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	Tara Cassidy Professional Corporation (Organization)
Decision number (file number)	P2021-ND-310 (File #022032)
Date notice received by OIPC	June 30, 2021
Date Organization last provided information	December 15, 2021
Date of decision	March 4, 2022
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 a law firm located in Calgary, 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, • date of birth, • social insurance number, • license number, • address and contact information (e.g., mailing address, telephone number and email address), • correspondence with the Organization (email or letters), • income tax returns, • medical records, • employment records, and • any other records related to work the Organization performed. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 5, 2021, the Organization discovered unauthorized access to its computer systems in the form of a ransomware attack. • An investigation determined that the threat actor opened/viewed seven (7) documents on the Organization's systems, but these documents did not contain any personally identifiable information. • The investigation also determined that the threat actor obtained domain administrator credentials and employed a number of "anti-forensic" measures such as deleting event logs. • The Organization reported it is possible that the threat actor could have accessed other areas of its computer environment, of which it is not aware. • The earliest evidence of unauthorized activity was January 4, 2021. • The threat actor provided the Organization with four (4) files from its network as proof that some data was exfiltrated, but the Organization's forensic investigation did not independently confirm that any data exfiltration had occurred. • The Organization reported that the four files provided by the threat actor as proof of exfiltration did not contain any personally identifiable information. • The forensic investigation concluded that the cause of the breach was likely exposed RDP (Remote Desktop Protocol) services exposed to the internet.
Affected individuals	The incident affected 770 individuals. .
Steps taken to reduce risk of harm to individuals	• Engaged a computer forensic investigation firm to assist with restoring systems and to investigate the cause and scope of the attack. • Offered affected individuals complimentary 12-month credit and "dark web" monitoring, as well as identity theft insurance and identity restoration services (minors are not eligible to these services). • Informed law enforcement. • Changed all passwords for its computer systems. • Removed RDP from system. • Considering additional security measures for its computer systems.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 28, 2021.
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, *The possible harm may include humiliation, embarrassment (sic) damage to reputation or relationships, loss of professional opportunities and fraud (e.g. credit/identify theft, social engineering, etc.)* I agree with the Organization's assessment. A reasonable person would consider that, particularly in combination, the contact, identity, employment, medical and tax information at issue could be used to cause the harms of identity theft, fraud, loss of professional opportunities, and damage to reputation or relationships. Medical information could be used to cause the harms of embarrassment and humiliation. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all 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 that it… *…believes there is a real risk that harm will result. The likelihood that harm will materialize is increased by the fact that this was a malicious attack designed to exfiltrate sensitive information in order to extort [the Organization], as well as the fact that it has been determined that some documents were accessed and exfiltrated (though none with personally identifiable information). The types of personal information that the threat actor could have accessed include highly sensitve (sic) personal information.* I agree with the Organization's assessment. A reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized intrusion and ransom demand). The perpetrators both accessed and stole some documents, although those particular documents did not contain personal information. However, the Organization cannot rule out whether the perpetrators viewed or accessed personal information.

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, particularly in combination, the contact, identity, employment, medical and tax information at issue could be used to cause the harms of identity theft, fraud, loss of professional opportunities, and damage to reputation or relationships. Medical information could be used to cause the harms of embarrassment and humiliation. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized intrusion and ransom demand). The perpetrators both accessed and stole some documents, although those particular documents did not contain personal information. However, the Organization cannot rule out whether the perpetrators viewed or accessed personal information. 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 notified the affected individuals by letter on July 28, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner