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	Wood Law Office (Organization)
Decision number (file number)	P2017-ND-17 (File #004252)
Date notice received by OIPC	November 7, 2016
Date Organization last provided information	November 30, 2016
Date of decision	January 13, 2017
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 in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • cell phone numbers, addresses and telephone numbers (including home contact information), • email address, • client files (copies of personal identification documents; medical, beneficiary, family, and financial information), • employment information (resume, banking details, Social Insurance Number, contact information and general correspondence), and • family folders and/or personal folders. This information is about identifiable individuals (clients, staff and personal and professional contacts) and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	

Description of incident	• In May 2016, the Organization was informed by its IT department that two (2) hard drives were missing. • The information at issue was stored on the drives. • The Organization confronted an ex-volunteer by telephone who admitted to taking the drives. The ex-volunteer refused to return the drives when demanded. • The Organization also reported that an evicted tenant "accessed the [Organization's] server remotely and changed the access codes. The re-establishment of the data access compromised the access authorization and allowed access to all parts of the database temporarily. The theft occurred during this period. We have since learned that the two individuals have been working together." • The Organization reported the incident occurred between January and March 2016.
Affected individuals	Approximately 1,000 clients, staff and personal and professional contacts were affected by this incident.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement in June 2016. • Shut down office IT systems and changed operating system and passwords, upgraded system. • Changed telephone system service provider. • Re-established user permissions protocols.
Steps taken to notify individuals of the incident	The Organization initially informed those individuals that telephoned the Organization to report contact by the ex-volunteer. The Organization has continued to identify and contact affected individuals verbally and in writing.
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 "Data could be used to embarrass or humiliate Criminal and other Clients. Damage to reputation or potential Blackmail or Extortion. Possible fraud and identity theft." I agree with the Organization. The information at issue is comprehensive and sensitive identity, employment, health and financial information. This information could be used to cause the harms of identity theft, fraud, hurt, humiliation, embarrassment, damage to reputation, blackmail, and extortion. 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 initially reported "Harm is not significant as Police recovered the Hard Drives quickly" and also "The Volunteer contacted some very dangerous Criminal Clients and may have instigated them to cause harm to [an employee of the Organization]… Staff and property." Further, although the "Database contains over a thousand Clients and Staff… only a small number were contacted before Police arrested the Volunteer and recovered the Hard Drives into evidence along with all of his Hardware and software." The Organization later reported "I am unsure of the exact date when the hard drive was recovered but I do know that the volunteer was in jail in September 2016 pending a bail application with one of the reasons for being in custody was the theft of the hard drive …The police never advised me of when they retrieved the hard drive, only that it was secure with them along with all of the volunteer's computer hardware and electronic mediums – and that was some time [sic] in September 2016." In my view there is a real risk of significant harm resulting from this breach. The incident is the result of malicious intent (theft), and the information was exposed for at least five months, and possibly longer (the Organization does not know exactly when law enforcement recovered the hard drives). The Organization has not confirmed that the personal information was not copied or forwarded on to other parties. The individual who admitted to taking the information has "contacted some very dangerous Criminal Clients and may have instigated them to cause harm to [an employee of the Organization]… Staff and property."

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 information at issue is comprehensive and sensitive identity, employment, health and financial information. This information could be used to cause the harms of identity theft, fraud, hurt, humiliation, embarrassment, damage to reputation, blackmail, and extortion. These are significant harms. The likelihood of harm resulting from this incident is increased because the breach is the result of malicious intent (theft), and the information was exposed for at least five months, and possibly longer (the Organization does not know exactly when law enforcement recovered the hard drives). The Organization has not confirmed that the personal information was not copied or forwarded on to other parties. The individual who admitted to taking the information has "contacted some very dangerous Criminal Clients and may have instigated them to cause harm to [an employee of the Organization]… Staff and property."

I understand that the Organization has continued to identify and contact affected individuals verbally and in writing since the incident occurred.

I require the Organization to notify all affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and provide me with written confirmation that it has done so on or before January 23, 2017.

Jill Clayton
Information and Privacy Commissioner