, and may have accessed personal information of the Organization's customers stored in the vendor's database. • The vendor discovered evidence of the breach on May 13, 2015 and notified the Organization on May 27, 2015. • The Organization is not aware of any fraud that has occurred as a result of this incident at this time.
Affected individuals	The incident affected 29 Canadians, including 6 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The vendor notified the U.S. Secret Service, as well as payment processors who subsequently notified credit card companies and issuing banks. • The vendor is working with payment industry partners to convert its system to a tokenization system where it will not store any credit card numbers in the future. At this time, credit card data for the Organization's customers has been removed from the vendor's systems.
Steps taken to notify individuals of the incident	Written notice of the incident was mailed to affected residents of Alberta on June 22, 2015.
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 that "As the information includes names, addresses and credit card numbers, which together constitute sensitive data and the unauthorized access was the result of an intruder, [the Organization] has taken the step of notifying customers of the incident and providing fraud and identity theft monitoring to potentially affected Canadians through Equifax." I agree with the Organization's assessment. The information at issue could be used to cause the harms of 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 noted that "the unauthorized access was the result of an intruder", and reported that, as a result, it "has taken the step of notifying customers of the incident and providing fraud and identity theft monitoring to potentially affected Canadians through Equifax." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the information was exposed for approximately 1 month between the time of the incident and the vendor becoming aware of it.

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. The information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the information was exposed for approximately 1 month between the time of the incident and the vendor becoming aware of it. 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 that written notice of the incident, in accordance with the Regulation, was mailed to affected residents of Alberta on June 22, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner