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	Kahane Law Office (Organization)
Decision number (file number)	P2019-ND-117 (File #010971)
Date notice received by OIPC	November 29, 2018
Date Organization last provided information	November 29, 2018
Date of decision	July 31, 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved "addresses" and "financial information". 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	• The Organization reported that, on August 8, 2018, "An individual accessed metadata in a document that included personal addresses and financial information". • The incident was discovered November 14, 2018 when the individual who accessed the metadata contacted the affected individual directly.
Affected individuals	The incident affected 2 individuals.

Steps taken to reduce risk of harm to individuals	The Organization reported that "A no contact order was obtained which requires all information that was accessed to be destroyed immediately". Further, "The firm is taking steps to ensure all meta data is wiped from any and all documents being sent out of the office."
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email sent November 14, 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 did not identify any potential harms that might result from the incident, and was not specific with regard to the type of information at issue, other than to say that it included "addresses" and "financial information". In the absence of more specific information, I will comment generally that "financial information" often includes the type of information that can be used to cause significant harms such as identity theft and fraud. "Addresses" can include email address, which is often used for phishing purposes, increasing vulnerability to identity theft and fraud. Address may also be used to make unwanted contact with an individual, which may or may not be a significant harm, depending on the circumstances.
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 "There is little likelihood of harm given the court order" and "The no contact order is police enforced, allowing an arrest if the order is breached". The incident at issue occurred on August 8, 2018 and was not discovered until November 14, 2018, a period of approximately 3 months. The Organization did not report when the court order to destroy the information was obtained. In my view, a reasonable person would consider that the likelihood of harm following the court order is very low. However, the Organization did not provide any information about the possible use and/or disclosure of the information at issue between the time the incident occurred and the issuing of the court order, other than to say the incident was discovered when the information was used to contact the affected individual directly. Given the lack of additional, mitigating information, I consider there was a real risk of significant harm to the affected individual in this case, at least until the court order was issued.

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. In the absence of more specific information, I will comment generally that "financial information" often includes the type of information that can be used to cause significant harms such as identity theft and fraud. "Addresses" can include email address, which is often used for phishing purposes, increasing vulnerability to identity theft and fraud. Address may also be used to make unwanted contact with an individual, which may or may not be a significant harm, depending on the circumstances. The incident at issue occurred on August 8, 2018 and was not discovered until November 14, 2018, a period of approximately 3 months. The Organization did not report when the court order to destroy the information was obtained. In my view, a reasonable person would consider that the likelihood of harm following the court order is very low. However, the Organization did not provide any information about the possible use and/or disclosure of the information at issue between the time the incident occurred and the issuing of the court order, other than to say the incident was discovered when the information was used to contact the affected individual directly. Given the lack of additional, mitigating information, I consider there was a real risk of significant harm to the affected individual in this case, at least until the court order was issued. The Organization is required to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individuals were notified by telephone and email sent November 14, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner