



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Credential Securities Inc. (Organization)
Decision number (file number)	P2015-ND-06 (File #P2837)
Date notice received by OIPC	August 28, 2014
Date Organization last provided information	February 2, 2015
Date of decision	February 24, 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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	<p>The Organization is incorporated in Alberta as an extra-provincial corporation.</p> <p>I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.</p>
Section 1(1)(k) of PIPA “personal information”	<p>The following information was involved in this incident:</p> <ul style="list-style-type: none">• name,• address,• telephone number,• Social Insurance Number (SIN),• banking information (including account number, institution, assets),• date of birth,• driver’s licence number. <p>This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.</p>

DESCRIPTION OF INCIDENT

loss unauthorized access unauthorized disclosure

<p>Description of incident</p>	<ul style="list-style-type: none"> • On August 22, 2014, the Organization was contacted by a client who advised he had received an email from a third party who had purchased filing cabinets from an auction house in Vancouver that contained a file with his information. • The Organization contacted the third party, and was told that 40 client files were found in the filing cabinet. The third party had emailed or called all 40 clients to inform them the files had been found. • The Organization immediately retrieved the files from the third party. • The Organization determined the filing cabinets had been sold to an auction house in September 2013 and the third party purchased 10 filing cabinets in November 2013. • The third party stored the filing cabinets in a locked facility until May 2014 at which point the third party discovered the files. • The Organization determined that a total of 67 files had been left in the bottom of the filing cabinet drawer. • The third party had shredded 1 file at the request of the client.
<p>Affected individuals</p>	<p>16 Albertans were affected by the incident.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • All employees received mandatory privacy training in September 2014. • Any employees who have more contact with client information will receive a full day of privacy training. • All clients with accounts were provided a new account number that is password protected. A note was placed on the affected accounts to monitor for abnormal activity. • The Organization offered credit support services to affected individuals.
<p>Steps taken to notify individuals of the incident</p>	<ul style="list-style-type: none"> • The Organization reviewed the contents of the files retrieved from the third party. • The Organization carried out a 411 search for individuals whose information was not current. • The Organization contacted their credit union partners to try to obtain current contact information. • Affected individuals were notified by telephone and email beginning August 25, 2014.

	<ul style="list-style-type: none"> • Of the 16 affected Albertans: <ul style="list-style-type: none"> ○ 9 were contacted successfully, ○ 5 could not be contacted, and ○ 2 did not respond to the email correspondence.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization recognized the affected individuals may be at risk of identity theft and fraud.</p> <p>In my view, the personal information involved is very sensitive. It includes name, address phone number, SIN, bank details, date of birth and driver’s licence number. The types of harm that could be caused as a result of this incident include identity theft or fraud. In my view, these are significant harms.</p>
<p>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.</p>	<p>The Organization assessed the likelihood of harm to individuals resulting from this breach as medium to low.</p> <p>I believe there is a real risk of harm resulting from this incident. Although the third party confirmed the filing cabinet was securely locked away from November 2013 until May 2014, it is not known if the filing cabinet was accessed by anyone between September 2013 and November 2013 when the auction took place.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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. The personal information involved includes name, address, telephone number, Social Insurance Number (SIN), banking information, date of birth and driver’s licence number and could be used to cause the significant harms of identity theft or fraud. Although the third party confirmed the filing cabinet was securely locked away from November 2013 until May 2014, it is not known if the filing cabinet was accessed by anyone between September 2013 and November 2013.</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization began notifying affected individuals via phone and email on August 25, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner