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	Deluxe Small Business Sales Inc., operating as MAC Highway (Organization)
Decision number (file number)	P2021-ND-002 (File #018806)
Date notice received by OIPC	December 23, 2020
Date Organization last provided information	December 23, 2020
Date of decision	January 26, 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 those 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 all or some of the following information: • first and last name, • email address, • physical address, • telephone number, and • customer identification number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA; however, the Organization says "the incident does not concern personal information as it involves business contact information." "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation

	to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies in this case.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization manages customer accounts through an administrative portal that is owned and managed by a third party, Endurance International Group, Inc., and operated as www.resellerclub.com. • On December 2 and December 17, 2020, authorized employees were unable to log in to the portal; on each occasion the passwords were reset. • On December 21, 2020, the Organization investigated and found the password to the portal had been compromised and an unauthorized individual had access to the customer accounts on December 2 and 17. • The Organization determined the intruder used his/her unauthorized access to the portal to register approximately one terabyte worth of websites, which the Organization reported was "presumably to be used to perpetrate fraudulent activity." • The Organization is continuing to investigate the matter and review relevant logs to identity any other relevant information regarding the intrusion.
Affected individuals	The incident affected approximately 41 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the websites and the intruder's access. • Reset passwords with passwords of maximum length and complexity. • Engaged a team to review all logs for potentially harmful actions. • Assigned a team to monitor the status of the security of the portal and report all anomalies. • Notified data protection authorities.

Steps taken to notify individuals of the incident	The Organization reported "…given the nature of information compromised and the apparent motivation of the intruder, there is no real risk of significant harm arising from this incident. [The Organization] does not therefore propose to notify customer contacts."
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 "the incident does not concern personal information as it involves business contact information, and in any event does not give rise to a real risk of significant harm." In my view, a reasonable person would consider that email addresses in combination with telephone numbers and customer identification could be used for the purposes of smishing (phishing), 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.	Among other things, the Organization reported: • "…the intruder used his/her unauthorized access to the administration portal to register approximately one terabyte worth of websites, presumably to be used to perpetrate fraudulent activity"; • "The motivation of the intruder does not therefore appear to be focused on theft of information", and • "At this stage no evidence has been found that indicates a compromise to [the Organization's] systems, or to www.resellerclub.com." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the information at issue was compromised due to the malicious action of an unknown third party (unauthorized access). The information was accessed on 2 occasions. The Organization can only speculate as to the intruder's motivation.
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 email addresses in combination with telephone numbers and customer identification could be used for the purposes of smishing (phishing), increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the information at issue was compromised due to the malicious action of an unknown third party (unauthorized access). The	

information was accessed on 2 occasions. The Organization can only speculate as to the intruder's motivation.

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), and confirm to my Office in writing, within ten (10) days of the date of this decision, that this has been done.

Jill Clayton
Information and Privacy Commissioner