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	Rennline Automotive (Organization)
Decision number (file number)	P2019-ND-072 (File #012113)
Date notice received by OIPC	February 22, 2019
Date Organization last provided information	February 22, 2019
Date of decision	June 3, 2019
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 is 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, • shipping and billing address, • order information, • payment card number, type, expiry date, and verification code (if provided). 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	• The Organization operates the e-commerce store rennline.com. • On January 18, 2019, the Organization discovered suspicious code on the website.

	• An investigation determined that the unauthorized code was added by an unauthorized individual so that payment card information entered by purchasers on the e-commerce website was copied and sent to an unauthorized server. The code was active between May 28, 2018 and June 13, 2018, June 15, 2018 and July 12, 2018, July 20, 2018 and August 13, 2018, and August 22, 2018 and January 18, 2019. • The incident was discovered on January 18, 2019, after the Organization was notified by its payment processor that cards that were used on the website showed signs of being used in fraudulent transactions.
Affected individuals	The incident affected 2,540 individuals.
Steps taken to reduce risk of harm to individuals	• Removed the code and worked with a cybersecurity firm to investigate the incident. • Recommending that affected individuals review their payment card statements for any unauthorized charges. • Notified the payment card brands so that they can issue alerts to card issuers regarding the potential for fraudulent charges on the cards involved. • Reported breach to law enforcement and cooperating with their investigation. • Providing a telephone number that customers can call with any questions they may have. • Taking steps to strengthen the security of the website .
Steps taken to notify individuals of the incident	The Organization reported that it is notifying affected individuals by letter on February 21, 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 "Stolen payment card information can be used to make fraudulent purchases." I agree with the Organization's assessment. A reasonable person would consider that the 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 "Because the payment card network rules generally provide that cardholders are not responsible [sic] for unauthorized charges, if reported timely, there is not a significant likelihood that harm will result. To further diminish the likelihood of harm, [the Organization] is recommending that the individuals involved closely review their payment card statements for any unauthorized charges." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the incident is the result of malicious intent (deliberate action). It appears the information may have been exposed for over 6 months. The Organization was informed of the unauthorized access by its payment processor reporting cards that were used on the website showed signs of being used in fraudulent transactions. The Organization can only speculate that affected individuals will not be held responsible for fraudulent charges.

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 financial 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 incident is the result of malicious intent (deliberate action). It appears the information may have been exposed for over 6 months. The Organization was informed of the unauthorized access by its payment processor reporting cards that were used on the website showed signs of being used in fraudulent transactions. The Organization can only speculate that affected individuals will not be held responsible for fraudulent charges.

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 by letter on February 21, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner