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	TeenSafe (Organization)
Decision number (file number)	P2019-ND-088 (File #008844)
Date notice received by OIPC	June 1, 2018
Date Organization last provided information	February 26, 2019
Date of decision	June 26, 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 individual 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: • Apple ID and associated password (for user); • email address (for the parent user); and • account names and device names (for larger groups of users). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• For certain time periods between February 1, 2018 and May 19, 2018, personal information about users on the Organization's application server was publicly accessible. • Although the server was not generally known outside the Organization's development team, the breach was identified by a reporter who was apparently looking for vulnerabilities in the Organization's systems. • The Organization was made aware of the issue on May 18, 2018.

	• The Organization reported that it has no evidence that the information was viewed or accessed by anyone other than the reporter.
Affected individuals	The incident affected one (1) individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Server is no longer available outside of the Organization. • Notified those users whose passwords were viewable to change their passwords.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by email on May 19, 2018.
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 "Access to an Apple ID and password may permit access to that user's Apple account" and "Access to an Apple account could permit access to additional information about the user and/or make purchases. The password may also be reused on other accounts. No significant harm arises from access to email addresses, which are frequently publicly available." In my view, a reasonable person would consider that email addresses and credentials could be used to compromise other online accounts and for phishing, resulting in increased 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 reported that "Harm is unlikely. There was one password for an Alberta user among over 300,000 lines of text, of which only 10, 000 lines were visible at any one time. Even if any unauthorized actor had accessed the server, of which there in no evidence except for the reporter that contacted Teensafe, it is unlikely they would have been able to access the Albertan's information." In my view, the likelihood of harm resulting from this incident is increased because the personal information was viewable on the Organization's server for approximately four months. The Organization is aware that a third party accessed the information, and has not provided any assurances that no one else accessed the information. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft, fraud and phishing attempts can occur months and even years after a data breach.

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 and credentials could be used to compromise other online accounts and for phishing, resulting in increased vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was viewable on the Organization's server for approximately four months. The Organization is aware that a third party accessed the information, and has not provided any assurances that no one else accessed the information. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft, fraud and phishing attempts can occur months and even years after a data breach. I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individual in an email on May 19, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner