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	Fossil Group, Inc. (Organization)
Decision number (file number)	P2019-ND-183 (File #013530)
Date notice received by OIPC	July 23, 2019
Date Organization last provided information	July 23, 2019
Date of decision	December 10, 2019
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"	Information involved in the breach included: • name, • address, • telephone number, • email address, • account username and password, and • payment card information number, expiry date and security codes). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website, Misfit.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization reported it believes an unauthorized third party placed malicious-code on its Misfit.com website, enabling an unauthorized party to obtain certain information pertaining to website users. • The Organization reported the breach occurred on May 14, 2019. It was discovered on June 18, 2019 by a security researcher who alerted the Organization that an unauthorized third party may have obtained certain information pertaining to website users.
Affected individuals	The incident affected 1,393 individuals, four of which are in Alberta.
Steps taken to reduce risk of harm to individuals	• Blocked the malicious code and took the website offline. • Engaged a third-party security expert to investigate. • Contacted U.S. law enforcement authorities. • Requiring users whose account passwords were affected to reset their passwords • Took steps to reduce the risk of a similar event occurring in the future, including blocking the malicious code and rotating administrator credentials to the site.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on July 23, 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 reported it "…believes the relevant issue could possibly give rise to the risk of identity theft, financial fraud and other misuse of personal information." I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. 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 said it "…believes an unauthorized third party obtained certain personal information of some Misfit.com users…". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate unauthorized access and malicious code). The information may have been exposed for over 1 month.

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 financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate unauthorized access and malicious code). The information may have been exposed for over 1 month. 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 affected individuals were notified by mail on July 23, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner