



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Servus Credit Union Ltd. (the Organization)
Decision number (file number)	P2015-ND-05 (File #P2886)
Date notice received by OIPC	October 14, 2014
Date Organization last provided information	December 19, 2014
Date of decision	January 26, 2015
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 <i>Personal Information Protection Act</i> (PIPA). As the Organization has already notified the individual, no further notification is required.
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 and the incident occurred in Alberta.
Section 1(1)(k) of PIPA “personal information”	The incident involved all or some of the following information about the individual: <ul style="list-style-type: none">• name;• address;• details and results of an internal investigation of the employee, including the decision to terminate the employee. This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none"> • A Human Resources manager emailed a letter to an employee at the employee’s request. The letter contained the results of an internal investigation of the employee and advised of the decision to terminate the employee. • The email was sent to the wrong email address. • The email was not encrypted. • The Organization became aware of the privacy breach shortly after transmission but efforts to recall the message failed and the Organization was unable to confirm that the email had been destroyed.
Affected individuals	1 employee
Steps taken to reduce risk of harm to individuals	The Organization has an information security policy that requires that files containing confidential information must not be transmitted via email unless encrypted.
Steps taken to notify individuals of the incident	<ul style="list-style-type: none"> • The Organization discovered the breach the same day when the HR manager telephoned the employee to confirm receipt of the email. • The Organization subsequently notified the affected individual by letter.
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.	<p>The Organization recognized the affected individual may be at risk for humiliation and reputational harm.</p> <p>In my view, the personal information involved is highly sensitive. It contains information about an investigation of the individual and of the Organization’s decision to terminate the individual. The types of harm that could result from unauthorized access to the personal information in this instance are humiliation and reputational harm. 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 reported that due to the sensitivity of the personal information involved and the inability of the Organization to retrieve the information or confirm the email had been deleted, it considered there to be a real risk of significant harm to the affected individual.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information has not been recovered and the Organization has been unable to confirm the email was deleted and not disclosed further.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<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 individual. The personal information involves sensitive information which could be used to cause significant harm in the form of humiliation and harm to reputation. The Organization has not been able to retrieve the information, nor to confirm the email was deleted and not disclosed further. These factors contributed significantly to my decision.</p> <p>I require the Organization to notify the affected individual in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individual by letter dated November 27, 2014 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.</p>	

Jill Clayton
Information and Privacy Commissioner