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	Scott Builders Inc. (Organization)
Decision number (file number)	P2017-ND-23 (File #001960)
Date notice received by OIPC	December 9, 2015
Date Organization last provided information	January 25, 2016
Date of decision	January 30, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals 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 Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • address, • telephone number, • Social Insurance Number, • financial, and • medical information. This information is about identifiable individuals 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 December 7, 2015, the Organization discovered an unauthorized user was logged on to its web-based computer system and was in the payroll auto deposit module. • The incident was discovered when the number of program licenses was exceeded and accounting personnel attempted to gain access and noticed an unfamiliar name.
Affected individuals	The incident affected 96 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately locked out the unauthorized user and shut down external access. • Contacted software provider and initiated investigation. • Users were asked to change passwords. • Reported incident to RCMP. • Introduced more rigorous technical security controls.
Steps taken to notify individuals of the incident	Notified all current and former employees starting December 8, 2015.
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 assessing the type of harm that could result from this incident, the Organization reported "potential financial loss, fraud, identity theft, negative effects on credit record. Highly sensitive unauthorized access to payroll and HR records." I agree with the Organization's assessment. The information at issue includes sensitive identity, financial and health information. This information could be used to cause the harms of identity theft, fraud, hurt, humiliation, embarrassment, and negative effects on credit record. 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 the unauthorized individual has not been identified and "we don't know whether this person only saw information or kept a file/pictures/printed etc.". In my view, the likelihood of harm is increased as the breach was the result of malicious intent (deliberate intrusion). The perpetrator has not been identified and the Organization has not been able to confirm whether the information was copied, printed or forwarded. 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 individuals as a result of this incident. The information at issue includes sensitive identity, financial and health information. This information could be used to cause the significant harms of identity theft, fraud, hurt, humiliation, embarrassment, and negative effects on credit record. The likelihood of harm is increased as the breach was the result of malicious intent (deliberate intrusion). The perpetrator has not been identified and the Organization has not been able to confirm whether the information was copied, printed or forwarded. The information has not been recovered. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified all current and former employees by email starting December 8, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner