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	Credit Union Central Alberta Ltd. (Organization)
Decision number (file number)	P2015-ND-16 (Case File #000160)
Date notice received by OIPC	January 26, 2015
Date Organization last provided information	March 23, 2015
Date of decision	April 23, 2015
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. I have jurisdiction because 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 the following information: • name, • telephone number, • home address, • date of birth, • Social Insurance Number (SIN), • driver's license number, • credit card number, • bank account number, • email address, • disciplinary records including employee harassment, • employment references, • performance evaluations, • benefits information,

	• income/salary, • medical information. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• During an office renovation, 57 boxes of paper records containing the personal information at issue were stored in an unlocked basement room between October 2014 and January 19, 2015. • The incident was discovered during an annual compliance review of the Organization's controls on January 16, 2015. • The Organization's Chief Governance & Compliance Officer was notified of the incident on January 19, 2015. • The unlocked room containing the information was accessible to 258 employees of the Organization and other entities operating within the same facility.
Affected individuals	A total of 2655 individuals were potentially affected, including current and previous employees of the Organization and credit union members.
Steps taken to reduce risk of harm to individuals	• The boxes were immediately moved to a room with locked doors. Access to the room was restricted to a limited number of individuals. • The Organization's Internal Audit, an independent oversight unit, conducted an inventory of the records. • A risk assessment was conducted to determine the impact of potential unauthorized access to personal information for the affected individuals. • An investigation was conducted. • The Organization committed to develop mandatory organization-wide privacy training by June 30, 2015. The training will be administered to all employees of the Organization. The Organization reported that steps will be taken to ensure all employees take annual refresher training. • A total of 64 credit unions in Alberta and Saskatchewan were potentially affected and were notified. • The Office of the Superintendent of Financial Institutions and Alberta Treasury Board and Finance were notified on January 22, 2015.

Steps taken to notify individuals of the incident	The Organization reported on March 17, 2015 that all current and previous employees were notified.
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 affected individuals may be at risk of identity theft, fraud, humiliation or damage to reputation. The Organization identified information in 39 boxes as being highly sensitive (name, SIN, credit card number, date of birth, benefits, salary, garnishment information, compensation, termination and disciplinary records). One (1) box contained internal audit reports and was identified as medium risk. Seventeen (17) boxes contained information of low sensitivity (name, address, home telephone number, and account number). I agree with the Organization that the types of harm that could result from unauthorized access to this information are identity theft, fraud, hurt, humiliation, embarrassment and/or damage to reputation. In my view, 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 assessed the likelihood of harm in this case as low because of the remote location of the records, and the limited number of individuals who could have accessed the records. The Organization noted that the general public does not have access to the area of the building where the records were stored, the incident did not result from malicious intent, and the Organization is not aware of any theft or misappropriation of the records. In my view, the likelihood of harm resulting from this incident is increased because of the length of time the personal information was unsecured (approximately 4 months). Although the incident was not the result of malicious intent, the Organization reported that 258 individuals potentially had access to the unlocked room. Further, the Organization could not confirm that the room and records had not been accessed during this period.

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 affected individuals. I agree with the Organization that the personal information at issue could be used to cause identity theft, fraud, hurt, humiliation, embarrassment and/or damage to reputation. In my view, these are significant harms. The likelihood of harm resulting from this incident is increased because of the length of time the personal information was unsecured (approximately 4 months). Although the incident was not the result of malicious intent, the Organization reported that 258 individuals potentially had access to the unlocked room. Further, the Organization could not confirm that the room and records had not been accessed during this period. These factors contributed significantly to my decision. I understand the Organization notified all current and previous employees affected by the incident in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner