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	Auburn University (Organization)
Decision number (file number)	P2015-ND-79 (File #P2642)
Date notice received by OIPC	April 3, 2014
Date Organization last provided information	April 11, 2014
Date of decision	December 23, 2015
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 the state of Alabama, U.S.A. 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, • Social Security Number. 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	One of the Organization's servers was compromised, resulting in unauthorized access to personal information stored on it.
Affected individuals	One (1) individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Vulnerability on server patched and investigation launched. • Retained specialized data security counsel to assist with the investigation. • Hired independent, third-party forensics experts to assess the extent of data potentially exposed. • Offered one free year of credit monitoring services and identity restoration services. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta (OIPC).
Steps taken to notify individuals of the incident	Notification sent by mail on March 20, 2014.
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.	In its report to the OIPC, the Organization did not specifically assess the harm that could result from this incident. However, the notification sent to the affected individual provided information for protecting oneself from identity theft, fraud and financial loss. In my view, the personal information involved is sensitive and could be used to cause the harms of identity theft, fraud and financial loss. 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.	In its report to the OIPC, the Organization did not specifically assess the likelihood of harm resulting from this incident. The notification sent to the affected individual advised of "an incident that may affect the security of your personal information," although the Organization is "unaware of any attempted or actual misuse of your personal information" In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization confirmed the information at issue was stored on the compromised server.

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 is sensitive and could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization confirmed the information at issue was stored on the compromised server. 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 a letter dated March 20, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner