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	Marin Software Incorporated (Organization)
Decision number (file number)	P2017-ND-32 (File #004881)
Date notice received by OIPC	February 1 ,2017
Date Organization last provided information	February 1, 2017
Date of decision	February 21, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates out of San Francisco, California, and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • home address, • business and personal email address, • social security number (SSN), • date of birth, • employment information, including role, title, salary, dates of employment, and • draft W-2 forms. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected from a resident of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On January 20, 2017, an unauthorized individual sent an email requesting employee payroll information and 2016 W-2 forms. The email appeared to have been sent by an Executive with the Organization. • In response, a payroll employee with the Organization created a spreadsheet report and provided it, via email, to the requestor. • The incident was discovered on January 24, 2017.
Affected individuals	A total of 795 individuals were affected, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement (FBI) and the Tax Division of the United States Attorney's Office for the Northern District of California. • Will file complaint with the Internet Crime Complaint Center. • Requiring employees to take mandatory training on email scams. • Will implement additional internal protocols for responding to requests for sensitive personal information • Evaluating data security systems.
Steps taken to notify individuals of the incident	Affected individuals were notified about the incident on January 25 and 26, 2017.
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 but did provide affected individuals with information to protect themselves from identity theft and tax refund fraud. In my view, the identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud, including tax refund 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 did not specifically assess the likelihood of harm resulting from this incident but did advise affected individuals that "You may also consider taking measures to protect yourself against tax refund fraud, which has increased in recent years." In my view, the likelihood of harm resulting from this incident is increased as it resulted from malicious intent (deliberate action to send spear phishing emails to obtain personal information). The unauthorized recipients are unknown and the information has not been recovered.

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 individual. The identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud, including tax refund fraud. The likelihood of harm resulting from this incident is increased as it resulted from malicious intent (deliberate action to send spear phishing emails to obtain personal information). The unauthorized recipients are unknown and the information has not been recovered. 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 all affected individuals in accordance with the Regulation on January 25 and 26, 2017. The Organization is, therefore not required to do so again.

Jill Clayton
Information and Privacy Commissioner