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	Dubsmash Inc. and Mobile Motion GmbH (collectively, Dubsmash) (Organization)
Decision number (file number)	P2020-ND-089 (File #012185)
Date notice received by OIPC	February 27, 2019
Date Organization last provided information	August 2, 2019
Date of decision	July 28, 2020
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: • public username, • encrypted password, • date of birth, • telephone number, • email address, and • country/language information. 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 in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization is a video messaging application for iOS and Android. • On February 8, 2019, a reporter contacted the Organization to request comment on the sale of potentially stolen information. • The Organization investigated to determine whether there had been any unauthorized acquisition of its users' personal information. • On February 11, 2019, the Organization purchased a database from an unidentified individual and confirmed that it contained information related to the Organization's users. • The Organization reported its investigation had not revealed a vulnerability that led to the information being compromised.
Affected individuals	The Organization identified 161,545,815 user email addresses which may have been affected by the incident. The Organization said it is not known how many Alberta residents were affected by the incident.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Provided information about the incident to media. • Strengthening security measures and ensuring networks and systems are secure. • Performed a comprehensive investigation though a digital forensic firm including access controls, account reviews, rights management programs, logs, potential past intrusions, server and workstations reviews, personal devices of staff, user privilege/access entitlement, account creation, and malware identification.
Steps taken to notify individuals of the incident	On February 14, 2019, the Organization notified its users by providing a public notice of the incident on its website and pushed a notification to users via the mobile application with a link to the website to inform them of the incident.
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 any harm that might result from this incident. In my view, a reasonable person would consider that contact and identity information could be used to cause the significant harms of fraud and identity theft. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts.

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 that significant harm would result from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and/or unauthorized third party). Organization purchased the database containing the users' personal information but it remains unclear whether other copies of the information still exist.

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 contact and identity information could be used to cause the significant harms of fraud and identity theft. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts.

The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and/or unauthorized third party). Organization purchased the database containing the users' personal information but it remains unclear whether other copies of the information still exist.

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, on February 14, 2019, the Organization notified its users by providing a public notice of the incident on its website and pushed a notification to users via the mobile application with a link to the website to inform them of the incident. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner