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

December 3, 2024

VIA EMAIL

PERSONAL AND CONFIDENTIAL

Daniel Michaluk
Partner and National Co-Leader, Cyber Security
Borden Ladner Gervais (BLG) LLP
22 Adelaide Street West, Suite 3400
Toronto, ON M5H 4E3
DMichaluk@blg.com

Dear Daniel Michaluk:

RE: FILE MR23-00112

INTRODUCTION:

On November 10, 2023, the Toronto Public Library (TPL) reported a cyber security breach under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) to the Office of the Information and Privacy Commissioner of Ontario (the IPC). File MR23-00112 was opened by the IPC to address this matter.

The breach relates to a ransomware attack. The threat actor(s) gained unauthorized access to TPL's network, encrypted certain network assets and exfiltrated data that included personal information.

BACKGROUND:

TPL explains that it is the busiest urban library system in the world, with over four million branch visits annually, 1.2 million registered library cardholders, and ten million registered resource holds per year. In addition to loaning library materials, TPL also offers access to dozens of eResources, online databases, and other digital services via the torontopubliclibrary.ca website, and on-site neighbourhood programming at its 100 branches. TPL fundraises through the Toronto Public Library Foundation (TPLF), which has raised over $100 million in donations since its 1997 inception.

On October 28, 2023, TPL discovered suspicious activity on its network. TPL learned that the threat actor(s) encrypted certain networks and stole/exfiltrated a large number of files stored on its file server. Over the following days and months, TPL issued public statements and cyber security

incident frequently asked questions to inform the public about the breach. TPL communicated that the incident caused significant disruptions resulting in a "full-scale shut down of TPL's technical environment,[…] the suspension of many core library services including TPL's website, access to the library catalogue, holds, and Your Account services; public computing and printing; and access to some digital materials and databases".

To investigate the incident, TPL immediately implemented its Major Cyber Security Incident Playbook and Privacy Breach Protocol, along with engaging its core incident response team. TPL retained external legal counsel and a third-party security consultant to assist with the containment, investigation, remediation and to conduct a forensic investigation into the cyber security incident. The City's Mayor's Office was informed as well as the Toronto Police Service and the City of Toronto (the City) as it is an "agency"[1] of the City.

TPL reported that the incident was contained within 24 hours of its discovery, by October 29, 2023. On November 14, 2023, TPL issued a public statement notifying the public regarding the breach and that current and former TPL and TPLF staff were impacted. TPL also communicated that some data relating to dependents and family members of staff had been impacted. TPL advised that cardholder, volunteer, and donor databases were not affected but some data about this group resided on the compromised file server. TPL explained that it was to begin an e-discovery process to fully understand the extent of the data at issue. TPL's services were fully restored by March 28, 2024.

TPL completed its e-discovery data analysis for beneficiaries and dependents in February 2024 and for other individuals in July 2024. The results of the e-discovery showed that in addition to approximately 8,018 current and former staff, approximately 1,874 of their beneficiaries and dependents, and 4,100 (or fewer) customers, donors, contractors, volunteers, and unsuccessful job applicants were affected by the breach.

The Personal Information at Issue:

The personal information of three groups of individuals was identified by TPL, as follows:

- Individuals (customers, donors, contractors, volunteers, and unsuccessful job applicants)
- Current and former TPL and TPLF employees since 1998
- Employee beneficiaries and dependents

The personal information of approximately 4,100 individuals relating to TPL includes the name and one or more of the following:

- Name
- Contact information (street address, e-mail address, phone number)
- Criminal background information
- Date of Birth (DOB)
- Gender

[1] Agencies – City of Toronto.

- Library card number
- Medical information (health references, treatment/diagnosis, prescription information, treatment provider, health card numbers, health insurance information)
- Physical descriptions and/or photo images (in incident reports)
- School information
- Signatures
- Status as complainant
- Status as having made an access request
- Status as donor
- Status as involved in a TPL incident/complaint
- Status as a TPL contractor

The personal information relating to approximately 2,500 current employees of TPL, 18 current TPLF employees, and the number of former employees of TPL and TPLF since 1998 is unknown (though estimated as approximately 5,500) includes the name and one or more of the following:

- Name
- Social insurance numbers (SIN)
- DOB
- Home address
- Employment information
- Payroll information
- Any government-issued identification provided to TPL

The personal information relating to approximately 1,874 employee beneficiaries and dependents the name and one or more of the following:

- Name
- Contact information (street address, email address, phone number)
- DOB
- Any government-issued identification provided to TPL (including SINs and other government identification documents and numbers)
- Medical information (health references, treatment/diagnosis, prescription information, treatment, provider, health card numbers, health insurance information)
- Payment card/financial account information
- School information
- Signatures

ISSUES:

As a preliminary matter, TPL stated, and I agree, that information accessed and exfiltrated by the threat actor(s) contains personal information under section 2(1) of the *Act*. There is no dispute that TPL is an institution as defined under section 2(1) of the *Act*.

The following issues were identified during the review of this matter at the Early Resolution stage:

1. Did TPL have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 to the *Act*?
2. Did TPL take adequate steps to contain the breach?
3. Did TPL take adequate steps to notify individuals affected by the breach?
4. Did TPL take reasonable remedial measures to address the breach?

DISCUSSION:

Issue 1: Did TPL have reasonable measures in place to prevent unauthorized access to personal information within its systems in accordance with section 3(1) of Regulation 823 to the *Act*?

Section 3(1) of Regulation 823 of the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

In Privacy Complaint Report PR16-40, Investigator Lucy Costa (refers to the equivalent regulation under the *FIPPA*) stated that there is no mandate for a "one size fits all" approach, noting:

> ...It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.[2]

The Ransomware Attack

TPL reported that the threat actor(s) accessed the network on August 3, 2023. There was no further malicious activity until October 5, 2023. The cyber security incident impacted a significant portion of TPL's network, including core Information Technology (IT) infrastructure, file servers, and corporate systems. TPL submitted that approximately 900 GB of data was exfiltrated from a file server by the threat actor(s), containing 780,000 files in 44 folders.

Based on the information provided by TPL, the root cause of the cyber security incident remains unknown. Initially, the threat actor(s) installed a remote access tool on an internet facing server that hosted a TPL printing service. TPL indicated that despite having endpoint malware and network security logging in place, the threat actor(s) entered the network and went undetected.

[2] See paras. 72 of Privacy Complaint Report PR16-40.

TPL advised that the investigation into this matter has concluded, and no direct evidence was found showing how the threat actor(s) installed a remote access tool and gained persistence. TPL acknowledged the system at issue was vulnerable, and that it believed the threat actor(s) likely exploited the vulnerability.

Measures in Place at the Time of the Incident

In answer to IPC questions regarding the security measures in place at the time of the attack, TPL submitted the following:

- Some enterprise applications and operating systems were end of life or unsupported by TPL's supplying vendor. These items had been identified and prioritized for remediation, which involved upgrading the enterprise application or reimaging entirely new solutions and retiring the legacy system.
- Critical end point patches were exclusively deployed through Microsoft Systems Centre Configuration Manager (SCCM).
- Domain controllers are hardened following standard procedures and policies.

Analysis

A "one-size-fits-all" approach to security measures cannot be applied to all institutions. However; institutions are required to have "reasonable" measures considering the "nature" of the records being protected.

TPL acknowledged that certain applications and operating systems were identified as end of life or unsupported by a third-party vendor needing remediation.

Considering that TPL is a large public-facing organization, I believe it should have up to date and effective security measures in place to protect personal information.

It is my view that if TPL had taken a more proactive approach to identify, analyze and address the privacy risks involved with its applications and systems (particularly those approaching end of life) including improvements to its patching system, the likelihood of a significant privacy breach could have been prevented or reduced. It is also concerning that over two months passed before the presence of the threat actor(s) was detected in TPL's network and that the root cause of the incident remains unknown. TPL believes however that the threat actor likely exploited an vulnerability and this understanding has supported strong corrective action.

Section 3(1) of Regulation 823 of the *Act* requires institutions to ensure security measures to prevent unauthorized access to records are "defined, documented and put in place."[3] Based on the information before me, I find that the TPL did not have reasonable security measures in place, as required under Regulation 823 of the *Act*.

[3] RRO 1990, Reg 823 | General | CanLII

In October 2022, the IPC published a Technology Fact Sheet addressing ransomware attacks, such as the one described above, titled How to Protect Against Ransomware[4]. The Fact Sheet discusses how this type of malicious software is becoming increasingly common and a serious threat to the security of electronic records. Organizations such as TPL can take proactive steps to reduce the risk of bad actor(s) gaining access to their Information Technology (IT) systems, including the following:

- **Put in place email security controls** to detect and prevent the delivery of emails with suspicious links, malicious attachments, and spoofed sender addresses.
- **Establish a vulnerability management program**
- **Follow system hardening best practices**. Hardening generally involves reducing the number of pathways that an attacker can take to get access to your network.
- **Develop strategies to mitigate risk to systems that are out of date**.
- **Restrict employee access** to suspicious websites.
- **Ensure that all employees receive up-to-date cybersecurity awareness training** that includes content about ransomware attacks and how they occur.
- **Install security tools** on all computers that can prevent malware, quarantine suspicious files, and issue alerts, such as enterprise antivirus tools or endpoint detection and response tools.
- **Use good authentication practices** including effective passwords, password management, strong multi-factor authentication, and limiting password reuse.[5]

Institutions need to regularly address risks identified in their systems and applications on a regular schedule, rather than waiting for issues to arise. I recommend TPL review the above-mentioned IPC guidance to ensure it has implemented sufficient preventative measures, make improvements to better adapt to the evolving threats, including ransomware, and take steps to keep its cybersecurity posture up to date.

Issue 2: Did TPL take adequate steps to contain the breach?

TPL discovered the attack in the early hours of October 28, 2023. To contain and conduct a forensic investigation, TPL reported it shut down its entire network, including all external access to the web and VPN, the same day of discovery as a precaution, despite all its systems not being impacted by the attack.

TPL's containment efforts were achieved within 24 hours of the discovery, on October 29, 2023. TPL reported that some TPL systems were open to the internet and accessible via LAN, but TPL deployed access controls throughout its network.

TPL explained that the stolen data was identified based on evidence gathered from the threat actor(s) and digital forensic evidence, TPL then engaged a third-party data mining vendor to examine the information at issue.

[4] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca)
[5] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca).

Over several months, TPL took the follow steps to contain the breach:

- Quarantined all endpoints, including servers and workstations and scanned them with forensic tools prior to migrating or restoring items onto a new network to ensure successful containment. The recovery of TPL's network was done by using secure backup repositories not impacted by the incident or rebuilding certain components.
- Due to the large physical complexity of its organization, each physical TPL location (over 100 sites) were visited to inspect, conduct a deep analysis, validate and remedy hardware during the recovery process including a quarantine period.
- More than 200 servers were forensically reviewed, cleaned and restored or rebuilt. Over 5,000 workstations were individually quarantined, evaluated and migrated to a clean network to restore endpoints for staff and public usage.
- Manual deployment of enhanced malware and security logging tools were used to capture forensic evidence. All endpoints and enterprise systems were patched to the most current patch management software prior to restoring its services. A more rigorous patch management regime was developed and deployed to ensure regular security patches are continuously maintained.
- Re-architected the affected public printing service with modern technology which will be launched in a secure state.
- In statements issued to the public, TPL acknowledged that the stolen data at issue may be published on the dark web. TPL stated in its communications with the IPC, that it is continually monitoring the dark web since the discovery of the attack and has not found evidence of publication of the data at issue or references to the incident.

Analysis

It is clear that vulnerabilities existed within the TPL environment at the time of incident, especially since the threat actor(s) went undetected in the TPL environment from August 3, 2023, until October 28, 2023. TPL did not provide specific details to the IPC regarding the actions the threat actor(s) took within its environment during this period until November 21, 2024.

Understanding that global cyberattacks are on the rise, it is imperative that TPL has an evolving cyber security posture and ensures that effective security measures are implemented within its networks to efficiently detect and prevent these types of attacks.

The reality of information at issue being posted or available on the dark web is explained in Privacy Complaint Report MR24-00114, by Investigator, Jennifer Olijnyk such that:

> …once data is stolen, it is beyond the [institution's] control. In such situations, one should assume that it is being used by bad actors and take steps accordingly. While dark web monitoring can be useful in discovering a breach or determining its extent, it doesn't change the fact that institutions cannot remove personal information posted by bad actors.[6]

[6] See para 37: MR21-00114 - Information and Privacy Commissioner of Ontario (ipc.on.ca).

Given that the breach was halted within 24 hours of discovery of the cyber security incident and that TPL continuously monitored the dark web for the data at issue, I am satisfied that TPL adequately determined the scope of the breach and took reasonable steps to contain the breach.

Issue 3: Did TPL take adequate steps to notify individuals affected by the breach?

Given the length of time it took TPL to determine what data was affected by the breach and the corresponding individuals, numerous public statements, updates and notifications were provided by TPL as follows:

N**ovember 14, 2023**: A public statement was issued to notifying the public of the breach and indirectly notified affected staff and former staff of TPL and TPLF. At this time, TPL advised that cardholder, volunteer and donor databases were not affected but some data about this group resided on the compromised file server. TPL explained that it was to begin an e-discovery process to fully understand the extent of the data at issue.

November 29, 2024: TPL held a town hall to answer questions from staff. To supplement its general notification on November 14, 2023, around the same time, TPL sent notices to approximately 3,100 current and former employees.

December 1, 2023: TPL began the e-discovery process and continued its forensic investigation. TPL commenced a separate, more focused e-discovery for dependents and beneficiaries because it considered them to be a priority given the possibility of sensitive information exposure.

January 5, 2024: TPL advised its forensic investigation was complete but that the e-discovery continued. IPC was advised that some, minimal customer personal information may have been affected. TPL aimed to identify all other affected individuals (including customers) by the end of March 2024.

February 2, 2024: TPL was to shortly notify 2,100 dependents of TPL employees. TPL advised it continued to analyze data and hoped to notify newly found affected parties by April/May of 2024.

March 14, 2024: Notice to TPL dependents and beneficiaries was completed.

April 26, 2024: After multiple extensions were granted by the IPC to TPL, it provided its breach report to the IPC. It was noted that TPL had yet to complete its data analysis to determine all individuals affected by the breach.

July 2024: TPL reported to the IPC its e-discovery vendor completed the data analysis.

TPLs efforts to Notify Affected Individuals of TPL (Customers, Donors, Contractors, Volunteers, and Unsuccessful Job Applicants)

In July 2024, I sought clarity regarding who was affected by the breach and when and how the individuals were notified. It is my view that there were inconsistencies in the information TPL

provided to me relating to customers, donors, contractors, volunteers and unsuccessful job applicants since the breach was reported in October 2023.

In response to my questions, TPL advised that approximately 7,552 customers were affected by the breach and that it intended to notify 226 of those customers on July 8 and July 9, 2024. The data at issue for these customers included some combination of name, mailing address, email address, phone number, DOB, credit card number, passport number, or work permit number. TPL offered a two-year credit monitoring service. TPL submitted that where mailing addresses were available, those individuals would receive a letter in the mail otherwise email notifications would be sent. Communication included details and the extent of the breach, the information at issue, and contact information within TPL for further inquiries. TPL stated that the steps it took to address the breach were not included in this communication as the information has already been made public by TPL.

TPL was asked why they decided to notify some affected individuals and not others and its rationale for making the decision. TPL advised that it "has notified all customers whose impacted information posed to them a real risk of significant harm".

The impacted customer data included some combination of name, mailing address, demographic information, library card number, and an expressed interest in or confirmed attendance at TPL programming. TPL submitted it did not believe exposing this type of data presents a real risk of significant harm (RROSH) to these customers and accordingly chose not to notify them.

It is unclear what threshold TPL considered to determine if there was a RROSH to its affected customers.

Ontario's privacy laws set out the rules for how public sector organizations should manage personal information. Specifically, section 2(1) of the *Act* defines "personal information" as recorded information about an identifiable individual, to include:

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> (c) any identifying number, symbol or other particular assigned to the individual,
> (d) the address, telephone number, fingerprints or blood type of the individual,
> …
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
> …
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

The IPC has held that it is important to examine the context in which information appears in determining whether the information is "about" an individual and whether the individual is "identifiable." Considering section 2(1) of the *Act* definition of "personal information" and the details of the impacted data TPL was advised of my view that the personal information of the customers such that a combination of information may reveal something of personal nature and an individual can be identified from this information. I also asserted that there is potential for misuse of the personal information that may result in harm to the affected customers, considering that the threat actor(s) inappropriately accessed their information.

Further, the IPC's Privacy Breaches: Guidelines for Public Sector Organizations sets out a useful framework for institutions to determine appropriate measures to take to meet their obligations under the *Act*. In particular, the IPC has a long-standing position that institutions should notify those affected by a breach as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, **taking into consideration the sensitivity of the information and whether it is likely to be misused [my emphasis]**. Additional informational about the method of notification and the communication to be included to those impacted is noted in this guidance document.

Based on the information before me, I recommended that TPL provide notification to the remaining 7,552 impacted "customers" whose personal information was accessed without authorization under the *Act* by the threat actor(s). Given the circumstances and the number of individuals affected, I suggested that TPL may want to consider a general notification.

Due to a failure to account for duplicates in the affected data set, TPL discovered it over-reported the number of affected customers. The actual number of affected customers was 4,336 (or fewer) which TPL reported may include duplicate information. TPL also clarified that the "customers" category includes "customers, donors, contractors, volunteers, and unsuccessful job applicants." After TPL's discussion with me regarding its application of its "harms test", it agreed to issue a general notice to this category of affected individuals. TPL had committed that this notice was going to be posted on its website and other appropriate media channels before the end of October 2024.

On November 26, 2024, TPL reported that it conducted a further data analysis and address matching for the remaining affected individuals. TPL submitted its able to directly notify some of the remaining affected individuals. TPL indicated that it believes approximately 4,100 individuals were impacted by the breach in this category, rather than 4,336 individuals that was reported earlier to the IPC. TPL explained that the change in the number of affected individuals is due to duplication and some of these individuals being employees who have already been notified.

On the same day, TPL committed to issuing indirect notification to the remaining individuals on its website and through other channels. TPL also committed to mail letters directly to affected contractors and volunteers. TPL committed to proceed with indirect and direct notification to the remaining individuals starting the end of November 2024.

Current and former TPL and TPLF employees since 1998

On April 26, 2024, TPL confirmed to the IPC that approximately 8,000 current and former TPL and TPLF employees since 1998 had been impacted and notified. At this time TPL submitted that the data at issue for this group included employment and payroll information as well as SINs. TPL explained a public notice regarding the incident was issued on its website and social media on November 14, 2023. TPL advised that the notice was shared with media, given to current and former employees directly, and posted on its website until April 2, 2024.

TPL reported that it directly notified approximately 3,100 of its current and former TPL and TPLF employees (whose contact information was available at the time) regarding the breach by letter, the week of November 27, 2023. TPL stated credit monitoring was offered to all current and former TPL and TPLF employees by mail and upon request for a period of two years. Communication included details and the extent of the breach, the information at issue, the steps taken to address the breach, that the IPC was notified about the breach and contact information within TPL for further inquiries. TPL submitted it held an employee town hall to answer questions about the notification on November 29, 2023.

Employee beneficiaries and dependents

On April 26, 2024, TPL confirmed to the IPC that approximately 2,000 employees' beneficiaries and dependents were impacted and notified regarding the breach by mail, the week of March 11, 2024. Communication included the details and the extent of the breach, the information at issue, that the IPC was notified about the breach and contact information within TPL. TPL submitted the data at issue for this group included medical and insurance benefits claims information.

On July 5, 2024, TPL advised that it discovered an additional 50 employee beneficiaries and dependents impacted and would be notifying these individuals in the upcoming weeks. TPL confirmed notification was completed by August 16, 2024.

On October 9, 2024, TPL clarified that 1,874 employee beneficiaries and dependents were notified by mail during the week of March 11, 2024.

Analysis

It has been the IPC's long-standing position that notification should be direct, such as by telephone, letter, email or in person.[7] Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people[8]. It is also IPC's position that notification should be provided to those impacted within a reasonable timeframe.

[7] Privacy Breaches: Guidelines for Public Sector Organizations | Information and Privacy Commissioner of Ontario (ipc.on.ca).
[8] Privacy Breaches: Guidelines for Public Sector Organizations | Information and Privacy Commissioner of Ontario (ipc.on.ca).

At this time, although the *Act* does not require an institution to notify affected individuals of a privacy breach, it is a best practice to notify individuals impacted by a breach. Institutions are encouraged to considering the number of individuals, sensitivity and the potential for abuse of the information at issue when deciding whether to notify. I encourage TPL in the future to notify individuals whose personal information has been breached in a timely manner.

Based on the eventual notice to all affected parties, directly or indirectly, I am satisfied that there are no remaining issues for this section.

Issue 4: Did the TPL take reasonable remedial measures to address the breach?

The IPC has published Privacy Breaches: Guidance for Public Sector Organizations (the Privacy Breach Protocol) explaining best practices for institutions to respond to privacy breaches addressing the steps to take to identify the scope of the breach, contain it, and notify those affected. It also emphasizes how to reduce the risk of future privacy breaches, including implementing preventative and remediation measures, such as training.[9]

Prevention

Considering that the threat actor(s) was in TPL's network for a significant period, since August 3, 2023, and went undetected until October 28, 2023, is concerning, even acknowledging that the threat actor was most active in the immediate lead up to its attack in late October 2023.

The IPC is future-oriented and encourages organizations to implement remedial measures to prevent privacy breaches. In this case, it is important that TPL ensure it has adequate measures in place to prevent unauthorized access to records. To detect, prevent and recover from a ransomware attack, if not already implemented, I suggest implementing the following:

- **Maintain regular backups** of information and systems in an offline environment.
- **Monitor the integrity of records** for irregular changes to large numbers of files or to highly sensitive information.
- **Detect the unauthorized use of tools and application programming interfaces** (APIs) that encrypt data.
- Use data loss prevention tools to log, monitor, and block network traffic of irregular file transfers to untrusted destinations or known file upload websites.
- **Configure computers** (user workstations, servers, and cloud infrastructure) **beyond default settings** to log a wide range of events and information. Actions that will help to ensure breach investigations have access to more detailed information include:
    - Taking steps to prevent logs from being modified, overwritten, or deleted without authorization after they are created.
    - Developing a retention schedule for event logs.

[9] Privacy Breaches: Guidelines for Public Sector Organizations | Information and Privacy Commissioner of Ontario (ipc.on.ca).

- **Combine event logs** from across your organization's Information Technology (IT) assets (including cloud infrastructure) into a centralized location. Consider using a security information and event management solution to develop a clearer picture of a ransomware attacker's activity.[10]

TPL stated that in March 2023, members of the IT team and TPL Marking and Communications team participated in a ransomware attack tabletop exercise which was used to further develop the TPL Major Cyber Security Incident Playbook.

TPL reported that staff complete cybersecurity awareness training on an annual basis. The subjects covered in the training include password security, social engineering, ChatGPT, multi-factor authentication (MFA), privacy by design, social media frauds and phishing attacks. Upon completion, staff are required to respond to an evaluation of their understanding of the training. TPL stated it performs simulated phishing attacks on staff annually, to assess their awareness of how to respond.

I recommend that TPL review its current privacy training program and revise it as necessary to ensure that it provides adequate and specific privacy protection against unauthorized accesses to personal information within its databases. The IPC strongly recommends that TPL keep up to date with best practices and adopt an industry standard cybersecurity framework along with investing in measures to address serious malicious threats.

TPL reported that the City's Council directed them on May 22 and 23, 2024, to formulate organizational cyber security frameworks to align with the City's over arching cyber security objectives, to establish international cyber security frameworks, including National Institute of Standards and Technology (NIST), ISO 207001 and other such frameworks, and the City's Digital Infrastructure Strategic Framework.

To prevent unauthorized access to systems and information, TPL advised it has the following security measures in place:

- The principle of least privilege is applied.
- Protective controls on accounts, servers and assets including MFA.
- Strong password policy with password lockout for multiple incorrect attempts.
- Firewalls.
- Up to date encryption on enterprise applications along with the deployment of extended validation certificates on all external hosted web sites.
- Remote access to enterprise applications has been enhanced with improved security.

Incident Management

TPL indicated that it has had a privacy breach protocol in place since 2008 and was revised in 2024. During the incident response, TPL's investigation included a review of Windows event logs, application logs, firewall logs, memory logging, internet service provider logs and endpoint

[10] See IPC Fact Sheet: fs-tech-how-to-protect-against-ransomware.pdf (ipc.on.ca)

detection and response telemetry. TPL's investigation also included antivirus scanning and persistency checks (autoruns, task schedulers, and services). TPL used a software to aggregate and analyze logs from endpoint devices to evaluate the presence of residual malware. During service recovery, TPL monitored network traffic to ensure no residual activity was occurring within the data centre while containment and recovery processes were underway. TPL advised that its investigation also relied upon a file list and proof of theft provided directly by the threat actor(s).

Ransomware Attack

TPL advised that it improved its policies and procedures around logging, monitoring system events and detecting potential security concerns by adopting a security information and event management system to aggregate event logs from critical security systems for integrated monitoring. TPL indicated that it has also deployed an endpoint detection and response solution throughout its network along with network segregation and/or segmentation.

To detect unauthorized or anomalous changes to file systems (i.e. file integrity monitoring), TPL has an intrusion detection system in place to monitor for attempts at unauthorized access and abnormal behaviour across endpoints within its network. To protect TPL's network from minor to severe data exfiltration, TPL enhanced network security policies to mitigate unauthorized lateral data movement between systems. TPL submitted that file sharing protocols have been limited where required and deprecated file sharing protocols have been disabled. With respect to backup recovery, TPL's backup and recovery services were not compromised during the cyber security incident. TPL reported that all data was recoverable up to the date of the cyber security incident. Following this incident, TPL advised that its backup and recovery services have been enhanced with a new solution.

Once the potential ransomware attack was detected, TPL reported it immediately isolated backup devices and secured them from the network. TPL submitted that its backup architecture was not compromised, and no backup data repositories or catalogues were compromised. Upon isolation, TPL advised that service restoration was initiated by leveraging the backup environment to restore systems from its state prior to the cyber security incident. TPL stated that its electronic records are backed up regularly.

Remote Exploit

TPL stated that ransomware was installed via an unauthorized remote access tool by the threat actor(s) on an unpatched external-facing system. To reduce the organization's attack surface relating to remote exploits, standard server hardening policies and configurations have been applied to its systems with firewalls being configured to expose only operationally necessary ports between systems. With respect to vulnerability and patch management policies and procedures, TPL advised that all enterprise applications have been upgraded onto the clean network. TPL indicated that up to date security patches were applied to server operating systems and endpoint devices during the recovery process.

TPL's threat intelligence capability included adopting modern technologies to protect its network against threats. TPL advised it receives regular security updates from the City's Office of the Chief

Information Security Officer. TPL submitted its IT leadership staff regularly attend Canadian Cyber Security Centre Threat Briefings every two weeks. In addition, TPL's Manager of IT Security maintains ongoing awareness of cybersecurity issues and trends and shares relevant reports with the broader IT leadership team. Furthermore, an annual cybersecurity update is presented to its Board of Directors.

CONCLUSION:

After considering the circumstances of this reported breach and the actions taken by TPL, I am satisfied that TPL responded adequately to the breach and that no further review of this matter is required.

Based on the information considered at the early resolution stage, I have reached the following conclusions:

1. At the time of the incident, TPL did not have reasonable security measures in place to protect the personal information as required by section 3(1) of the Regulation 823 under the *Act*.
2. Upon discovery of the threat actor(s), TPL adequately determined the scope of the breach and took steps available to contain the breach.
3. TPL has taken adequate steps to notify affected individuals regarding the breach under the *Act*.
4. TPL now has reasonable measures in place to protect personal information as required by section 3(1) of Regulation 823 under the *Act*.

RECOMMENDATIONS:

Based on the above conclusions, I recommend the following:

1. Complete notification to all those individuals whose personal information was accessed without authorization under the *Act* by the threat actor(s).
2. Review its current privacy training and revise it as necessary to ensure that it provides adequate and specific privacy protection against unauthorized accesses to personal information within its networks as well as keeping up to date with cybersecurity industry standards.

To ensure TPL has reasonable security measures in place to prevent unauthorized access to personal information on its system, I encourage TPL to review the following IPC resources:

- Privacy Complaint Report MR21-00114.
- Technology Fact Sheet: How to Protect Against Ransomware, which includes cybersecurity industry frameworks and standards.
- Privacy Breaches: Guidelines for Public Sector Organizations.

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

Yours truly,

Harpreet Bains
Analyst

Cc: Shane Morganstein, Associate, BLG