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	Gerald J. Kugelmass Professional Corporation (Organization)
Decision number (file number)	P2019-ND-033 (File #007536)
Date notice received by OIPC	January 17, 2018
Date Organization last provided information	February 14, 2018
Date of decision	February 19, 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 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, • email address, • social insurance number, • driver's licence, and • other personal information contained in solicitor/client communications. 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 January 8, 2018, the Organization was advised by several individuals that they had received an email from the Organization requesting they download a file by clicking on a link. The Organization did not send the email.

	• During the week of January 8, 2018, the Organization's IT consultant advised that the imposter might have had unauthorized access to the Organization's emails. • The Organization reported the intrusion was via the web, not via the local desktop, so the compromise was to the Organization's email account and not to the system itself. The Organization's emails appear to be undisturbed. The IT consultant further advised that nothing else on the computer was accessed and that the system is secure. • The Organization reported that it has received no information that anyone downloaded the file, although one person tried to open the file by clicking on the link provided, but entered the wrong password and did not proceed further. • The Organization is not aware of any loss or misuse of the information to date.
Affected individuals	The incident affected approximately 50 individuals.
Steps taken to reduce risk of harm to individuals	• Took steps to deny the intruder any further access, and advised possible recipients that the email was not from the Organization and should be deleted. • Reported the matter to the Law Society of Alberta. • Changed passwords, scanned computers, and rectified the IT problem (including removing the rule inserted by the imposter to delete inbound emails), and secured the system.
Steps taken to notify individuals of the incident	Affected individuals were notified by emails sent between January 15, 2018 and January 18, 2018, and on February 22, 2018.
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 client information in my emails is largely communications between myself and clients respecting their files. Although there may be some financial information, I believe it to be marginal compared to the other information. It appears that if there was any harm here at all, it would be minimal." In my view, a reasonable person would consider that the email addresses, identity, and legal information at issue could be used to cause the significant harms of identity theft and fraud, as well as for phishing purposes, resulting in increased vulnerability to identity theft and fraud.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a	The Organization reported that that it has "…received no information that anyone downloaded the file" and "…it does not appear that the purpose of the intrusion was to review…email information."

cause and effect relationship between the incident and the possible harm.	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 due to the malicious action of an unknown third party (deliberate intrusion). Further, it is not known how long the intruder had access to the information. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.

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 email addresses, identity, and legal information at issue could be used to cause the significant harms of identity theft and fraud, as well as for phishing purposes, resulting in increased vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, it is not known how long the intruder had access to the information. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.

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). I understand the Organization notified affected individuals in emails sent between January 15, 2018 and January 18, 2018, and on February 22, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner