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** | Shady Hill School (Organization) |
| **Decision number (file number)** | P2020-ND-173 (File #017326) |
| **Date notice received by OIPC** | September 18, 2020 |
| **Date Organization last provided information** | September 18, 2020 |
| **Date of decision** | December 3, 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 the individual 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>• name,<br>• contact information,<br>• giving history, and<br>• social security number.<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. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On July 16, 2020, the Organization received notice that its third-party service provider, Blackbaud, had been the target of a ransomware attack.<br>• The Organization reported:<br><br>*Blackbaud ransomware occurred from 2/20/2020 to 5/20/2020 where cyber criminals had access to personal* |

| | |
|---|---|
| | *information. Blackbaud with the help of the FBI paid the ransom and ensured all exfiltrated information was destroyed.* |
| **Affected individuals** | The incident affected 823 individuals, including one individual residing in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | The Organization reported its service provider:<br><br>• Halted system access as soon as the intrusion was detected.<br>• Paid the ransom demand in return for assurances that all copies of data would be destroyed.<br>• Notified the Federal Bureau of Investigation.<br>• Implemented changes to their data security protocols to prevent a similar incident from occurring again.<br><br>The Organization:<br><br>• Notified affected individuals and informed them to remain vigilant in monitoring their credit reports for identity theft and fraud.<br>• Retained its own forensic cyber investigators to thoroughly research its database to detect possible exposures. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on September 18, 2020. |
| **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 harms that might result from the breach included "possible identity theft and/or fraud".<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and donor information at issue could be used to cause the harms of identity theft and fraud. These are 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 assessed the likelihood of harm as "possible with access to other identifying information along with social security number".<br><br>In my view, 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 action, ransom demand). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this |

| | |
|---|---|
| | possibility. The information appears to have been exposed over the course of 3 months. |

**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 contact, identity and donor information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility. The information appears to have been exposed over the course of 3 months.

I require the Organization to notify the affected individual 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 individual in a letter dated September 18, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner