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	Peace Hills General Insurance Company (Organization)
Decision number (file number)	P2018-ND-47 (File #007853)
Date notice received by OIPC	February 20, 2018
Date Organization last provided information	March 23, 2018
Date of decision	April 9, 2018
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 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, • address(es), • social insurance number, • date of birth, • signature, • telephone number, • income tax records, • Alberta Health Care Number, • medical information, • bank records, and • correspondence regarding trial date and incarceration. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On January 23, 2018, internal mail intended for a branch office employee was inadvertently sent to an unauthorized recipient. • The Organization reported that "This mail was in a brown window envelope box and contained personal information of an individual involved in a claim with [the Organization]. This was caused by human error whereby the complete address was not indicated on mail which left [the Organization's] office." • The mail was placed in a courier bag, picked up by a courier service's driver and delivered to their local distribution centre "…who opened [the] box once it recognized the mailing address was incomplete." • The courier service recognized the name of an insurance company, and re-directed the mail accordingly. The insurance company happened to be dealing with the same client (the affected individual). An employee with the insurance company opened the box before realizing it was not intended for the insurance company. • The insurance company employee reported the matter to the Organization on January 31, 2018. The box was received by the intended recipient on February 2, 2018. • The Organization reported that it appeared all the contents were received and nothing was tampered with.
Affected individuals	The incident affected one (1) individual from Alberta.
Steps taken to reduce risk of harm to individuals	• The information was recovered. • Staff will be reminded to review outgoing mail for complete addresses.
Steps taken to notify individuals of the incident	The affected individual was notified of the breach by telephone on March 22, 2018.
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 information could be used to cause the possible harms of "…financial fraud/identity theft due to breach of individual's name, date of birth, social insurance numbers, signature, Alberta Health Care number, tax records, etc. Possible humiliation due to trial/incarceration correspondence." I agree with the Organization's assessment. The contact and identity information at issue, particularly in conjunction with financial, medical, and legal information, could be used to cause the harms of identity theft and fraud. Financial, legal and medical information could also be used to cause the harms of hurt, humiliation and embarrassment. These are all 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 "…it is unlikely that "real risk of significant harm" could result out of this occurrence. This was an isolated situation caused by human error. While some of the information was of a sensitive nature and could be used for criminal purposes, it was redirected to and received by our employee "X", as intended. There was no evidence that tampering had occurred with this box, aside from opening it. The courier company redirected the box to Company "Y" and Company "Y's" employee contacted our employee right away to determine if they were awaiting these documents. Company "Y's" employee acted quickly and is in the same industry, therefore, would understand the importance of looking no further at these documents. All information appears to be recovered and affected a single individual, whose lawyer has been accordingly advised." In my view, a number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the unintended recipient reported the breach to the Organization, and the mail contents were returned to the Organization. Nonetheless, considering the sensitivity of the information at issue and that there is a professional relationship between the affected individual and the unintended recipient, I find that there is a real risk of the significant harms of hurt, humiliation and embarrassment.

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 contact and identity information at issue, particularly in conjunction with financial, medical, and legal information, could be used to cause the harms of identity theft and fraud. Financial, legal and medical information could also be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms. A number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the unintended recipient reported the breach to the Organization, and the mail contents were returned to the Organization. Nonetheless, considering the sensitivity of the information at issue and that there is a professional relationship between the affected individual and the unintended recipient, I find that there is a real risk of the significant harms of hurt, humiliation and embarrassment.

The Organization is required to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that the affected individual was notified of the breach by telephone on March 22, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner