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	Goodman Mintz LLP (Organization)
Decision number (file number)	P2020-ND-154 (File #016261)
Date notice received by OIPC	June 23, 2020
Date Organization last provided information	June 23, 2020
Date of decision	November 20, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a chartered professional accounting firm based in the province of Ontario and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved tax reporting and financial information for current and former clients: • income statements, • information necessary for the preparation for tax filing, such as tax slips, business expenses, charitable donations, RRSP contributions, • banking information and statements, • brokerage information and statements, • credit card information, • information regarding Canada Revenue Agency accounts, filings and activities, such as payments made, • names and contact information, • Social Insurance Numbers and dates of birth, • payroll information regarding the employees of clients for whom payroll services are provided, including income, Social Insurance Numbers and dates of birth, • copies of personal, corporate, HST, T4, T5, trust and charity returns.

	Some of this information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from individuals who telephoned the Organization. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 12, 2020, an employee with the Organization turned on his computer and found that he could not access data files from the Organization's server. • The issue was caused by a malware infection known as "REvil"; the first evidence of malicious activity was on June 10, 2020. • The attacker(s) demanded a ransom in exchange for the decryption key, and if the ransom was not paid, the files would remain encrypted, and any data that had been extracted would be published. • The Organization did not pay the ransom. • The Organization reported that it cannot "positively establish that personal information, including information of individuals in Alberta, has or has not been removed from [its] systems"; however, "its information technology consultants have established that approximately 10 GB of data was exfiltrated from its systems based on firewall logs". • The Organization reported that it is not possible to determine the nature of the data; however, certain information from its systems has been published on Twitter accounts and the Organization has located a website on the 'dark web' purporting to be from the attacker(s) which threatens to auction the information obtained from the Organization. • The Organization reported that it was still investigating the extent to which this incident resulted in personal information being extracted from its systems.
Affected individuals	The incident affected approximately 902 current and former employees, two of whom are resident part-time in Alberta. The incident also affected approximately 175 to 250 employees of clients of the Organization.

Steps taken to reduce risk of harm to individuals	• Engaged information technology specialists. • Disconnected the affected computers and servers. • Ran multiple full virus scans on those believed not to be affected. • Rebuilt and reformatted the affected server and computers. • Changed all internal passwords. • Changed firm bank credentials. • Provided notice to current and former clients. • Provided notice to police, and other organizations who may assist in reducing the risk of harm. • Offered complimentary credit monitoring service to the affected individuals. • Identification of further security measures to reduce the risk of such incidents in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified initially by email, mail or telephone on June 16, 2020 and another notice was sent June 23, 2020. Some affected individuals were notified indirectly, in cases where the Organization acts as a payroll processor for a corporate client. The Organization reported that it would not have any contact information for such employees to allow a direct notification of them and therefore requested its clients notify their employees.
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 information potentially impacted includes sensitive financial information. As a result, there is a potential for this information to be used for identity theft, spear phishing, fraud, and other crimes, as well as social harms such as embarrassment, or public disclosure of private information. As described above, we continue to work with information technology specialists to establish the extent to which personal information was impacted.* In my view, a reasonable person would consider the contact, identity (including social insurance numbers and date of birth), and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing 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 cause and effect relationship between the incident and the possible harm.	The Organization reported, *The incident was caused by the ransomware REvil, which is used by criminal undertakings. These malicious actors are known to publish data they access, and to conduct auctions selling such data to other criminal undertakings. At the time we prepared this notice, we are working with our information technology consultants to establish the extent to which personal information may have been accesses or extracted in a manner that may lead to these harms. However, as described above, we are aware that some information that appears to have been obtained from our firm as a result of this incident has been published, and there have been threats to auction information obtained from our firm. As a result, we conclude that the likelihood of harm is high, but will continue to assess this with our information technology consultants.* I agree with the Organization's assessment. A reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. Although the Organization was able to rebuild its system and did not pay a ransom, it nonetheless cannot determine the nature of the personal information exfiltrated from its systems. As well, some data appears to have been exfiltrated to a Twitter account and a website on the dark web. Further, the personal information was exposed to the attacker for approximately 3 days.

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 the contact, identity (including social insurance n a reasonable person would consider the contact, identity (including social insurance numbers and date of birth), and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. Although the Organization was able to rebuild its system and did not pay a ransom, it nonetheless cannot determine the nature of the personal information exfiltrated from its systems. As well, some data appears to have been exfiltrated to a Twitter account and a website on the dark web. Further, the personal information was exposed to the attacker for approximately 3 days.

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 majority of the affected individuals in writing or by telephone on June 16, 2020 and a further notice was sent June 23, 2020. The Organization is not required to notify these affected individuals again.

The Organization reported that direct notification would not be possible for some individuals "…where we act as a payroll processor for a corporate client, we process the payroll information of identifiable employees of the corporate client; however, we would not have any contact information for such employees to allow a direct notification of them. We will request our client notify its employees of the incident and our offer of …credit monitoring….".

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…", although 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."

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

Jill Clayton
Information and Privacy Commissioner