Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MR21-00090

SAULT STE. MARIE POLICE SERVICES BOARD

December 10, 2024

Summary: The Sault Ste. Marie Police Services (the police) reported to the Office of the Information and Privacy Commissioner of Ontario that their network servers were infected with ransomware and that, as a result, records of personal information stored on data drives on the servers were encrypted.

In response, the police took steps to contain, investigate, remediate and inform local residents about the ransomware attack. However, the police did not believe that the attack resulted in a privacy breach because their investigation determined that the information was encrypted in place, and neither obtained or exfiltrated by the threat actor.

In this report, I find that the threat actor's encryption of the data drives affected the personal information stored on them by making this information inaccessible to the police. I also find that the ransomware attack resulted in an unauthorized use of personal information and, therefore, a privacy breach under the *Municipal Freedom of Information and Protection of Privacy Act*.

I am satisfied with the steps taken by the police to contain the breach. Although the police informed the public of the breach through a press release issued at the time of the ransomware

attack, I find that there would be no useful purpose in deciding whether they should renotify affected individuals given the passage of time since the breach. I am not entirely satisfied with the police's investigative and remedial steps because they have not reviewed their policies and practices in protecting personal information. As such, I find that the police have not responded adequately to the breach and recommend that they conduct this review.

Further, it appears that the police understand the nature of their information holdings, the threats posed by ransomware attacks and the steps required to mitigate these attacks. However, despite requests, the police did not provide this office with materials relating to their privacy training practices and, therefore, I could not evaluate the reasonableness of these practices which are important for reducing the risk of a threat actor gaining unauthorized access to an institution's records. Because of this, I am not satisfied that the police haves reasonable measures in place to prevent unauthorized access to records as required by section 3(1) of Regulation 823 under *MFIPPA* (security of records) and recommend that they ensure that their training materials comply with this section.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56; sections 2(1) and 31; General, R.R.O. 1990, Reg. 823, under the *Municipal Freedom of Information and Protection of Privacy Act*, section 3(1); *Personal Health Information and Protection Act, 2004*, S.O.2004, c.3, Sched. A., section 2 (definitions); and General R.R.O. 1990, Reg. 460, under the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31.

Orders, Decisions and Investigation Reports Considered: Investigation Report I93-044M, Privacy Complaint Reports MI10-5 and PR16-40; and PHIPA Decisions 253, 254 and 255; and CYFSA Decision 19.

BACKGROUND:

[1] The Sault Ste. Marie Police Services reported to the Office of the Information and Privacy Commissioner of Ontario (IPC) that their network servers were attacked by ransomware on August 26, 2021.

[2] The police discovered the attack after Remote Monitoring and Management (RMM) software installed on their computer system alerted their Information Technology (IT) staff that two computer servers went offline.

[3] The attack encrypted records stored on data drives on the servers and, consequently, locked the police out of these records. The affected information related to human resources, finance services, public complaints, freedom of information requests, the criminal record check database, taxi/limo administration, the warrant shared database, closed-circuit television footage, audio from the police's communication system and the police's intranet.

[4] In response to the attack, the police immediately shut down their servers and took steps to contain it. The police also informed local residents about the attack,

shortly after it occurred.

[5] Despite these steps, the matter moved to the Investigation Stage of the IPC's complaint process because this office had concerns about the police's response to the attack, as well as the measures in place to prevent unauthorized access to records within the police service.

[6] As part of my investigation, I requested and received written representations from the police. Wherever possible, I have left out references in this report to the specifics of the police's cybersecurity safeguards, as per the police's request.

PRELIMINARY ISSUE:

[7] The police advised that the encrypted records contain information described in paragraphs (a) to (h) within the meaning of "personal information" under section 2(1) of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*).

[8] Therefore, as a preliminary matter, I find that these records contain "personal information" within the meaning of section 2(1).

ISSUES:

1. Did the police respond adequately to the breach?

2. Do the police have reasonable measures in place to prevent unauthorized access to records?

DISCUSSION:

Issue 1: Did the police respond adequately to the breach?

[9] Although the police reported the ransomware attack to this office, in their view, the attack did not result in a privacy breach under *MFIPPA*. The police take this position because their investigation into the attack found that the affected information was encrypted in place and neither obtained nor exfiltrated by the threat actor.

[10] Respectfully, I disagree with the police's position that the attack did not amount to a privacy breach.

[11] Section 31 of *MFIPPA* prohibits the use of personal information by an institution except in certain circumstances. This section states:

> An institution shall not use personal information in its custody or under its control except,
>
> (a) if the person to whom the information relates has identified that information in particular and consented to its use;
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
>
> (c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the *Freedom of Information and Protection of Privacy Act*.

[12] Accordingly, a use occurring outside of these circumstances would not be authorized under *MFIPPA*.

[13] Although *MFIPPA* does not define the term "use", the modern approach to statutory interpretation cited by the Supreme Court of Canada in *Bell ExpressVu Limited Partnership v. Rex*, 2002 SCC 42 (CanLII) at para. 26 and *TELUS Communications Inc. v. Wellman*, 2019 SCC 19 (CanLII) at para. 47, is set out in Elmer Driedger's text on *Construction of Statutes* (2nd ed. 1983), which states:

> [T]he words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament".

[14] Subsection 64(1) of the *Legislation Act, 2006* also applies to the interpretation of an Ontario statute. This subsection requires that the legislation be given "such fair, large and liberal interpretation as best ensures the attainment of its objects."

[15] Other statutory definitions within the privacy and access context can be informative in determining how the Legislature intended the term "use" to be interpreted. In particular, section 2 of the *Personal Health Information Protection Act, 2004* (*PHIPA*) defines "use" as follows:

> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning.

[16] In my view, using this broad definition of "view, handle or otherwise deal with the information" to interpret the term "use" in section 31 is consistent with

the scheme and objects of *MFIPPA*. These objects can be derived from the purpose provisions under section 1 of *MFIPPA* that includes among its purposes:

> (b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

[17] In this matter, the police reported that the threat actor encrypted records of personal information making the information inaccessible to the police. In my view, transforming the accessibility of the information was a kind of "handling" of or "dealing with" that information by the threat actor and, therefore, a use within the meaning of section 31 of *MFIPPA*.

[18] As there is no evidence before me that this use by the threat actor occurred within one (or more) of the permitted circumstances set out under section 31 (indeed the available evidence suggests the opposite given the nature of this ransomware attack), I, therefore, find that it was an unauthorized use of personal information.

[19] For these reasons, I find that the ransomware attack resulted in a privacy breach under *MFIPPA*.

[20] Moreover, a series of decisions[1] issued by this office considered different situations involving cyberattacks on organizations. In each of these decisions, the adjudicator considered (among other issues) whether the cyberattack at issue resulted in an unauthorized use of the affected individuals' personal health information or personal information.

[21] Three of these decisions concerned ransomware attacks involving the encryption of the organization's servers by a threat actor.[2] In each of these decisions, the adjudicator found that the encryption affected the information in the servers by making the information unavailable and inaccessible to authorized users and, therefore, amounted to an unauthorized use of the information.

[22] Although, these decisions were not decided under *MFIPPA*, they concern the security and protection of electronic personal (health) information and, therefore, in my view, are informative here. They support my above conclusion that the encryption event at issue in this case was a use of personal information, and that such use was unauthorized.

[23] Accordingly, it must be determined whether the police responded adequately to the breach. To that end, the IPC's "Privacy Breaches: Guidelines for

---

[1] See PHIPA Decisions 253, 254 and 255, and CYFSA Decision 19.
[2] See PHIPA Decisions 253 and 254, and CYFSA Decision 19.

Public Sector Organizations" (the IPC's Privacy Breach Guidelines)[3], which provides institutions with guidance on how to respond to privacy breaches, is informative.

[24] More specifically, these guidelines recommend steps that institutions should take to contain the breach, investigate it, reduce the risk of a similar breach from reoccurring, as well as notify affected individuals.

Containment

[25] To contain a breach, institutions should identify the nature and scope of the breach, determine what personal information is involved, and take containment measures, which include ensuring that no personal information has been retained by an unauthorized recipient and that the breach does not allow unauthorized access to any other personal information.[4]

[26] In addition to shutting down their network servers and restricting access to them, the police contacted and worked with certain law enforcement organizations and third-party organizations to investigate the ransomware attack, rebuild and repair their IT infrastructure, replace their network servers and clean any accessible data on the computers of individual users.

[27] According to the police, to date, none of the affected personal information has been exfiltrated or made public, and the purpose of the attack appears to have been to hold it ransom.

[28] For these reasons, I am satisfied with the steps taken by the police to contain the breach.

Notification

[29] The police issued an August 30, 2021, news release giving notice that they "became aware of a virtual ransomware attack on [their] systems" on August 26, 2021, and that their "(IT) staff are working through the attack to regain access to effected [sic] systems."

[30] In addition, publicly available meeting minutes of the Sault Ste. Marie Police Services Board dated October 28, 2021, and November 25, 2021, and news articles dated February 25, 2022, and May 5, 2022, all referenced the attack.

[31] The October 28, 2021, meeting minutes state:

---

[3] The IPC's Privacy Breach Guidelines is available at: https://www.ipc.on.ca/en/resources-and-decisions/privacy-breaches-guidelines-public-sector-organizations

[4] See footnote 3.

The Chief reported that there are limited reports due to the cyberattack. The data is still not available and will not be for the foreseeable future.

[32] The November 25, 2021, meeting minutes state:

> Insp. Duguay provided an update and noted the investigation into the cyberattack is still ongoing. Initially the cyberattack encrypted police services administrative and record management systems, essentially locking the Service out from its own system. The data remains encrypted, and the OPP continue to work on defeating the encryption. The Service IT Department, along with partners has worked to rebuild the networks affected by the attack. The Service is currently awaiting a security certification to be completed. Once the security certification has been issued, the Service will be able to re-establish external networks and partners.

[33] The February and May news articles gave notice that "police operations have continued throughout the cyberattack, and [that the police] are 90 per cent back to where [they] were pre-cyber attack" and that "with the effect the cyberattack had on the [police] service, there were a number of priority systems that needed to be rebuilt and restored."

[34] The police advised that no further details regarding the attack would be released because, in their view, a privacy breach had not occurred.

[35] As discussed above, I found that the threat actor's encryption of the personal information resulted in an unauthorized use of this information contrary to section 31 of *MFIPPA* and, therefore, was a privacy breach.

[36] Where a breach occurs, IPC's Privacy Breach Guidelines recommends that institutions should notify affected individuals as soon as reasonably possible of a breach where it "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."[5] However, where law enforcement is involved, institutions should ensure that notification will not interfere with any investigations.[6]

[37] Notification should "be direct, such as by telephone, letter, email or in person" and "[i]ndirect 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."7

---

[5] See footnote 3.
[6] See footnote 3.
[7] See footnote 3.

[38] Further, notification should include:

- the details of the extent of the breach and specifics of the personal information that was compromised;
- the steps taken and planned to address the breach, both immediate and long-term;
- a suggestion to take certain steps, if financial information or information from government-issued documents is involved;
- contact information for someone within your organization who can provide additional information and assistance, and answer questions; and
- a statement that they have a right to make a complaint to the IPC and how to do so.[8]

[39] In this matter, the police did not confirm the number of individuals affected by the breach, although, given the various types of personal information at issue, in my view, it likely affected many people.

[40] As the affected personal information remains encrypted and the police's investigation found no evidence of exfiltration, it is not clear whether the breach "poses a real risk of significant harm to [these individuals], taking into consideration the sensitivity of the information and whether it is likely to be misused". As such, it is not clear whether the police should have given direct notice of the breach to affected individuals in accordance with the IPC's Privacy Breach Guidelines.

[41] However, I am mindful of the fact that the police provided some notice to the public about the extent of the ransomware attack, and of the investigative and remedial steps they took to address it. I am also mindful of the fact that the breach occurred more than three years ago.

[42] For these reasons, I find that it would serve no useful purpose in recommending that the police renotify affected individuals of the breach in accordance with the IPC's Privacy Breach Guidelines and, as a result, do not need to decide whether the breach in this case met the threshold of "real risk of significant harm to the individual".

---

[8] See footnote 3.

Investigation and Remediation

[43] When investigating a breach, institutions should:

- identify and analyze the events that led to the breach;
- review their policies and practices in protecting personal information, privacy breach response plans and staff training to determine whether changes are needed; and
- take corrective action to prevent similar breaches in the future and ensure that their staff are adequately trained.[9]

[44] In this matter, the police's IT staff, as well as certain law enforcement organizations and third parties investigated the ransomware attack using certain techniques and found that the affected information was encrypted in place and neither obtained nor exfiltrated by the threat actor.

[45] Regarding the origin of the breach, the police's investigation determined that the threat actor either exploited an identified vulnerability within a software patch of an identified email server or a device(s) connected to their public-facing Internet Protocol (IP) addresses[10].

[46] With respect to remediation, the police advised that they purchased new computer networks systems, including servers, and changed their public-facing IP addresses to a different subnet to further distance themselves from where their access points were at the time of the attack. The police also advised that, following a trust restoration review by a third-party vendor, they received certification on December 1, 2021, that their rebuilt network was safe from malicious threats.

[47] Further, the police advised that they took the following remedial steps, which involve the use of cloud-based tools providing Software as a Service to ensure reliability and that they remain operational in the event of a cyberattack:

- moved from local networks to cloud-based email servers;
- enhanced and increased network segregation;
- added a network activity, server and device monitoring tool that provides real-time alerts to their IT staff and third-party consulting agency;

---

[9] See footnote 3.

[10] Generally, a public-facing IP address is an address given by your internet service provider to your network and is used to communicate over the Internet.

- added Endpoint Detection and Response to their antivirus solution for all workstations and servers that allows for faster triage and isolation should a threat actor be detected;

- enhanced their Security Operation Centre with 24-hour monitoring of server and workstation activity by a third-party vendor that provides alerts about abnormal resource usage and malicious activity; and

- changed and moved their RMM software to a hosted solution that enables high security and availability to manage all their network connected devices.

[48] To reduce the risk of a similar breach from reoccurring, the police advised that, as they continue to rebuild their databases, more ransomware attack training will be rolled out to their staff. The police also advised that they instituted monthly simulated phishing attacks through a third-party vendor, and, in June 2022, all staff were mandated to complete online training related to security awareness and phishing training.

[49] Specifically, regarding staff ransomware attack training, the police advised that, before the breach, they implemented simulated cyberattacks to train staff and that, since January 2022, these simulated attacks have been occurring monthly.

[50] Moreover, the police advised that cybersecurity awareness training is an ongoing initiative for all members and that training materials are delivered through online learning modules that are regularly updated to include emerging cybersecurity threats. The police also advised that members are immediately informed of significant or trending cyber threats.

[51] Further, the police advised that they are developing a new SharePoint "Self Help Knowledge Base" that will be made available to all staff to provide them with commonly used procedures and training videos as they are created.

[52] However, the police confirmed that they did not review their policies and practices in protecting personal information because they believe that a breach did not occur based on finding no evidence that personal information was obtained or exfiltrated due to the attack.

[53] The IPC's Privacy Breach Guidelines recommend that institutions review their policies and practices in protecting personal information following a breach to determine whether changes are needed.[11] As the police did not do this, I am not satisfied with their steps taken to investigate and remediate the breach.

---

[11] See footnote 3

[54] Accordingly, I recommend that the police review their policies and practices in protecting personal information post-breach to determine whether changes are needed in light of any lessons learned and my findings in this decision.

Issue 2: Do the police have reasonable measures in place to prevent unauthorized access to records?

[55] Above, I found that the ransomware attack resulted in unauthorized use of records of personal information.

[56] Regarding the protection of these records, section 3(1) of Regulation 823 requires that the police "ensure that reasonable measures to prevent unauthorized access to the records in [their] institution are defined, documented and put in place, taking into account the nature of the records to be protected."[12]

[57] This section does not "necessitate that every possible measure be pursued to prevent unauthorized access", rather it requires that the reasonable measures appear to be "fair and suitable under the circumstances."[13]

[58] This requirement "applies throughout the life-cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal".[14]

[59] Further, in Privacy Complaint Report PR16-40, the investigator stated the following about section 4(1) of Regulation 460 under the *Freedom of Information and Protection of Privacy Act*, which is the provincial access and privacy law equivalent of section 3(1) of Regulation 823 under *MFIPPA*:

> From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. 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.

[60] Accordingly, it must be determined whether the police have reasonable

---

[12] Section 1(b) of *MFIPPA* provides that one of the purposes of this legislation is "to protect the privacy of individuals with respect to personal information about themselves…" As such, in my view, section 3(1) of the Regulation 823 should be read as applying to privacy breaches involving unauthorized use of personal information and I note that the police did not dispute this.

[13] Investigation Report I93-044M.

[14] Privacy Complaint Report MI10-5.

measures in place to prevent unauthorized access to the affected records in the circumstances.

[61] To that end, the IPC's "How to Protect Against Ransomware" fact sheet (the Ransomware Fact Sheet)[15] is informative. This guide recommends that institutions be accountable with respect to information security by creating a foundation for this accountability, as well as formalizing, implementing, maintaining and improving this accountability.

[62] More specifically, the Ransomware Fact Sheet recommends that institutions "can reduce the likelihood and impact of successful ransomware attacks by having a strong cybersecurity program" that includes the key steps of:

- knowing your assets and information holdings across their entire lifecycle;
- understanding the ransomware threat landscape and taking steps to mitigate threats; and
- establishing a formal cybersecurity incident management program.

[63] As part of my investigation, I reviewed the police's IT and Support Services Policy Orders and Cyber Attack Response Guide.

IT Policy Order

[64] The police's IT Policy requires that staff use technology resources only for the purpose of conducting the police's business. This policy prohibits staff from uploading any software onto the police's computers unless authorized to do so where such authorization is only given after the software has been thoroughly scanned for viruses.

[65] Further, the IT Policy warns staff that they will be subject to discipline up to and including termination if they tamper with or disable any technological security devices, and that audits may be conducted to ensure compliance.

Support Services Policy Order

[66] The police's Support Services Policy outlines their quality assurance processes and establishes an Audit Committee that is responsible for overseeing these processes. This policy also requires that the police's policies are reviewed on an annual basis and that compliance auditing systems are implemented to ensure the overall integrity and effectiveness of the police.

---

[15] The Ransomware Fact Sheet is available at: https://www.ipc.on.ca/resources/guidance-for-organizations/

Cyber Attack Response Guide

[67] The police's Cyber Attack Response Guide sets out steps that their staff should take to limit the effectiveness of a cyberattack. This guide also describes indicators of an attack and the steps to be taken by staff where a workstation user clicks a dangerous link or opens an untrustworthy attachment, a server or network resource is unavailable, or a printer is printing out non-police documents.

[68] Further, the Cyber Attack Response Guide requires that malware be removed, and any identified vulnerabilities patched. Regarding recovery, this guide provides that a third-party network security consultant be contacted and a method for the consultant to monitor and scan all network traffic and systems be established.

Staff Training

[69] The police advised that they ensure that staff are made aware of their policies at new employee orientations and introductory training, as well as at annual in-service training sessions

[70] However, despite my requests, the police did not provide this office with materials relating to their privacy training practices. Without the power to compel production of this material and without the opportunity to otherwise review these practices, I am not satisfied that they constitute reasonable measures in place to prevent unauthorized access to records.

Cybersecurity Program

[71] The Ransomware Fact Sheet recommends that institutions have a strong cybersecurity program to protect themselves from ransomware attacks by taking the key steps of knowing their assets and information holdings, and understanding the threats posed by these attacks and mitigating them.

[72] With respect to these steps, the police advised that their asset inventory is maintained by their RMM software which provides hardware specifications, device serial numbers, as well as software inventory of the devices and patch levels of all their software.

[73] The police also advised that they have identified the Government of Ontario's "Corporate policy on information sensitivity classification"[16] as a document that could potentially assist them with classifying and labelling information and IT assets. This policy "outlines the requirements and best practices that the Ontario government uses to classify and secure sensitive

[16] https://www.ontario.ca/page/corporate-policy-information-sensitivity-classification#section-3.

information and information systems".

[74] Moreover, regarding risk management, the police advised that any new systems, network configurations or security measures that they implement are evaluated by the police's IT Coordinator to ensure that it meets security guidelines provided by the Ontario Police Technology Information Co-operative (OPTIC)[17] and the Royal Canadian Mounted Police. The police also advised that, before they implement or make changes to their technology, they must first inform OPTIC to have it evaluated and approved.

[75] To protect against ransomware attacks, the police advised that, daily, the servers are backed up and that the backups are encrypted and stored on a separate storage device and in a cloud redundant backup. All the police's cloud services are also encrypted and backed up to a different Canadian-based cloud data centre.

[76] Further, the police advised that all their network servers and end user workstations have antivirus software installed, and that critical patches and updates are applied regularly to the software and operating systems that they use. The police also advised that their records management data and computer-aided dispatch systems are both on separate computer systems (and, as a result, were not affected by the ransomware attack).

[77] Moreover, the police explained that all inbound and outbound email is filtered through a cloud-based email security appliance that scans, blocks, and notifies email recipients of potentially malicious emails and file types.

[78] Regarding user privileges, the police advised that they follow the principle of least privilege[18] and, as such, a user of their computer systems only has access to that which the user requires to do their work. The police also advised that users cannot execute any unapproved code or software.

Analysis

[79] The police advised that, although they had firewalls, patch management through their RMM software and traffic inspection tools at the time of the breach, the threat actor used encryption tools (built into a certain product). The police also advised that their RMM software was one of the first programs targeted by the

---

[17] OPTIC includes 8,287 officers: 2,894 from 43 municipal Ontario, Canada police agencies and 5, 393 from the Ontario Provincial Police. OPTIC is the largest data-sharing cooperative in North America. For more information, visit: https://nicherms.com/casestudy/nicherms-forms-foundation-for-the-largest-police-data-sharing-system-in-north-america/

[18] The principle of least privilege starts from the assumption that users should have limited rights to access and perform limited functions on computer systems. See the Ransomware Fact Sheet for more information about this principle.

attack and, as a result, their IT staff did not receive any further alerts about the affected servers going offline or rebooting.

[80] Although institutions "should have safeguards in place to prevent and detect the methods ransomware attackers use to get initial access to a network and take further actions,"[19] as indicated above, it appears that the police have measures in place relating to information security accountability and protecting themselves from ransomware attacks.

[81] In my view, these measures show that the police understand the nature of their information holdings, the threats posed by ransomware attacks and the steps required to mitigate these attacks. As such, I find that they are consistent with the Ransomware Fact Sheet.

[82] However, without reviewing the police's privacy training materials, I cannot evaluate the reasonableness of this measure which is important for ensuring that staff receive up-to-date cybersecurity[20] awareness training and thereby reduce the risk of attackers gaining access to their computer systems.

[83] For these reasons, I am not satisfied that the police have reasonable measures in place to prevent unauthorized access to records as required by section 3(1) of Regulation 823. Accordingly, I recommend that the police review and ensure that their training materials constitute reasonable measures to prevent unauthorized access to records.

CONCLUSIONS:

Based on the results of the investigation, I have reached the following conclusions:

1. The encrypted records contain "personal information" within the meaning of section 2(1) of *MFIPPA*.

2. The ransomware attack resulted in an unauthorized use of personal information by the threat actor contrary to section 31 of *MFIPPA* and, therefore, was a privacy breach.

3. I am not satisfied that the police responded adequately to the breach because they have not reviewed their policies and practices in protecting personal information post-breach.

---

[19] See footnote 15.
[20] See footnote 15.

4. I am not satisfied that the police have reasonable measures in place to safeguard the affected records as required by section 3(1) of Regulation 823 under *MFIPPA* because the police did not provide the IPC with their relevant training materials.

RECOMMENDATIONS:

1. In response to the breach, the police should review their policies and practices in protecting personal information to determine whether changes are needed in light of this breach and my findings in this decision.

2. The police should review and ensure that their training materials constitute reasonable measures in place to prevent unauthorized access to records of personal information in accordance with section 3(1) of Regulation 823, taking into account the nature of the records to be protected.

Within three months of receiving this report, the police should provide this office with proof of compliance with the above recommendations.

Original Signed by: December 10, 2024

John Gayle
Investigator