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	Imperial Oil Limited (Organization)
Decision number (file number)	P2018-ND-087 (File #008652)
Date notice received by OIPC	May 10, 2018
Date Organization last provided information	May 10, 2018
Date of decision	July 26, 2018
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 in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported: *It is unclear what data was exposed since data was over written by the perpetrator, however the potential personal information may have included:* • *title/salutation;* • *first name, last name;* • *address;* • *home phone number;* • *communication language; and* • *Esso Extra points balance.* 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization's EssoExtra Loyalty Program mobile application, which is hosted and managed externally by the Organization's third party vendor, Exchange Solutions International, was the focus of an attack by an unknown third party. • As a result, loyalty program member accounts were accessed by a third party, allowing a perpetrator to redeem points for merchandise and gift cards in BC and Alberta. • The unauthorized activity occurred between February 11, 2018 and March 22, 2018 and was first identified on February 21, 2018. • Technical defects were researched and confirmed March 9, 2018 and then the required corrections were implemented on March 15, 2018 and March 22, 2018.
Affected individuals	The incident affected 377 accounts.
Steps taken to reduce risk of harm to individuals	• Disabled the functionality that led to the application being vulnerable to an attack as soon as the problem was understood. • Remediated and tested the application. • Will undertake a full security penetration test by a third party security firm to verify that there are no further vulnerabilities. • Any loyalty points removed from a customer's account will be reinstated and the customers notified in writing.
Steps taken to notify individuals of the incident	The Organization reported that "Attempts to contact impacted customers with telephone numbers occurred as the incident unfolded….Impacted customers are being notified in writing by email or direct mail."
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 the information at issue is "is considered less sensitive as it does not contain extremely sensitive information (i.e. full credit card numbers, SIN, etc.)." Further, "The types of harm that could result are believed to be minimal, but could potentially include exposure of basic customer contact data or loss of loyalty points if fraudulently redeemed. Imperial has committed to ensuring that any such impacts as a result of this incident are resolved to ensure users are provided with access to their accounts and all loyalty points would be reinstated." Finally, the Organization also reported that it assessed "the risk of harm to be low. However, out of an abundance of caution, and in recognition of the fact that multiple pieces of low-risk personal information were potentially gathered at the same time, [the organization] did think it was appropriate to notify the Alberta OIPC."

	I agree with the Organization that the information at issue is less sensitive than if identity or financial information had been compromised (social insurance number, credit card number). However, I am concerned that the contact information at issue in this case, in conjunction with information that individuals are members of the Organization's loyalty program, provides a comprehensive enough profile that individuals could be at risk for spear phishing, which I have previously said is a significant harm.
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.	In assessing the likelihood of harm resulting from this incident, the Organization reported: • *ESI evidence supports that this breach was conducted by a lone operator from Alberta Canada.* • *The application has many security controls to prevent unauthorized access including encryption. The breach was due to undetected security vulnerability in the back end API.* • *lt is unlikely that any harm will result from this breach.* • *There is clear evidence of financial fraud and theft being the motive.* • *There is not enough PII data to suspect any risk of identity theft.* • *There were 377 customers affected by this breach.* • *lt is unclear if any vulnerable individuals are involved. The program does not collect any demographic information with respect to age.* In my view, the likelihood of harm resulting in this case is increased because the breach was the result of malicious action of an unknown third party (deliberate intrusion and fraudulent redemption of points). The information was potentially exposed for over a month. While there is evidence of financial fraud and theft being the motive, this does not abrogate the possibility that malicious actors would use the information for spear phishing purposes.
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. The contact information at issue in this case, in conjunction with information that individuals are members of the Organization's loyalty program, provides a comprehensive enough profile that individuals could be at risk for spear phishing, which I have previously said is a significant harm.	

The likelihood of harm resulting is increased because the breach was the result of malicious action of an unknown third party (deliberate intrusion and fraudulent redemption of points). The information was potentially exposed for over a month. While there is evidence of financial fraud and theft being the motive, this does not abrogate the possibility that malicious actors would use the information for spear phishing purposes.

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).

I understand the Organization reported that "Attempts to contact impacted customers with telephone numbers occurred as the incident unfolded….Impacted customers are being notified in writing by email or direct mail."

I require the Organization to confirm to my office within ten (10) days of the date of this decision that affected individuals in Alberta have been notified in compliance with the Regulation.

Jill Clayton
Information and Privacy Commissioner