JANUARY 2022

Summary of Resolution for MR21–00033 – the Regional Municipality of Durham

The Regional Municipality of Durham (the "Region") reported that, on or around January 20, 2021, an unauthorized party gained access to the Region's data within a third party file sharing application used by the Region, Accellion FTA.

As the Region determined that personal information and personal health information was disclosed in this case, the organization reported the privacy breach to the Office of the Information and Privacy Commissioner of Ontario ("IPC" or "our office").

THE ROLE OF THE IPC:

The IPC is the oversight body for Ontario's **privacy laws**, which sets out rules for how Ontario's public institutions and health care providers collect, use, disclose, safeguard and dispose of personal information and personal health information.

When a privacy breach is reported to the IPC, our office will assess the breach to ensure that the reporting organization has taken reasonable steps to contain the incident, notify affected individuals, and prevent a future occurrence. We will also assess whether, at the time of the breach, the organization had reasonable administrative, technical and physical safeguards to ensure the security and confidentiality of personal information and personal health information under its control.

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

SCOPE AND BACKGROUND OF THE BREACH:

The reported cyberattack on the Region was part of a widespread effort by cyber actors to exploit vulnerabilities in Accellion FTA in late 2020 and early 2021.[1] Vulnerabilities in Accellion FTA were exploited in order to attack government bodies and private sector industries across the globe. This activity affected many organizations and individuals worldwide.

Based on the Region's investigation, it reported that, on or around January 20, 2021, an unauthorized party was able to gain access to its data by exploiting a previously unknown vulnerability in Accellion FTA. The unauthorized party then exfiltrated personal information and personal health information from documents that had been transferred to or from the Region using Accellion FTA.

The Region advised that it became aware of the cyberattack on March 25, 2021, when it received a ransom note relating to this matter. The Region confirmed that it took immediate steps to secure its systems and conduct an investigation.

The Region reported that approximately 105,945 individuals had personal information or personal health information affected or potentially affected by the reported breach. According to the Region, a wide range of information was potentially affected by the reported breach, including: names, dates of birth, contact information, genders, parents/guardians, workplaces, employment histories, connections to employee assistance programs, Ontario Education Numbers, schools, grade levels, class information, school systems, citizenships, religions, financial information, property roll numbers, occupancy/tenants for property, rental amounts, vehicle information, government issued identification, participation in a partner assault response program, court orders, safety comments, names of probation officers, member identification numbers and/or benefits with Ontario Works/ODSP, referrals, immunization records, health card numbers, vaccine eligibility, lab test results, health care treatment received, and information about ambulance calls.

Following this attack, the Region reported that some of the data affected by the breach was posted on the dark web, including personal information and personal health information.

CONTAINMENT:

The Region reported that, upon discovery of the reported breach, its IT teams, working with the third party provider of Accellion FTA, Accellion (now Kiteworks), took immediate steps to secure its systems. The Region also confirmed that it notified law enforcement about the cyberattack.

[1] See Joint Cybersecurity Advisory, **Exploitation of Accellion File Transfer Appliance - AA21-055A**, issue on February 24, 2021. This joint advisory was the result of a collaborative effort by the cybersecurity authorities of Australia, New Zealand, Singapore, the United Kingdom, and the United States.

NOTIFICATION:

In order to provide notice of the reported breach, the Region confirmed that it published information about the breach on its website and sent direct written notices to almost all individuals whose personal information or personal health information was potentially affected by the cybersecurity incident.[2] It also set up a dedicated call centre to answer questions about this matter and offered complimentary credit monitoring services for individuals who may have had financial information affected by the breach.

SAFEGUARDS AND REMEDIATION:

The Region confirmed that it was responsible for the user management and patch management of Accellion FTA. It also advised that, except in limited circumstances when the Region required technical support, Accellion did not have access to the Region's data.

At the time of the reported breach, the Region appears to have had a number of reasonable measures in place to protect itself from a cyber breach of this nature, that is, an attack on the Region's personal information and personal health information holdings through a file transfer application.

For example, in order to protect the organization from a cyberattack and ensure the security of its data, the Region confirmed that, at the time of the reported breach, it had a mechanism in place for the organization to stay informed of updates for Accellion FTA. Equally important, the Region confirmed that it had a patch management procedure set up to ensure products (including Accellion FTA) were patched regularly and as patches or security updates became available. At the time of the reported breach, the Region confirmed that, if needed, it had a specific procedure in place for patching critical vulnerabilities in an expedited manner. Indeed, the Region advised that it relied on this critical vulnerabilities procedure to update Accellion FTA on multiple occasions in early 2021. In order to minimize the potential impact of an attack involving Accellion FTA, the Region also confirmed that it had a retention policy in effect for information uploaded to the application.

In addition, the Region advised that it has taken the following proactive steps to protect the organization from cyberattacks:

- employees receive ransomware and cybersecurity training (including simulated phishing attacks);
- antivirus software performs real-time scans at both end-user devices and servers;

[2] Five individuals potentially affected by the breach were deceased and the Region did not have information about their estate representatives. The Region added written instructions to its files to provide notice to estate representatives, should they contact the organization about the deceased parties in the future. The Region made a similar note for three potentially affected individuals for whom the Region did not have contact information.

- user accounts are given privileges and granted access rights only for that which is necessary for that user's work duties; and,
- electronic records are regularly backed up and tested to ensure that they can be restored.

Because the attack involved the exploitation of a vulnerability that was previously unknown (a zero-day attack), the measures taken by the Region to protect itself from a cyberattack could not have been effective at preventing the reported breach in this case. The Region explained it was notified by Accellion of the relevant vulnerability in Accellion FTA on January 22, 2021, two days after the cyberattack had occurred. Upon learning of this vulnerability on January 22, 2021, the Region advised that it shut down Accellion FTA the same day, until January 25, 2021, when a patch was available and successfully applied to the application. However, the Region's mechanism to receive updates for Accellion FTA and its patch management procedure were unable to protect the organization from the cyberattack that had already occurred in this case unbeknownst to the Region.

In response to the reported breach, the Region agreed to implement logging requirements for monitoring/detecting security events (such as data exfiltration) with respect to all file-sharing applications in use. Going forward, this measure can help the Region to detect, understand and recover from cybersecurity incidents in a more informed and timely manner. The Region also advised that it has stopped using Accellion FTA.

CONCLUSION:

The personal information and personal health information potentially affected by this reported breach was highly sensitive.

Overall, at the time of the reported breach, the Region appears to have had a number of reasonable safeguards in place to protect itself from a cyberattack of this nature. In response to the reported breach, the Region agreed to take further reasonable measures to help the organization detect and manage future cybersecurity incidents.

After considering the circumstances of the reported breach and the steps taken by the Region in response to this matter, the analyst was satisfied that no further review is required.

POSTSCRIPT:

The IPC works hard to resolve breaches that are reported to our office and has a very high success rate. This is due to the cooperation of organizations with our process and their willingness to consider our office's recommendations.

In this day and age, cyberattacks have become more and more common. While not all cyberattacks are preventable, this case should serve as stark reminder of the importance of not only responding well to cyberattacks, but also of ensuring that strong and current defenses are in place to identify and mitigate the risk of an attack from occurring in the first place. This includes carrying out robust due diligence when selecting software and other technology for use.

At the time of the breach, Accellion FTA was legacy software that was still supported by the vendor. Following the reported breach, the Region advised that it has transferred users to alternative file sharing applications. While migrating from legacy systems to new systems is a challenge for all organizations, it is important to keep up with the curve of technology in order to take advantage of the latest security protection measures.

For more information, see the IPC's:

- **Your Privacy & Ontario's Information and Privacy Commissioner**
- **Your Health Information and Your Privacy**
- **Identity Theft - A Crime of Opportunity**
- **Filing a Privacy Complaint**
- **Filing a Health Privacy Complaint**
- **Protecting Against Ransomware**
- **Protect Against Phishing**
- **Working From Home During The Covid-19 Pandemic**
- **Planning For Success: Privacy Impact Assessment Guide**
- **Communicating Personal Health Information By Email**
- **Privacy And Security Considerations For Virtual Health Care Visits**
- **Fact Sheet: The Secure Transfer Of Personal Health Information**

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