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	Legal Aid Alberta (Organization)
Decision number (file number)	P2019-ND-045 (File #010241)
Date notice received by OIPC	November 9, 2018
Date Organization last provided information	November 28, 2018
Date of decision	March 5, 2019
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 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. Pursuant to section 56(1)(a) of PIPA, a commercial activity is any transaction, act, conduct or regular course of conduct that is of a commercial character. 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 Organization reported "As this potential breach is so dated there is little information available that can be confirmed independently in an expedited fashion". However, the Organization also said the employee whose tablet was stolen advised as to the type of information that would have been on the device, including: • client name and email address, • letters advising of upcoming court dates, • notes from meetings with clients, and • details about criminal offences and defence strategy. 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 2, 2015, an employee who was acting as duty counsel at the Courthouse had his tablet stolen. • The information at issue was stored on the tablet. • The Organization does not have any records indicating whether the tablet was encrypted; however, it said the practice at the time would have been to encrypt mobiles and laptop devices and have a strong password. The employee believes the device had encryption software. • The breach was discovered November 2, 2018 as the result of a subsequent theft of a tablet in October 2018.
Affected individuals	The Organization is trying to determine the number of individuals affected by the incident.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the Sheriff at the Courthouse, law enforcement, and an investigation occurred. • Taking steps to identify potential affected individuals. • Reviewing policies relating to laptop and tablet use. • Investigating other data security options including remote wipe capability on all devices. • Providing training to staff on privacy, practice management and data security. • Requested that the Courthouse place locks on rooms utilized by duty counsel.
Steps taken to notify individuals of the incident	The Organization is trying to determine the number of individuals affected by the incident.

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 possible harms that may occur as a result of the breach include: • "Reputational harm and humiliation … by way of the alleged involvement in criminal proceedings", • "Identity theft by way of release of names, email addresses and physical addresses …" I agree with the Organization's assessment. A reasonable person would consider that the legal information at issue could be used to cause the significant harms of hurt, humiliation, embarrassment and reputational damage. In my view, email addresses could be used for phishing purposes.
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 that it "…cannot be confirmed whether or not this Tablet was encrypted. However, it was the practice …at the time to encrypt all laptops and tablets issued to staff". In addition, the tablet was protected by a "strong password". The Organization also reported that "…despite the security measures on the device, malicious intent is present as the device was stolen, it cannot be ascertained whether there was encryption or remote wiping capability and the device was not recovered. On balance it is possible that harm could result." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the tablet has not been recovered. The Organization cannot confirm whether encryption software was installed and used.

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 that the legal information at issue could be used to cause the significant harms of hurt, humiliation, embarrassment and reputational damage. In my view, email addresses could be used for phishing purposes. The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the tablet has not been recovered. The Organization cannot confirm whether encryption software was installed and used.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) **and confirm to my office in writing within ten (10) days of the date of this decision that it has done so.**

Jill Clayton
Information and Privacy Commissioner