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	Samsung Electronics Canada Inc. (Organization)
Decision number (file number)	P2021-ND-090 (File #012213)
Date notice received by OIPC	February 28, 2019
Date Organization last provided information	February 28, 2019
Date of decision	March 30, 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 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 all or some of the following information: • name, • address, • email, • telephone number, and • product purchase details. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third party, Glentel Inc., to operate its website.

	• Glentel advised the Organization that, on November 29, 2018, an employee's email account was compromised following a successful phishing attempt. As a result, the intruder was able to view personal information related to purchases made on the website. • Glentel advised the incident was contained the same day that it occurred.
Affected individuals	The incident affected 9,787 individuals, including 1,256 located in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported that Glentel: • took steps to address and successfully contain the vulnerability, • secured the affected employee's account, • reported the incident to the police, and • retained cybersecurity experts to investigate.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on February 22 and 25, 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 did not specifically identify harm(s) that might result from this incident, but its notice to affected individuals advised them to... *...be cautious of emails that: 1) come from unrecognized senders; 2) ask you to confirm personal or financial information over the Internet; 3) aren't personalized; or 4) try to engage you to act quickly by threatening you with frightful information.* The notice also said: *Do not click on links, download files or open attachments in emails from unknown senders. Beware of links in emails that ask for personal information and emails that ask you to sign into a service to look at a document. These may be attempts to steal your account credentials.* In my view, a reasonable person would consider that the contact and transaction information at issue, particularly when combined with email addresses, 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 provide an assessment of the likelihood of significant harm resulting from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party (deliberate phishing attack).

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 at issue, particularly when combined with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party (deliberate phishing attack).

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 mail on February 22 and 25, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner