Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

January 6, 2025

VIA EMAIL

PERSONAL & CONFIDENTIAL

Elmira Chimirova
Senior Legal Counsel
Freedom of Information Coordinator
Legal Services
Toronto District School Board
5050 Yonge Street
Toronto, ON M2N 5N8

Dear Elmira Chimirova:

RE: Reported Breach MR23-00097

On October 12, 2023, Toronto District School Board (the school board, or TDSB) reported a breach of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act* or *MFIPPA*) to the Office of the Information and Privacy Commissioner of Ontario (IPC). File MR23-00097 was opened by the IPC to address this matter.

The circumstances of the breach involved the unauthorized access to and possible exfiltration of information belonging to current and former students, parents, and staff at five TDSB schools by an unknown threat actor. The threat actor gained unauthorized access to the affected schools' systems by obtaining the login credentials of a school's Vice-Principal (VP) through a social engineering attack and unauthorized access to a browser cache connected to the Vice-Principal.

I. Background

What happened?

On October 6, 2023, TDSB discovered one of its schools was the subject of a cyberattack when a threat actor posted messages on Telegram (an instant messaging service) alerting the school to the attack. The attack involved unauthorized access to computers belonging to the VP of Lakeshore Collegiate Institute (LCI). The threat actor accessed and possibly exfiltrated personal information contained in the VP's computers and OneDrive account that belong to current and former students, parents, and staff of five TDSB schools, including LCI.

The school board determined that the VP's computers were compromised on September 28, 2023, with the first unauthorized access to personal information occurring on October 3, 2023. TDSB believes the threat actor stole the VP's school board login credentials through social engineering,

then physically accessed the VP's desktop and laptop computers in her office and proceeded to compromise the VP's OneDrive account. The school board suspects that the VP's OneDrive credentials were obtained from the computer's browser cache.

The threat actor used a USB key in the attack which the school board believes was programmed to be an "information stealer". The threat actor accessed information from the OneDrive account that included the personal information of current and former students, parents, and staff of LCI and four other schools. The attack also affected two school board webservers and defaced LCI's website with a threatening message.

The threat actor posted a message on Telegram threatening to disclose the exfiltrated information if the school board did not notify the public of the incident within a certain timeframe. On October 16, 2023, the threat actor deleted all of their online posts related to this matter leading the school board to believe that their demands were retracted.

The school board's investigation included an investigation by its authorized security partner. The school board has no information regarding who the threat actor may be, but believes it was most likely a person who entered the VP's office while the VP was away from their desk. While the school board submits its investigation found no evidence that any personal information was exfiltrated by the threat actor, these details were not shared with the IPC.

II. Issues

Institutions, when confronted with a breach of personal information, must take appropriate steps in response. These steps include identification of the scope of the breach, containment of the personal information involved, notification of those affected, and investigation and remediation of the breach. The IPC guidance to institutions on these steps is set out in *Privacy Breaches: Guidelines for Public Sector Organizations*.[1]

There is no dispute that TDSB is an institution, or that the information that was inappropriately accessed by the threat actor is personal information as defined by section 2(1) of the *Act.*

The following issues were identified during the review of this breach at the early resolution stage:

1) **Did TDSB take adequate steps to contain the breach?**
2) **Did TDSB take adequate steps to notify the individuals who were affected by the breach?**
3) **Did TDSB take reasonable remedial measures to prevent similar breaches in the future?**

[1] privacy-breach-protocol-e.pdf

Did TDSB take adequate steps to contain the breach?

TDSB's analysis of the impacted data determined that personal information belonging to current and former students and parents of five schools was accessed without authorization by the threat actor. Staff information was also affected by the breach.

When asked how many individuals were affected by the incident, the school board advised that current and former students and parents of five schools were affected. The school board would not provide an estimated number of affected individuals.

The personal information inappropriately accessed consisted of student names, student numbers, dates of birth, grades, class subject, class schedules, timetables, email addresses, courses passed or failed, parent emails and contact information. In some cases, Special Education forms and health card numbers were accessed and exfiltrated.

On October 6, 2023, TDSB discovered that one of its schools was subject to a cyberattack when the threat actor posted messages on Telegram alerting it of the attack. The threat actor posted messages on Telegram, threatening to disclose the exfiltrated information if the TDSB did not notify the public of the incident within a certain timeframe. The school board believes that the threat actor retracted their demands when it deleted all online posts related to this matter.

To contain the breach, the school board disconnected the VP's computers and obtained forensic images to assist in its investigation. The school board also disconnected LCI's website from the network. The school board had all LCI staff reset their passwords, implement Multi-Factor Authentication (MFA) for all LCI users and TDSB IT Services re-imaged all LCI computers.

TDSB also retained a third-party breach coach and a negotiator to assist in this matter.

Based on the information before me, it appears that this matter has not been contained. While I acknowledge the school board's belief that the threat actor retracted their demands as a result of removing online posts related to this matter, this belief is an assumption and is not a factual conclusion. I was not provided with information that would support TDSB claim that the personal information accessed by the threat actor was not also stolen.

Despite TDSB not providing the IPC with information to support its belief that personal information was not stolen by the threat actor, it is my view that the school board took reasonable measures to attempt to contain the matter.

Did the TDSB take adequate steps to notify the individuals who were affected by the breach?

As a preliminary matter, there is no provision under the *Act* requiring that institutions notify individuals whose personal information has been breached while in its custody or control. As indicated in the IPC's *Privacy Breaches: Guidelines for Public Sector Organizations*, institutions should notify those affected if it is determined that the breach poses a real risk of significant harm to the individual, considering the sensitivity of the information and whether it is likely to be misused.

On October 12, 2023, the school board issued a letter to the current members of the LCI community (students, student's parents, and school staff) notifying them of the breach. This notice included details of the breach, steps taken to address the breach, that the school board notified the IPC of the breach, information on how to file a complaint with the IPC and contact information at TDSB should affected individuals have questions or concerns. This notice did not include a description of the personal information at issue, as the TDSB did not have these details at this time. Following the notice to current members of the LCI community, TDSB gave notice of the breach to the current members of the other affected schools.

The school board reported that it did not have contact information for affected former students, parents and staff and sought to issue a general notice to the public. In these efforts, TDSB sought input from the IPC in giving this general notice.

The IPC recommended that the school board post its general notice in prominent places at each affected school site, on each affected school's website and on the school board's website.

On April 19, 2024, the school board provided a draft general notice for the IPC's review. Upon review of the draft, it was noted that affected individuals were notified that their personal information was accessed but the notice did not include any language notifying individuals that their personal information was/may have been exfiltrated by the threat actor. On April 23, 2024, the IPC recommended that the school board amend its draft general notice to include language notifying affected individuals that their personal information was accessed *and* exfiltrated. At this time and to the date of this report, the IPC has not been provided with the evidence that shows that no exfiltration occurred.

On April 25, 2024, the school provided an amended draft general notice. The amended notice did not include language notifying affected individuals that their personal information may have been exfiltrated by the threat actor. TDSB explained that it was their preference to keep the language in the notice as simple as possible keeping in mind that there are parents who are not familiar with certain terminology (i.e. "exfiltrated"). I agree with TDSB's position to keep the language in the notice as simple as possible; however, a strong argument could be made that most parents/guardians are familiar with the term "exfiltrated" and its definition. In addition, on May 1, 2024, in considering the TDSB's concerns of simple and plain language, the IPC recommended that it substitute "exfiltrated" with "stolen". However, TDSB did not accept this recommendation. While TDSB takes the position that it was not necessary to notify that information was exfiltrated as they have evidence to this effect, at the time this discussion took place in April, 2024, TDSB had not provided the IPC with evidence of this, nor did it seem that they had formed this position at that time.

On May 6, 2024, the school board posted its general notice on each school website. Despite the IPC's recommendations, the notice did not notify individuals that their personal information was exfiltrated by the threat actor and was not physically posted at affected school sites. On the same date, the school board issued a notice to affected staff by email. Again, this notice did not notify staff that their personal information was exfiltrated by the threat actor.

Analysis of the TDSB's Notice Efforts:

While I appreciate that TDSB opted to engage in the notification process, I find that TDSB's decision to omit critical information in its notice and not to post physical notices at affected school sites may impede affected individuals' ability to make an informed decision on how to protect personal information impacted by this breach.

In coming to this conclusion, I am mindful that it is generally better for institutions to provide direct notification to individuals who may have been affected by a privacy breach. Direct correspondence is more likely to draw the individual's attention to the potential impact of the breach on their personal privacy, compared to a posted notice. However, in this case, given the potentially large number of individuals impacted by this incident and the circumstances of this breach, it was reasonable for the institution to determine that direct notice was not feasible for former students, parents, and staff.

TDSB notified affected parties that their personal information was accessed without authorization, but their notices did not include important information regarding the possibility of personal information being exfiltrated by the threat actor.

As TDSB provided no information to the IPC to support their assertion that no personal information was exfiltrated by the threat actor, nor did it appear that it had formed this position at the time of giving notice, it is the IPC's position that TDSB did not take adequate efforts to notify affected individuals of the real impact to their personal information. By not taking adequate efforts to notify affected individuals of the real impact of their personal information, TDSB denied affected individuals the opportunity to take appropriate action to protect themselves.

Did TDSB take reasonable remedial measures to prevent similar breaches in the future?

The IPC's *Privacy Breaches: Guidelines for Public Sector Organizations* states that the investigation and remediation of a breach should include: a review of the circumstances surrounding the breach; a review of the adequacy of existing policies and procedures in protecting personal health information; a determination of whether the breach was a result of a systemic issue; and corrective action to prevent similar breaches in the future.

Investigation of the Attack:

TDSB retained a third-party breach coach and a negotiator to assist in this matter. Based on the investigation, the threat actor initially compromised the VP's computers on September 28, 2023. The school board reported that this compromise was a result of a social engineering attack. The threat actor then obtained the VP's OneDrive credentials from a browser cache.

The school board determined that the first unauthorized access to data on the computers occurred on October 3, 2023 and discovered the attack on October 6, 2023 through Telegram.

The school board does not know the threat actor's identity, but believes the person entered the VP's office while away from their desk.

The school board reported the incident to the Toronto Police Services and to the IPC.

Remediation Efforts:

Based on the information provided, this breach was as a result of a social engineering attack and the availability of login credentials in a browser cache.

Upon discovery of the breach, the school board disconnected the VP's computers and LCI's website from the network, preventing further access to personal information.

The school board had all LCI staff reset their passwords and implement MFA and will implement MFA across the school board. The school board also implemented Microsoft Defender Credential Guard, tamper protection and removed all non-production systems from its network. Further, the school board will also use a recommendations report provided by its authorized security partner to enhance the school board's security measures and safeguards.

On October 25, 2024, all LCI staff underwent cybersecurity awareness training with a TDSB representative from its Cyber Security Team. This training included commons strategies to prevent another physical breach. This training is regularly provided on a quarterly basis and includes topics such as "What is Social Engineering?", "What is the Most Common Social Engineering Attack?", "Distraction Techniques by Students", "Hacking Tendencies in Library", "Keylogger User", and "Good Practices for Password Use".

Review of Existing Privacy Policies and Procedures:

The school board provides security awareness training on a quarterly basis to all staff, in addition to privacy training during the onboarding process. Privacy training is available on the school board's professional development platform should staff require refresher training.

In addition to privacy training during the onboarding process, I recommend that the school board provide training to all its staff on an annual basis.

TDSB's cybersecurity incident management program and privacy protocol involve the school board's Cyber Security Risk Management Team, Freedom of Information and Privacy Office, Legal Services, Enterprise Risk Management, Communications, Enterprise Administration, Business Analytics and Systems, Application Administration, Field Services, and the affected school or department.

Most relevant to this breach, the school board has a Data Privacy Breach Playbook and Data Breach Protocol in place. Polices and procedures of note include:

- Online Code of Conduct
- Policy P094 – Freedom of Information and Protection of Privacy
- Operational Procedure PR676 – Freedom of Information and Protection of Privacy
- Policy P088 – Acceptable use of Information Technology Resources
- Operational Procedure PR736 – Privacy Breach Procedure

At the conclusion of each incident, the school board conducts a post-mortem meeting to discuss methods of improvement and any changes to make to the incident playbook.

III. Conclusion and Recommendations

Based on the information before me, it appears that the breach of the school board's systems was a result of the lack of staff awareness and training regarding social engineering, weak authentication for access to computers, the lack of physical safeguards providing threat actor(s) access to computers, credentials/authentication information being stored in a browser cache and a lack of encryption of personal information.

While the school board has taken steps to remediate the matter by providing cybersecurity awareness training to staff, implementing MFA, Microsoft Defender Credential Guard, tamper protection and removed all non-production systems from its network, I recommend that the school board implement:

- proper physical controls (you may wish to consult the National Institute of Standards and Technology's (NIST) guidance SP 800-12 as a resource regarding Physical and Environmental Security),
- update its security policy and configuration procedures to ensure that authentication information is not stored in browser caches,
- encrypt sensitive data/personal information, and
- a cybersecurity program to assist it in managing cybersecurity risks in a holistic manner.

After considering the circumstances of this reported breach, the actions taken above, and the recommendations made, I am satisfied that no further review of this file is required. We may re-open this matter if additional information comes to our attention suggesting a need for further inquiry.

The IPC thanks you for your cooperation in this matter and ongoing commitment to ensure compliance with the *Act*. This letter will serve as confirmation that this file is now closed.

Yours truly,

Raymond Borja
Analyst