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	500px Inc. (Organization)
Decision number (file number)	P2019-ND-115 (File #011111)
Date notice received by OIPC	February 14, 2019
Date Organization last provided information	February 14, 2019
Date of decision	July 31, 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"	The incident may have involved the following information: • first and last name, • username associated with, • email address associated with account, • hashed password, • date of birth, if provided • city, state/province, country, if provided • gender, if provided. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 8, 2019, the Organization became aware that someone was offering to sell the Organization's user data on the dark web. A sample of user account data provided, appeared to be genuine. • That same day, the Organization's engineering team confirmed a potential security issue affecting approximately 14.8 million 500px user accounts. • Based on its investigation, the Organization believes that an unauthorized party gained access to its systems and acquired certain user data on approximately July 5, 2018.
Affected individuals	The incident affected approximately 14.8 million user accounts, including less than 5,000 in Alberta.
Steps taken to reduce risk of harm to individuals	• Launched a comprehensive review of systems and engaged a third-party expert to assist in the investigation. • Implemented system-wide password reset and forced reset of certain passwords. Requiring all users to reset their account passwords. • Vetted and modified access to servers, databases, and other sensitive data-storage services. • Auditing all source code to ensure no remaining security issues. • Taking steps to further secure website, mobile apps, internal systems, and security process. • Modifying internal software development process. • Reported to data protection authorities, and law enforcement.
Steps taken to notify individuals of the incident	All affected individuals were notified by email beginning February 11, 2019 and expected to be completed by February 15, 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: *Given the nature of the personal data involved, the matter could lead to phishing or spam or other misuse of the affected personal data.* *In addition, if a user had not changed his or her password on 500px since October 2012, there is a risk that, due to the hashing algorithm used at that time, the user's hashed password could be reverse-engineered to allow an unauthorized party to compromise his or her 500px account. This risk affected only a small percentage of users' hashed passwords. We have alerted the relevant users about this risk and taken steps to protect their accounts.*

	At this time, we have no indication of unauthorized access to the affected accounts. I agree with the Organization's assessment that a reasonable person would consider that the contact and identity information at issue could be used for identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Given the information provided by the Organization, credentials could be used to compromise affected accounts, and possibly other online accounts. These are all 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 "At this time, there is no indication of unauthorized access to any of the accounts, and no evidence that other data associated with the user profiles was affected, such as credit card information (which is not stored on our servers) or any other sensitive personal information." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and theft of personal information. The information was available for sale on the dark web. The incident was not detected for approximately 7 months.

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 identity information at issue could be used for identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Given the information provided by the Organization, credentials could be used to compromise affected accounts, and possibly other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and theft of personal information. The information was available for sale on the dark web. The incident was not detected for approximately 7 months.

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 that all affected individuals were notified by email between February 11 and 15, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner