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	Glentel Inc. (Organization)
Decision number (file number)	P2021-ND-084 (File #012386)
Date notice received by OIPC	March 5, 2019
Date Organization last provided information	March 5, 2019
Date of decision	March 16, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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 Organization reported: *The incident resulted in unauthorized disclosure of two kinds of personal information, as follows:* *<u>Category A: Customer Information</u>* *The incident resulted in the disclosure of information of about 207 customers in Alberta who purchased a third party extended warranty during the period November 26 to 28, 2018….* *The affected information included internal-facing information about each transaction as well as the following personal information about the customers involved in the transaction and their mobile devices: transaction date, customer name, customer email address, warranty agreement ID number, and customer's device ID number.*

	<u>Category B: Business Contact information</u> *The incident resulted in the disclosure of the names and, in some instances, other business contact information of approximately 118… employees (most, if not all, of whom are located in British Columbia) and approximately 38 employees of organizations with which [the Organization] has business relationships across Canada, including potentially in Alberta.* 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. The Organization reported some of the information is "business contact information", which 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 e mail 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 disclosure of 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, the business contact information is not excluded from the application of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 29, 2018 an employee in the Organization's head office in Burnaby, British Columbia received a fraudulent email from an unknown third party. • The email appeared to be from the Organization's Chief Executive Officer and attached a link to a fraudulent website. The email deceived the employee into disclosing the employee's credentials for their work email account. • The unknown third party then used the employee's credentials to access the employee's work email account and establish rules based on key words, to automatically forward certain emails to an unauthorized Gmail account.

	• On November 29, 2018, approximately 60 emails from the employee's work email account were forwarded before the incident was discovered and contained. • The incident was discovered on the same day.
Affected individuals	The incident affected approximately 207 customers in Alberta and "potentially" employees in Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to contain the incident, including suspending the employee's credentials and isolating their personal computer. • Investigated the incident to verify that it has been contained and did not affect other work email accounts. • Engaged external legal counsel and an information technology forensic consultant to conduct a further investigation. • Notified the third-party provider of the extended warranties purchased by the individuals. • Reported the incident to the RCMP and to Google. • Provided head office employees with supplementary training regarding phishing emails. • Enhanced rules to prevent spam and phishing emails and to detect unauthorized auto-forwarding rules for work emails. • Implementing administrative measures to minimize internal access to customers' personal information, and to improve safeguards for the internal use of customer information. • Considering implementing additional technological measures to protect its information technology systems.
Steps taken to notify individuals of the incident	The Organization reported that it gave notice by email to all customers on February 4, 2019, but that it "…does not intend to give notice to the individuals (i.e. employees) in Category B described above, because [the Organization] believes that the unauthorized disclosure of their personal information (i.e. names and business contact information), which is low sensitivity information, does not present a real risk of significant harm to the relevant individual."
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 said the business contact information at issue "(i.e. names and business contact information), which is low sensitivity information, does not present a real risk of significant harm to the relevant individual." The Organization's notice to affected customers also said: *You should be vigilant against third parties attempting to gather information from you using deceptive emails (commonly known as "phishing") and links to fake*

	websites. In particular, you should remain alert for fraudulent emails …You should not disclose any of your passwords by phone or email … In my view, a reasonable person would consider that the contact and transaction information, as well as email addresses, particularly in combination, 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 did not specifically assess the likelihood of significant harm resulting fro this incident. In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent and involved deliberate action impersonating the Organization's Chief Executive Officer, a link to a fraudulent website, compromised credentials, and an unauthorized email forwarding rule. Additional phishing emails were sent from the compromised account.

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 and transaction information, as well as email addresses, particularly in combination, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm is increased because the breach resulted from malicious intent and involved deliberate action impersonating the Organization's Chief Executive Officer, a link to a fraudulent website, compromised credentials, and an unauthorized email forwarding rule. Additional phishing emails were sent from the compromised account.

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 customers by email on February 4, 2019. The Organization is not required to notify these affected individuals again. I understand the Organization did not notify affected employees of the breach; however, based on the Organization's report of the incident, it is not clear if the personal information of any of these employees was collected in Alberta, or involved email addresses and would result in a real risk of significant harm, such that I would have jurisdiction to require the Organization to notify these individuals.

Jill Clayton
Information and Privacy Commissioner