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	Co-operators General Insurance Company and Co-operators Life Insurance Company (the Organization)
Decision number (file number)	P2020-ND-143 (File #014694)
Date notice received by OIPC	December 13, 2019
Date Organization last provided information	December 13, 2019
Date of decision	November 6, 2020
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • credit card number, • name on credit card, • CSV number. Information included in a client spreadsheet included: • name of policy owner, • name of others associated with the policy, • address, • telephone number, • email address, • policy type, premium amounts, policy numbers, renewal dates, policy limits and deductible amounts. This information is about identifiable individuals 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 November 18, 2019, the Organization was notified by a client that their credit card number had been used to make a fraudulent premium payment. • The Organization investigated and found that the client's credit card number was likely used by a former employee to fraudulently pay the premium on the former employee's insurance policy. The former employee had previously held the role of insurance agent, but his employment had been terminated on July 19, 2018. • Upon further investigation the Organization determined that there were a 6 separate attempts between October and December to use unique credit card numbers to make premium payments on the former employee's insurance policy. Of those 6 attempts, 2 involved the credit card numbers of clients of the Organization, and 1 involved the credit card number of a partner of a client. Four (4) attempts were successful. • The Organization has not been able to definitively conclude whether the former employee used the credit card information of others, but confirms there has been a loss of and unauthorized use of client personal information. • Prior to these events, and immediately following the termination of the former employee, the Organization was aware that the former employee may have been soliciting the Organization's clients. On August 27, 2018, the Organization's internal investigation found that the former employee had emailed a spreadsheet containing client information to his own personal email account on July 18, 2018, and on 4 other occasions between March 1, 2017 and May 22, 2018.
Affected individuals	The Organization reported that up to 2,800 individuals may be affected.
Steps taken to reduce risk of harm to individuals	Demanded the former employee return or destroy all confidential information and immediately cease and desist from soliciting the clients of the Organization. The former employee confirmed in an email dated August 29, 2018 that he had not retained any information. The Organization now questions this confirmation.
Steps taken to notify individuals of the incident	The Organization reported it "will be sending notice via mail to the affected clients on December 17, 2019".

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 "The credit card information could be used in a fraudulent manner. This may result in direct out-of-pocket expenses for the affected individauls [sic], or indirect financial harm, such as a degradation of credit score. The contact information contained within the client spreadsheet could be used in a number of harmful ways, including to perpetrate fraudulent activities such as phishing." I agree with the Organization's assessment. A reasonable person would consider the financial information at issue could be used to cause the harms of identity theft and fraud. Insurance information, particularly when associated with email address, could be used for phishing purposes, increasing vulnerability to 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: *We have no concrete evidence that credit card information of our clients was taken by the former employee. However, given that client credit information is involved, and has already been used in a manner that could have caused harm, to the extent that the credit card information was taken by the former employee, we consider the likelihood that harm will result to be high for the 2 clients and 1 partner of our client who's credit card information was used inappropriately.* *We are not aware of any use of the information contained in the spreadsheets by the former employee. However, given the possibility that the former employee was involved in fraudulent activities as described above, we consider the likelihood that harm will result to be medium.* In my view, a reasonable person would consider the risk of harm is increased as the incidents appear to be the result of deliberate, malicious action and resulted in fraudulent activity.
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. A reasonable person would consider the financial information at issue could be used to cause the harms of identity theft and fraud. Insurance information, particularly when associated with email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.	

The risk of harm is increased as the incidents appear to be the result of deliberate, malicious action and resulted in fraudulent activity.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization reported it "will be sending notice via mail to the affected clients on December 17, 2019". **I require the Organization to confirm in writing, within 10 days of the date of this decision, that the affected individuals whose personal information was collected in Alberta, were notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner