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	Sunrise Medical Canada Inc. (Organization)
Decision number (file number)	P2016-ND-33 (File #000419)
Date notice received by OIPC	March 12, 2015
Date Organization last provided information	March 12, 2015
Date of decision	June 21, 2016
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 is incorporated in Ontario 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 the following information: • name, • address, • date of birth, • social insurance number, and • salary. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 15, 2015, thieves threw a rock through a ground floor window of the Organization's North American headquarters, located in Fresno California, USA. The thieves stole a laptop belonging to the Human Resources department, which contained the personal information at issue. The thieves fled the scene before law enforcement could arrive in response to the security alarm. • The Organization reported the laptop was password protected but not encrypted. • Local police were informed of the theft. The laptop has not been recovered.
Affected individuals	One individual in Alberta.
Steps taken to reduce risk of harm to individuals	• Credit monitoring services for one year were offered to the affected individual as well as guidance on how to monitor personal information, such as bank accounts, credit cards and other financial transaction statements. • Reported to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	Notification sent to affected individual by email and letter on February 16, 2015.
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 the thieves could potentially use the information to commit identity theft. I agree with the Organization. The personal information involved includes identity information which could be used to cause the harms of 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 the risk of harm resulting from this incident is "material, but not high." The Organization reported that laptops are commonly stolen for their resale value, and not the information stored on them, and noted that the laptop was not identified as belonging to the Human Resources Department, and was protected with a strong password. In my view, there is a real risk of harm resulting from this incident. The personal information was stored on a laptop that was stolen, indicating malicious intent. Further, the laptop was not encrypted, increasing the possibility the information may be

	accessed. I am not persuaded by the Organization's argument that the risk of harm is not high because the theft was for the value of the laptop. The Organization cannot know the intent of the thief or the intent of those who may ultimately end up in possession of the laptop.

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 personal information involved includes identity information which could be used to cause the significant harms of identity theft and fraud. The personal information was stored on a laptop that was stolen, indicating malicious intent. The laptop was not encrypted, increasing the possibility the information may be accessed. The Organization cannot know the intent of the thief or the intent of those who may ultimately end up in possession of the laptop.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual in accordance with the Regulation by email and letter on February 16, 2015. The Organization is, therefore not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner