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** | Solium Capital UI-C (Organization) |
| **Decision number (file number)** | P2020-ND-052 (File #013679) |
| **Date notice received by OIPC** | August 23, 2019 |
| **Date Organization last provided information** | August 23, 2019 |
| **Date of decision** | May 22, 2020 |
| **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 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:<br><br>For 78 employees (Category 1):<br>• name,<br>• job title,<br>• hourly rate (salary and bonus for 2015-2016 years),<br>• SR & ED credit information (which includes educational background) for 28 of the individuals.<br><br>For 95 other employees (Category 2):<br>• name,<br>• date of hire,<br>• SR&ED credit information (office location, PTO dates, work email address, and SR&ED projects worked on).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.<br><br>Some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean |

| | |
|---|---|
| | "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."<br><br>Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose."<br><br>In this case, I considered that the possible unauthorized access to and use of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies to the business contact information. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • The Organization reported that one of its contracted service providers, TSGI Corporation, determined that a former employee had surreptitiously and unlawfully downloaded data to a remote server during his short-term employment from January 31-February 27, 2019.<br>• The data included some confidential information about the Organization's current and former employees.<br>• The service provider first informed the Organization about the breach on February 26, 2019 and on March 6, 2019 confirmed that the Organization's data was among the client data that was stolen from the service provider's network.<br>• The service provider's former employee has since been arrested and charged. |
| **Affected individuals** | The incident affected 173 individuals residing in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | The Organization:<br>• Notified all affected individuals.<br>• Arranged fraud/identity theft and credit monitoring services to affected employees for a minimum of 1 year.<br>• Reviewed service provider agreements to ensure that there are adequate contractual data protections and security safeguards regarding personal information it provides to service providers.<br>• Reviewed cybersecurity and privacy policies and procedures.<br><br>The Organization reported that its vendor:<br>• Changed passwords on systems, devices and applications. |

| | |
|---|---|
| | • Shut down any remote access capability.<br>• Monitored inbound and outbound traffic from its system.<br>• Cooperated with the Calgary Police Service.<br>• Notified affected individuals.<br>• Assessed providing credit monitoring to any affected individual.<br>• Notified data protection authorities.<br>• Engaged external legal counsel.<br>• Engaged third party forensic consultants to assist with investigation. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified in writing on April 26, 2019. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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:<br><br>*Because the information of… employees in Category 1 includes personal and financial information that is several years old and likely no longer accurate (2015-2016 years), it is [the Organization's] assessment that there is a negligible risk of identity theft, fraud and financial loss to these employees in addition to humiliation and embarrassment of having employment compensation information potentially disclosed.*<br><br>*The personal information in Category 2 is not sensitive and could not likely be used to harm the employees without additional personal information.*<br><br>In my view, a reasonable person would consider that the financial and employment information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. |
| **Real Risk**<br>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 is…<br><br>*…of the view that the likelihood that harm could result to the … employees in Category 1 is extremely low. The personal information in Category 1 is of low sensitivity and the potential harms consist of humiliation or embarrassment by having salary and/or employment information disclosed. It is the view of [the Organization] that there is similarly a negligible risk of identity theft or fraud to the individuals in Category 1 as a result of the Incident.* |

| | |
|---|---|
| | *In [the Organization's] view, there is no real risk of harm associated with the personal information in Category 2. [The Organization] understands from TSGI that, since the Incident, the former TSGI employee has been arrested and the stolen data has been located. [The Organization] further understands that there is currently no evidence one way or another indicating that the information of the… employees was further disseminated or disclosed prior to being recovered.*<br><br>In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month and the Organization cannot say for sure if it was disseminated or disclosed prior to being recovered. It appears that information was used for extortion (although not to extort individuals). |

**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 financial and employment information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month and the Organization cannot say for sure if it was disseminated or disclosed prior to being recovered. It appears that information was used for extortion (although not to extort individuals).

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 that affected individuals were notified in writing on April 26, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner