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	J.M. Smucker (Organization)
Decision number (file number)	P2014-ND-18 (File #P2700)
Date notice received by OIPC	February 28, 2014
Date Organization last provided information	July 4, 2014
Date of decision	November 12, 2014
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify that individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA. The Organization reported that an Alberta billing address was used to place an order via its online system. It is likely the source of transmission of the information is Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • email address, • telephone number, • credit card number, • credit card expiration date, • credit card verification code. This information is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization's online ordering and billing system was compromised by malware. • The Organization reported that the system was compromised on December 23, 2012. Personal information in the system was exposed for approximately 14 months (between December 2012 and January 2014). • The Organization was made aware of the breach when it was notified by the United States Federal Bureau of Investigation on February 12, 2014.
Affected individuals	One individual from Alberta was affected.
Steps taken to reduce risk of harm to individuals	• The compromised system was retired. • A security vulnerability assessment was performed on the new system.
Steps taken to notify individuals of the incident	A written notification was sent to the individuals affected by the incident.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 recognized the affected individuals may be at risk of harm. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to the personal and financial information in this instance are identity theft, financial loss and/or 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 due to the sensitivity of the personal information involved there is a real risk of significant harm to the affected individual. In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed by an unauthorized individual with malicious intent. In addition, the information was exposed for 14 months (from December 2012 to February 2014) before the Organization was made aware the system had been compromised.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization, I have decided that there is a real risk of significant harm to the affected individual. The personal information involved is highly sensitive and could be used to cause identity theft, financial loss and/or fraud. The incident was the result of malicious intent and the personal information was exposed for approximately 14 months. These factors contributed significantly to my decision. 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. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner