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	Belal Najmeddine Professional Corporation o/a Edmonton Law Office (Organization)
Decision number (file number)	P2023-ND-015 (File #028340)
Date notice received by OIPC	December 13, 2022
Date Organization last provided information	February 19, 2023
Date of decision	April 24, 2023
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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is located in Edmonton, Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • mailing address, • email address, • telephone number, • Social Insurance Numbers, • bank statements, • credit card statements, • tax returns, • notices of assessment, • "[email] correspondence on client files," including: content of communication between "clients," "counsellors, lawyers, court officials, clerks," "judge and their assistants," and • email attachments such as court documents (orders, affidavits, etc.). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

	Some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Pursuant to section 4(1)(d) of PIPA, the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the loss / theft of the personal information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, PIPA applies to the personal information about the affected individuals in Alberta. Due to the nature of the Organization, there may be personal information that may be contained in a court file. This personal information is excluded from the application of PIPA under section 4(3)(k).
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 3, 2022, a break-and-enter occurred at the Organization's office. The incident was discovered by police. • The Organization conducted an inventory following the incident; "thieves … stole anythign [sic] that appeared to be of value including computer screens … but most importantly, the law firms [sic] server and back up drive containing information on client files such as correspondence between lawyers and clients. The drives and server are password protected." • In a January 20, 2023, update, the Organization's IT provider advised "the information was not encrypted but only protected by passwords." • "2 of 4 thieves were … arrested," however, the server and backup drive were not recovered.
Affected individuals	The incident affected an estimated "4000 people" in Alberta.
Steps taken to reduce risk of harm to individuals	• Implemented additional technical, administrative, and physical safeguards. • Changed certain information technology practices to reduce risk of re-occurrence.

Steps taken to notify individuals of the incident	"All active clients (approximately 2000)" are being notified by email, telephone, or in-person, beginning on or about December 13, 2022. The Organization submitted a proposal to notify the remaining affected individuals indirectly.
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 on January 20, 2023: *There could be the possibility of identify theft occurring, fraud, but most likely embarrassment, If [sic] anything.* I accept the Organization's assessment. A reasonable person would consider that the identity (name, Social Insurance Number), contact (mailing/email address, telephone number), financial (tax return, notice of assessment, bank/credit card statements) information, and court documents, could be used to cause the harms of identity theft, fraud, embarrassment, hurt or humiliation, and damage to reputation. Email addresses could be used to for the purposes of phishing, increasing the affected individuals' vulnerability to the above. 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 realiity [sic] is that the parties who stole our hardware were unsoffisticated [sic] … . If they were to make any attempt to use the server, they would likely attempt to wipe out the content and sell the hardware at a local pawn shop. I also don't imagine that any of these individuals have the know-how in order to crack through the security on the server and back-up.* *… the server is password protected. We do not believe anyone's private information will be disclosed; … Police have already apprehended 2 of 4 individuals. … the chances that either have the ability to hack into the server are extremely limited.* The Organization added on January 20, 2023: *Nothing has been recovered nor have I heard anything from the police … I am fairly confident the items were likely thrown out in a dumpster and subsequently destroyed. In fact, we located some of our electronics in a dumpster behind the neighbouring building … The risk of that harm occurring is significantly low. …*

	In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised as the result of malicious intent (break-and-enter, theft). The Organization has not recovered the stolen server nor backup drive; the personal information was password protected, but not encrypted.

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.

The identity (name, Social Insurance Number), contact (mailing/email address, telephone number), financial (tax return, notice of assessment, bank/credit card statements) information, and court documents, could be used to cause the harms of identity theft, fraud, embarrassment, hurt or humiliation, and damage to reputation. Email addresses could be used to for the purposes of phishing, increasing the affected individuals' vulnerability to the above. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised as the result of malicious intent (break-and-enter, theft). The Organization has not recovered the stolen server nor backup drive; the personal information was password protected, but not encrypted.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization began notifying "approximately 2000" "active clients" by email, telephone, or in-person, beginning on or about December 13, 2022. The Organization confirmed telephone and in-person notifications meet the requirements of the Regulation, however, a sample of the email notification provided for review did not include a description of the personal information involved in the loss, as required by section 19.1(1)(b)(iii) of the Regulation.

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…", however section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

On February 3, 2023, the Organization submitted reasons for why direct notification to the remaining affected individuals is unreasonable in the circumstances. The Organization proposed indirectly "notifying all potentially affected individuals by including a statement at the bottom of each and every single email … [and] taking out an advertisement in all major newspapers for a 2-4 week period." In this case, I accept that providing direct notification of the incident to certain individuals is unreasonable for the reasons provided in the Organization's submission.

Where contact information for affected individuals is readily available, the Organization is required to notify affected individuals in Alberta in accordance with section 19.1 of the Personal Information Protection Act Regulation (Regulation). The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals whose email notices did not meet the requirements of the Regulation have been provided a supplemental notice, describing the personal information affected in the incident as required in section 19.1(1)(b)(iii) of the Regulation.

I accept the Organization's submission that it is reasonable in the circumstances to indirectly notify the remaining affected individuals whose contact information is not readily available by the means suggested by the Organization's submission.

The Organization may consider attaching a statement informing email recipients of the incident and referring them to a notice that meets the requirements of section 19.1(1) of the Regulations if it has a blog or a website for a period of at least 4 months.

The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that indirect notification as described in their submission above has been issued, in accordance with the requirements outlined in section 19.1(1)(b) of the Regulation.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance