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

June 12, 2025

**VIA EMAIL**

**PERSONAL AND CONFIDENTIAL**

Daniel Michaluk
Partner
Borden Ladner Gervais LLP
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Suite 3400
Toronto, ON M5H 4E3

Dear Daniel Michaluk:

**RE: Reported Breach MR24-00003**

On January 16, 2024, the Toronto Zoo (the Zoo) 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 MR23-00003 was opened by the IPC to address this matter.

The circumstances of the breach involved a ransomware attack on the Zoo that resulted in unauthorized access, encryption, exfiltration, and dark web exposure of personal information belonging to a significant number of Zoo employees, volunteers, donors, members, and guests.

## I. Summary of the Breach

On January 5, 2024, the Zoo was subject to a ransomware attack. The threat actors first gained access to the Zoo's environment on December 27, 2023, by compromising an employee's virtual private network (VPN) account. At the time of the breach, access to the Zoo's VPN was not protected by multi-factor authentication (MFA).[1]

The Zoo discovered the breach on January 5, 2024. The Zoo reported that it was unable to determine how the VPN account was initially compromised. However, the account holder "admitted to using a small number of passwords across multiple services."

The threat actors had unauthorized access to the Zoo's environment for 10 days. After gaining initial unauthorized access via the compromised VPN account, the threat actors engaged in

[1] The Zoo advised that it was in the process of implementing network upgrades to enable MFA at the time of the attack, but had not yet deployed it on its VPN.

privilege escalation techniques to gain access to domain administrator user accounts and expand their access to the Zoo's environment.

As a result of the attack, 80 Zoo servers were encrypted with ransomware and 130-140 GB of files containing personal information of Zoo employees, volunteers, donors, guests, and members (amounting to approximately 1.2 million records) were stolen by the threat actors and posted on the dark web.

## II. Issues:

As a preliminary matter, it is agreed that the Zoo is an institution under *MFIPPA*, that the data impacted by the breach included records containing personal information, and that the breach resulted in unauthorized access to and encryption, exfiltration, and dark web exposure of personal information that was in the custody or control of the Zoo.

As such, the sole issue in this report is whether the Zoo responded adequately to the breach.

**Issue 1 - Did the Zoo respond adequately to the breach?**

The IPC has published guidance on best practices for institutions to follow when responding to privacy breaches. *Privacy Breaches: Guidance for Public Sector Organizations* (the "Privacy Breach Protocol") states that in response to a breach, organizations should take steps to identify the scope of the breach, contain it, and notify the individuals who were affected. They should also investigate the breach to determine how it occurred and take steps to prevent similar breaches in future.

As part of my review of this matter, I requested information from the Zoo about its response to the breach with respect to scope, containment, notification, investigation, and remediation. Based on the information provided by the Zoo, which is set out in the following sections, I find that the Zoo responded adequately to the breach.

**Scope of the Breach:**

The Zoo reported that the breach impacted the following categories of individuals:

| Category of Impacted Individual | Types of Personal Information Compromised |
|---|---|
| 1. Zoo Guests and Members<br><br>All Zoo guests and members who purchased a general admission or membership between 2000 to April 2023.<br><br>Category size: 640,000 individuals | Transaction data including first and last names, and in some records, street address information, phone numbers and e-mail address information[2]; and (only for guests and members making credit card transactions between January 2022 and April 2023), the last four digits of credit card |

[2] Approximately 1.2 million records containing this information were exposed, with an estimated 50 percent duplication rate and approximately 27,000 records about groups (including businesses, schools, etc.).

| Category of Impacted Individual | Types of Personal Information Compromised |
|---|---|
| | numbers (both active[3] and expired) and associated expiration dates.[4]<br><br>In addition, a smaller subset of this group (compromised of 302 organizations and two individuals) had their full expired credit card numbers and expiry dates exposed.[5] |
| 2. Donors<br><br>All donors who made monthly donations to the Zoo Wildlife Conservancy in January 2024.<br><br>Category size: 145 individuals. | Names and personal banking information. |
| 3. Volunteers<br><br>Individuals who volunteered at the Zoo between September 26, 2022, to April 29, 2023.<br><br>Category size: 97 individuals. | Names, birthdates, email address, driver's licence information, home address, and telephone number. |
| 4. Zoo Employees<br><br>All current, former, and retired Zoo employees dating back to 1989.<br><br>Category size: 5,300 individuals. | Names, earnings information, social insurance numbers, birthdates, telephone numbers, and home addresses. |

Based on the information provided by the Zoo, I am satisfied that the Zoo took reasonable steps to determine the scope of the breach and has provided adequate information about the number of individuals affected by the breach and the types of personal information exposed.

**Discovery and Containment:**

The Zoo reported that it first discovered the incident in the early morning of January 5, 2024, when Zoo technical staff noticed that various network services were down. The Zoo later discovered a ransom note.

[3] The Zoo reported that as of January 1, 2024, the month the breach occurred, the impacted data set contained 86,213 active credit cards. As of January 1, 2025, the impacted data set contained 54,146 active credit cards.
[4] Approximately 114,927 records containing this information were exposed.
[5] Approximately 304 records containing this information were exposed.

The Zoo reported that it took the following steps after the breach was discovered to contain the breach and eradicate the threat:

- Restricted all internet traffic;
- Installed advanced endpoint detection across the network;
- Decommissioned 78 servers and built 34 new servers in a secure, clean environment;
- Wiped and re-imaged all client devices;
- Restored data from available clean backups (subject to monitoring upon initiation);
- Rotated all passwords and with an updated and strengthened password policy; and
- Re-initiated services based on expert sign off.

Based on the information provided by the Zoo about its containment efforts, it appears that the Zoo took reasonable steps to contain the breach following its discovery. However, the IPC notes that as of this time the stolen information at issue remains indexed and linked on the dark web, and therefore the incident remains uncontained. The Zoo has advised that the links to the impacted data on the threat actors' leak site are currently inactive, and have been for some time, but this could change.

**Notification:**

The Zoo engaged in the following efforts to notify the affected individuals of the breach.

Initial Notice to the Public:

On January 8, 2024, the Zoo posted a general notice of the incident to its website, letting the public know it was experiencing a ransomware/cyber incident, and that it was investigating the impact, if any, to guest, member, and donor records.[6] It also shared this notice on its social media accounts.

Notice to Employees:

*General Notice to Employees*

On January 17, 2024, the Zoo posted an update to its website and social media accounts confirming that some personal information of current, former, and retired Toronto Zoo employees (dating back to 1989) had been stolen.[7] The Zoo advised that the stolen information included past earnings information, social insurance numbers, birthdates, telephone numbers, and home addresses. The Zoo offered current, former, and retired Zoo staff complimentary two-year credit monitoring services, and provided contact information for those who wanted to sign up for it.

The Zoo also posted answers to 18 FAQs that addressed issues such as the scope of the breach and the steps individuals could take to protect themselves.[8]

[6] https://www.torontozoo.com/mediaroom/press2024/20240108#press
[7] https://www.torontozoo.com/mediaroom/press2024/20240117#press
[8] https://www.torontozoo.com/cyberincident

*Direct Notice to Employees*

In addition to the general notice to employees, the Zoo directly notified all 444 current Zoo employees who were impacted by the breach via Zoo email accounts on January 17, 2024. Further, on January 17, 2024, the Zoo directly notified 1,077 affected former employees who were employed by the Zoo within the past five years[9], by email or mail, based on available contact information.

The direct notice letters to employees included details about the incident, the types of information stolen, offered credit monitoring services, and provided contact information for follow up questions.

Of the 5,300 total employees that were impacted by this breach, 1,521 were sent a direct notice.

Notice to Donors

The Zoo directly notified impacted donors by letter on January 19, 2024.

The direct notice letters to donors included details about the incident, the types of information stolen, offered credit monitoring services, and provided contact information for follow up questions.

Notice to Volunteers

The Zoo's general notice of the incident dated January 17, 2024, noted that a limited number of Zoo volunteers were impacted and that confidential personal information may have been stolen.

Further, on January 18, 2024, the Zoo directly notified all impacted volunteers by email. The direct notice letters to volunteers included details about the incident, the types of information stolen, offered credit monitoring services, and provided contact information for follow up questions.

Notice to Zoo Members and Guests

*Direct Notification to Full-Credit Card Group*

Between October 28, 2024, and November 1, 2024, the Zoo directly notified 304 Zoo guests and members who had their full expired credit card information exposed (the full credit card group). The direct notice letters to these individuals included details about the incident, including that the information at issue had been posted on the dark web, the types of personal information stolen, and provided contact information for follow up questions.

The notice letter to this group of individuals was the first notice letter from the Zoo that included information about the dark web leakage, as all other direct notices pre-dated this finding, and the

[9] The Zoo advised that it selected five years as the cutoff date because it judged its contact information for employees who departed the Zoo more than five years earlier to be insufficiently reliable.

Zoo did not update its general website notices to include this information upon discovering it in February 2024.

*General Notification to Zoo Guests and Members*

Initially, the Zoo decided not to notify the impacted Zoo guests and members of the breach, aside from the full credit card group, based on its assessment that there was no reasonable risk of significant harm to these individuals as a result of the breach. Accordingly, the Zoo deemed notification to this group to be unnecessary.

After discussions with the IPC about this, where it was recommended that the Zoo should notify this group of individuals that their personal information was stolen and posted on the dark web, the Zoo agreed to issue a general notice to Zoo guests and members. Given the large scope of this group (approximately 640,000 individuals) the IPC notes that resort to a general notice for this group was reasonable in the circumstances.

Accordingly, on February 28, 2025 (over a year after the breach was discovered), the Zoo issued a general notice to Zoo guests and members on its website and social media accounts.[10] The general notice included details about the breach, including that the stolen personal information was posted on the dark web, the categories of Zoo guests and members that were impacted, the types of personal information impacted, the steps individuals could take to protect themselves, that the breach had been reported to the IPC, and contact information of the person at the Zoo individuals could contact for follow up questions.

Based on the information before me about the Zoo's notice efforts, I am satisfied that the Zoo took reasonable steps to notify the various groups of affected individuals about the breach. However, the IPC notes that the Zoo should have notified Zoo guests and members of the breach much sooner. Further, the Zoo should have updated its online notices to include that the stolen personal information had been posted to the dark web upon discovering this in February 2024.

**Investigation:**

The Zoo reported that it retained third-party cyber security experts to help it investigate the circumstances of breach, including threat actors' point of entry to the Zoo's environment, the actions taken by the threat actors in the Zoo's environment, and the impact of attack on the Zoo's systems and records. The results of the investigation are set out as follows.

*Point of Entry*

The Zoo advised that the threat actors first gained access the Zoo's network on December 27, 2023, via a compromised VPN account.[11] The Zoo determined this to be the point of compromise by reviewing VPN session logs, which showed that the compromised VPN account was used by the threat actors based on its correlation with other evidence of malicious activity.

[10] https://www.torontozoo.com/mediaroom/press2025/20250228#press
[11] The account belonged to a non-IT staff member. It did not have domain administrator privileges.

The Zoo does not know how the account was initially compromised by the threat actors, but shared the following details:

- As part of its investigation, the Zoo spoke with the account holder, who did not recall any suspicious activity related to their account, but admitted to using a small number of passwords across multiple services;
- The Zoo was unable to confirm the date of the employee's last password change;
- The account was not protected by MFA at the time of the breach; and
- The Zoo reviewed the account to look for phishing e-mails, but found none, and there was no evidence of brute forcing.

*Actions Taken by Threat Actors in Zoo's Environment*

The Zoo provided the following timeline of the threat actors' activities in its environment:

- On December 27, 2023: the threat actors used the compromised VPN account to establish a VPN session. The threat actors authenticated to various systems, enumerated domain administrator accounts, escalated privileges by changing administrator passwords, and used credential dumping tools to extract additional credentials from memory.

- Between December 27, 2023, and January 5, 2024: the threat actors used the additional accounts they compromised to establish Remote Desktop Protocol sessions to systems in the Zoo network.

- On January 5, 2024: the threat actors installed and ran file transfer and compression utilities[12], accessed various files and folders, and created two archive files[13] containing millions of records of personal information.[14] The threat actors then deployed ransomware to various systems in the Zoo's environment.

*Impact of Attack on Zoo's Systems and Records*

As a result of the attack, 80 on-premises servers were encrypted with ransomware and 130-140 GB of data was stolen from the Zoo's environment. This amounted to approximately 1.2 million records of personal information.

The Zoo explained that while 80 servers were encrypted, its investigation determined personal information was only stolen from one server, a finding that was consistent with the threat actors claim and apparent motive. The server from which personal information was stolen was a windows

[12] A file transfer utility is a tool that enables users to transfer files from one computer or device to another over a network or the internet. A file compression utility is a tool that reduces the size of files to make them easier to store or transfer.

[13] An archive file is a single file that that contains one or more files or folders that have been bundled together, often for easier storage, organization, or transfer.

[14] The Zoo advised that the archive files were unavailable for analysis at the time of investigation (likely due to threat actor obfuscation), but the file names matched the parent-level directors accessed by the threat actors, which indicates the threat actors stole what they accessed.

file server that contained human resource files and a copy of the Zoo's old customer information system ("Admits").

The Zoo advised that the other 79 encrypted servers ran network services, and one included a backup copy of the Admits database. The Zoo reported that other than the copy of the Admits database, any personal information in these 79 servers was likely about Zoo employees and their use of the Zoo's IT services.

Initially, the Zoo's investigation into the scope of personal information in the stolen records proved difficult due to its lack of access to this data. This lack of access was the result of the threat actors' encryption activities, and due the fact that the backup copy of these records was accidentally written over by the Zoo.[15]

To overcome these issues, the Zoo made several attempts to download the stolen data from the threat actor's leak site. The downloads failed several times. Once it was able to download the full stolen dataset on May 30, 2024, the Zoo analyzed it to determine the scope of impacted individuals and types of personal information impacted. The Zoo completed this analysis on or around August 2024. The results of this analysis are set out above under "Scope."

Based on the information provided by the Zoo, I am satisfied that Zoo took reasonable steps to investigate the circumstances of the breach and has provided sufficient information about its root cause, the series of actions taken by the threat actors in its environment, and the impact of the attack on the Zoo's systems and records.

**Remediation:**

The IPC's *Privacy Breach Protocol* 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 information, and corrective action to prevent similar breaches in the future.

*Circumstances of the Breach*

The circumstances of this breach revealed that, at the time of the breach, there were several gaps in the Zoo's security and information practices that left the Zoo vulnerable to an attack of this nature and magnitude. These gaps include:

- Access to the Zoo's VPN was protected by password alone, without MFA. This significantly reduced the security of remote access and enabled the threat actors to authenticate using compromised credentials. The lack of MFA represents a critical gap in the Zoo's access management practices at the time of the attack.

- The compromised employee account used a reused password across multiple platforms, increasing the likelihood that the VPN credentials were obtained through credential stuffing or another form of reuse-related compromise.

[15] The Zoo explained that it did not follow proper procedures for rotating and storing the back-up tapes.

- The threat actors remained undetected within the Zoo's environment for approximately 10 days, raising questions about potential deficiencies in its system logging, monitoring, and anomaly detection practices at the time of the attack.

- The Zoo retained transaction records containing personal information for longer than it was required to by its retention by-laws, reflecting a failure to dispose of personal information it was no longer required to keep.[16] The number of individuals affected by the breach and scope of information stolen could have been much smaller had the Zoo not retained this personal information unnecessarily. It is unclear if there was also over-retention of other affected record types, such as employee records.[17]

- At the time of the breach, the Zoo was unaware it continued to store partial and full credit card numbers, and its initial public notice of the breach stated that it did not currently store any credit card information. This indicates further deficiencies in the Zoo's information management practices at the time of the attack.

- The Zoo's file server backup was not stored in a secure, offline (immutable) environment, allowing the threat actors to encrypt it during the attack. This reflects a gap in the Zoo's backup and recovery strategies at the time of the attack.

- A backup of the Zoo's Admits database was stored on a system not designated for that function, highlighting further weaknesses in the Zoo's records and information management protocols.

- The Zoo did not have a records management policy applicable to convenience copies of records, which resulted in unnecessary duplication and retention of personal information.

- 80 Zoo servers were successfully encrypted by the threat actors during the attack, suggesting that the Zoo's network segmentation was insufficient to prevent lateral movement within its environment.

- Approximately 130–140 GB of data was exfiltrated from the Zoo's systems, raising questions about the adequacy of the Zoo's data loss prevention measures at the time of the attack.

---

[16] At the time of the breach, transaction data was required to be retained for six years from the applicable transaction date. However, the Zoo retained transaction data dating back to 2000. The Zoo advised that it retained this information within a full archive of its old Admits database. The Zoo did not parse the data in this archive to retain only the six years of data required by its retention by-law, which resulted in significant over retention.

[17] The Zoo was asked if it complied with its retention periods applicable to employee records. The Zoo advised that it had not fully mapped this exposed information to the applicable record series that applied at the time of the incident, and that doing so would be impracticable. However, it noted that a significant amount of the employee exposure was derived from records retained in compliance with retention periods that were very lengthy, and that have now been replaced with shorter retention periods. It did not specifically confirm to the IPC if any employee exposure was the result of over-retention.

- At the time of the incident, the Zoo did not have a comprehensive cybersecurity program in place, underscoring broader gaps in its cybersecurity governance and incident response preparedness.

*Review of and Updates to Practices and Policies*

The Zoo reported that at the time of the attack, it had reasonably assessed its vulnerabilities, had plans to address them despite its limited resources, and was working on implementation. For instance, the Zoo advised that it had new firewalls in place and had partly implemented new segmentation, which limited the blast radius of the attack. Further, despite the expense of endpoint detection, it had reached an arrangement with the City to obtain and deploy advanced endpoint detection, which was scheduled for rollout in January 2024. Last, the Zoo noted that the enforcement of multi-factor authentication rested on the rollout of a new VPN and Active Directory. This rollout was in progress in December 2023, when the Zoo ran into technical problems before the holidays.

The Zoo reported that following the breach, to reduce the likelihood of a similar incident, it made the following improvements to its security posture:

- Multi-factor authentication implemented for all VPN accounts
- New advanced endpoint detection (with monitoring 24/7)
- Newly enhanced network segmentation
- New, state of the art, firewalls and VPN
- Newly tightened privileges regarding file access
- Newly enhanced password policy
- New privileged access management server logs vendor and administrator access across network
- New system to push patches to all systems and new development environment to facilitate testing of patches
- New, automated backup system and backup testing practices
- Updated cyber security training
- Enhanced physical access controls

Additionally, the Zoo advised that in June 2024, it entered into a memorandum of understanding with the City Chief Information Security Officer (CISO) that contemplates receipt of the following cyber security services[18]:

- Threat Risk Assessment
- Penetration Testing
- Application Security Consultation
- Identity and Access Management Review
- Privacy Impact Assessment
- Third-Party Risk Assessment
- Business Continuity and Disaster Recovery Planning
- Cyber Awareness Training

[18] The Zoo shared additional details with the IPC regarding the implementation of these services. However, these details will not be shared publicly for security reasons.

- Phishing Campaigns
- Assessment of Critical Cyber Controls
- Cyber Policies
- Vulnerability Assessment and Monitoring
- Patch and Vulnerability Advisory
- Managed Email Security
- Endpoint Detection and Response
- Log Ingestion and Monitoring
- Tabletop exercise with CISO

Further, in May 2024, the Zoo implemented a new records classification and retention schedule (By-Law 848-2024, replacing former By-Law 87-92) to better manage the records and information created or received by the Zoo. This by-law establishes retention periods for records of personal information and authorizes the destruction of such records once the retention period has expired.

Notable changes in this by-law include newly shortened retention periods for certain employee record types, and a requirement that convenience copies of records be tracked and destroyed or disposed of no later than the retention period of the original document.

Additionally, the Zoo advised that it is currently working towards achieving secure and timely destruction of paper records that include personal information. The Zoo has assigned responsibility for tracking retention periods to a clerk, who will bring record disposal requests to the attention of record series owners for disposal authorization. The Zoo advised that applying this approach to electronic records is a work in progress, with responsibility assigned to the Chief Human Resource Officers working in collaboration with the Chief Transformation Officer.

Regarding convenience copies of records, the Zoo advised that it is now operationalizing the commitment in By-Law 848-2024 to manage convenience copies so they are destroyed in accordance with the schedule. The Zoo advised that it will work the deletion of convenience copies into an annual "spring cleaning" event to be implemented, and in doing so, will (a) identify and reinforce the staff duty to delete personal information that is currently set out in its Protection of Privacy Policy, and (b) specifically ask staff to purge convenience copies of records containing personal information from personal file shares and confirm to their supervisors that this has been done. The Zoo will support the periodic purging of convenience copies that contain personal information with an annual system audit.

Based on the information provided by the Zoo, I am satisfied that the Zoo has taken reasonable steps to assess the circumstances surrounding the breach and has implemented reasonable remedial measures to reduce the likelihood of a similar incident occurring in the future, including enhanced security controls and improved record and information management practices.

The IPC notes that the circumstances of this breach should serve as a cautionary reminder to all *MFIPPA* institutions of the critical importance of having security best practices in place, including MFA, and the importance of adhering to retention schedules for records of personal information. The creation and adherence to retention/disposition schedules is a fundamental component of robust security and information practices that must not be overlooked. In this case, had the Zoo

adhered to its retention schedules, the scope of the breach could have been substantially reduced. Further, had MFA been in place at the time of the attack, this breach may have been prevented altogether.

## III. Conclusion and Recommendations

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

Specifically, I am satisfied that the Zoo took reasonable steps to contain the breach, determine its scope, and notify the affected individuals, though it should have completed notice to the Zoo member and guest group much sooner. I am further satisfied that the Zoo took reasonable steps to investigate the circumstances of the breach, and that it has implemented reasonable measures to prevent a similar breach from occurring in the future. However, the IPC may re-open this matter if additional information comes to our attention suggesting a need for further inquiry.

Based on our review of this matter, the IPC makes the following recommendations to the Zoo:

1. Perform a comprehensive threat risk assessment and penetration test on the Zoo's environment as soon as possible, and on a regular basis thereafter. This will allow the Zoo to proactively identify, assess, and address potential security vulnerabilities in its environment.

2. Conduct regular reviews of the Zoo's record retention schedules to ensure they remain compliant with legislative requirements, industry best practices, and are reflective of the Zoo's current operational needs. By-law 848-2024 replaced an older record retention by-law that was over 30 years old, and that was established to deal with paper records, no longer reflected the Zoo's organizational structure or operation, and included record series that were no longer relevant. Going forward, regular reviews of the Zoo's new record retention by-law will help avoid reoccurrence of these issues.

3. Amend the Zoo's record retention by-law to impose a requirement that records containing personal information be securely destroyed upon expiration of the applicable retention period, rather than just "authorizing" their destruction. Likewise, update the Zoo's *Protection of Privacy Policy* to explicitly require records of personal information to be disposed of when their retention period set out in By-law 842-2024 expires.

4. Ensure adherence to the Zoo's retention and disposition schedules applicable to records of personal information through regular, ongoing monitoring and compliance audits. Timely and appropriate destruction of records is an essential component to avoiding unnecessary retention of personal information, and to reducing the impact of privacy breaches such as this one.

5. Complete a review of the Zoo's record holdings containing personal information against the Zoo's revised retention schedules and rectify any instances of over-retention at the earliest reasonable opportunity.

6. Develop and disseminate clear guidance to staff on what constitutes a convenience copy of a record. Ensure that all staff are trained to identify and manage these copies appropriately to reduce redundancy and support data minimization.

The IPC also urges the Zoo to review and follow the guidance set out in the IPC's guidance documents *Technology Fact Sheet: Protecting Against Ransomware*, *Technology Fact Sheet: Protect Against Phishing*, *Privacy Breaches: Guidelines for Public Sector Organizations*, and *Improving Access and Privacy with Records and Information Management* to ensure that its practices, policies, and procedures are sufficient to minimize the risk of a similar breach in the future.

The IPC thanks the Zoo for its 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 by the IPC.

Yours truly,

Denise Eades
Analyst