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	PAX Labs, Inc. (Organization)
Decision number (file number)	P2016-ND-50 (File #003536)
Date notice received by OIPC	August 17, 2016
Date Organization last provided information	August 17, 2016
Date of decision	August 24, 2016
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 an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • billing and shipping address, • credit or debit card number, expiration date, and security (CVV) code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Alberta customers who made purchases on the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 15, 2016, the Organization discovered that an unauthorized party had gained access to one of its cloud-based website servers on June 25, 2016, and installed unauthorized software. • The Organization removed the software on July 15, 2016. Subsequently, an unauthorized party added similar software on July 22, 2016, which was removed that same day. • The Organization's investigation revealed that the unauthorized party or parties accessed personal payment card information of approximately 6,000 customers who had purchased from the Organization's websites between June 25, 2016 and July 15, 20l6, and on July 22, 2016. • No payment card PIN numbers or other forms of personal information were accessed.
Affected individuals	The incident affected approximately 6,000 individuals, including 20 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Worked with third-party forensic experts to investigate incident. • Reported the incident to payment card processors. • Enhanced security measures, including more aggressive firewall rules and detailed system monitoring tools, have been put in place. • Providing 12 months of free identity theft monitoring services to affected Canadian individuals.
Steps taken to notify individuals of the incident	The Organization reported it "is in the process of delivering notice to each of the affected individuals of the unauthorized access of their personal information."
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 "there is a risk of unauthorized charges on the individuals' credit cards." I agree with the Organization. The information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 did not specifically assess the likelihood of harm resulting from this incident, but reported it believes the steps it has taken will "minimize the scope of such harm." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of a deliberate intrusion by an unauthorized party and the attack was repeated a week after the initial incident was contained. Further, the information was exposed for almost three weeks before the Organization became aware of the breach.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the affected individuals.

The information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the incident was the result of a deliberate intrusion by an unauthorized party and the attack was repeated a week after the initial incident was contained. Further, the information was exposed for almost three weeks before the Organization became aware of the breach.

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 provide me with written confirmation that it has done so on or before September 9, 2016.

I understand the Organization is in the process of delivering notice to each of the affected individuals.

Jill Clayton
Information and Privacy Commissioner