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	The Legal Aid Society of Alberta (Organization)
Decision number (file number)	2017-ND-87 (File # 005786)
Date notice received by OIPC	June 2, 2017
Date Organization last provided information	June 20, 2017
Date of decision	June 29, 2017
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 56 of PIPA "non-profit organization"	The Organization is incorporated under Alberta's *Societies Act* and is a "non-profit-organization" as defined in section 56(1)(b)(i) of PIPA. Under sections 56(2) and (3), PIPA only applies to personal information that is collected, used or disclosed by non-profit organizations in connection with a commercial activity. In this case, the personal information at issue was collected and stored in an information system that is used to arrange for legal aid services to be provided by lawyers in private practice. In Decision P2013-D-01, an Adjudicator with my Office found [at paragraph 37] that the Organization "…carries out a commercial activity when it assesses individuals for legal aid coverage, arranges for legal aid services to be provided by lawyers in private practice, and provides legal aid services through its staff lawyers. Further, this is the case whether or not the individual pays or partly pays for the services." I have jurisdiction because the information at issue was collected in connection with a commercial activity, as contemplated in section 56(3) of PIPA.

Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • name of bank, branch address, financial institution number, transit number, bank account number, and • amount to be debited from client's account. 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 April 11, 2017 an employee of the Organization received a completed Pre-Authorized Contribution form from a client. The form provides consent to withdraw an agreed payment amount from a client's account, and included the personal information at issue. • That same day, an employee of the Organization inadvertently included the form in an email sent to another client. • The unintended recipient contacted the Organization on April 13, 2017 to report the incident. • The Organization contacted the unintended recipient and advised them to permanently delete the record. However, to date, the Organization has been unable to confirm this was done.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Contacted the unintended recipient and advised them to permanently delete the record. • Followed up with the employee who sent the information and the employee attended privacy training.
Steps taken to notify individuals of the incident	The affected individual was notified by letter to her last known address on May 11, 2017.

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 risk to this client is financial in nature including fraud, identity theft and/or negative effects on a credit record if Client B were to use this information in an inappropriate manner." I agree with the Organization. The identity and financial information at issue could be used to cause the harms of identity theft, fraud and negative effects on a credit record. 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 the likelihood of harm resulting from this incident as low because: • The information was exposed to only one individual who reported the incident to the Organization, and whose tone indicated she was sympathetic to the affected individual's information being erroneously disclosed. • The unintended recipient had applied to the Organization for family matters, and not criminal matters. • The incident occurred as a result of human error and not malicious intent. In my view, the likelihood of harm resulting from this incident is reduced because the incident resulted from human error rather than malicious intent, and the unintended recipient reported the matter to the Organization. However, although the Organization reported that it had followed up with the unintended recipient to request that the information be deleted, the Organization has not, to date, been able to confirm this was done.

DECISION UNDER SECTION 37.1(1) OF PIPA
Given the information reported by the Organization, and considering the circumstances, I have concluded that there is a real risk of harm in this case. The identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. The likelihood of harm resulting from this incident is reduced because the incident resulted from human error rather than malicious intent, and the unintended recipient reported the matter to the Organization. However, although the Organization reported that it had followed up with the unintended recipient to request that the information be deleted, the Organization has not, to date, been able to confirm this was done.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by letter dated May 11, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner