Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Investigation into MGM (MGM Resorts International) breach highlights how to assess risk, and need for timely assessment

PIPEDA (Personal Information Protection and Electronic Documents Act) Findings #2022-004

19 May 2022

Complaint under the *Personal Information Protection and Electronic Documents Act* (the "Act")

Report of findings

Overview

In February 2020, the Office of the Privacy Commissioner of Canada (the "OPC") became aware of media reports regarding a large-scale data breach MGM (MGM Resorts International) suffered in 2019. Not having received a breach report on the matter, the OPC (Office of the Privacy Commissioner of Canada) engaged with MGM (MGM Resorts International) to obtain additional information about the breach and the involvement of any personal information belonging to Canadians.

After receiving confirmation that Canadian personal information was affected by the breach, considering the potential impact on Canadians who were affected but had not yet been notified of the breach, and considering the significant passage of time since MGM (MGM Resorts International)'s confirmation of the breach, the Commissioner initiated a complaint to investigate [1](#fn1) whether MGM (MGM Resorts International) had complied with its mandatory breach reporting obligations under PIPEDA (Personal Information Protection and Electronic Documents Act). [2](#fn2)

Our investigation found that MGM (MGM Resorts International) contravened the mandatory breach reporting provisions of PIPEDA (Personal Information Protection and Electronic Documents Act). While MGM (MGM Resorts International) determined that there was a breach of its security safeguards in the summer of 2019, MGM (MGM Resorts International) failed to promptly assess whether the breach posed a real risk of significant harm ("RROSH") to affected Canadians. We found that the breach posed a RROSH (real risk of significant harm) and that MGM (MGM Resorts International) did not report the breach to the Privacy Commissioner or notify affected individuals as soon as feasible.

In response to recommendations by our Office, MGM (MGM Resorts International) agreed that it would make amendments to its privacy breach response framework or process by 30 June 2022, to ensure that where MGM (MGM Resorts International) learns of a breach that may involve personal information of Canadian residents: (a) MGM (MGM Resorts International) will promptly conduct a RROSH (real risk of significant harm) assessment, consistent with the OPC (Office of the Privacy Commissioner of Canada)'s published guidance; and if MGM (MGM Resorts International) determines that such a breach gives rise to a RROSH (real risk of significant harm), MGM (MGM Resorts International) will, as soon as feasible (b) provide a report to the Privacy Commissioner, and (c) notify affected individuals.

We therefore find the matter to be **well-founded and conditionally resolved**.

Background and Complaint

1. MGM Resorts International ("MGM") is a U.S. (United States)-based entity that owns and operates a number of hotels and casinos located in the United States. MGM (MGM Resorts International) frequently interacts with its Canadian customer base through its marketing activities, online reservations, and partnerships with Canadian organizations such as Air Canada Vacations, Cirque du Soleil, and Canadian Automobile Association.
2. In February 2020, the Office of the Privacy Commissioner of Canada (the "OPC") became aware of media reports [3](#fn3) regarding the publication of personal information of about 10.6 million MGM (MGM Resorts International) guests on a "hacking" forum. Per these reports, the information appeared to include names, contact details, dates of birth and for about 1,300 individuals, certain identification numbers (driver's licenses, passports or military ID cards). In these media reports, MGM (MGM Resorts International) also confirmed that a breach occurred during the summer of 2019 and that it had contacted all impacted hotel guests in accordance with state laws.
3. As the OPC (Office of the Privacy Commissioner of Canada) had not received a breach report from MGM (MGM Resorts International) at that time, the OPC (Office of the Privacy Commissioner of Canada) contacted MGM (MGM Resorts International) in February 2020 to obtain additional information about the breach and the involvement of any personal information belonging to Canadians.
4. MGM (MGM Resorts International) explained that, based on its investigation of the breach, it determined that on approximately 7 July 2019, an unauthorized third party gained access to an external cloud server containing certain MGM (MGM Resorts International) guest data. The unauthorized actor was able to gain access by logging into a third-party platform used by MGM (MGM Resorts International) software developers, using an MGM (MGM Resorts International) employee's credentials (which had been compromised in a previous data breach, not associated with MGM (MGM Resorts International) – a credential stuffing attack) and exploiting a coding flaw (on that third-party platform) to bypass multi-factor authentication. Subsequently, the unauthorized actor identified a temporary access token that they used to access MGM (MGM Resorts International) guest data on an external cloud server. The token allowed the attacker to gain access to the database for approximately one hour. During that time, the attacker ex-filtrated a data set containing certain MGM (MGM Resorts International) guest data. The attacker then offered it for sale online. MGM (MGM Resorts International) claimed that in the online sale offer, the attacker said that the data set had little value due to its poor condition. MGM (MGM Resorts International) did not offer any corroborative evidence to substantiate this.
5. MGM (MGM Resorts International) further explained that it became aware of the online sale posting on or about 10 July 2019, and at that time, MGM (MGM Resorts International) engaged a "leading third-party data security expert" and an "e-discovery expert", to conduct a forensic investigation and assist in MGM (MGM Resorts International)'s efforts to understand and assess the incident and the affected data. With the assistance of these third-party experts, MGM (MGM Resorts International) took steps to ensure that the unauthorized party no longer had access to the MGM (MGM Resorts International) guest data on its external cloud server. After consulting with U.S. (United States) law enforcement, MGM (MGM Resorts International) also purchased a copy of the data set from the attacker on 24 July 2019, in return for the vendor's agreement to remove the posting. [4](#fn4) MGM (MGM Resorts International) claimed, based on work with its third-party consultants, that the impacted data set was in poor condition and not readily useable.
6. After the OPC (Office of the Privacy Commissioner of Canada) contacted MGM (MGM Resorts International) in February 2020, MGM (MGM Resorts International) commenced further analysis and later confirmed that

1,934,090 Canadians were affected; including 5,635 Canadians whose government identifier (e.g., passport number, Nexus number, health card number, military identification number) was compromised. At this time, in late April 2020, MGM (MGM Resorts International) advised that it would be notifying affected Canadians imminently.

7. Additionally, in its breach report to the OPC (Office of the Privacy Commissioner of Canada) on 3 June 2020, MGM (MGM Resorts International) explained what remedial measures had been implemented to protect against a similar breach occurring in future and against potential harm to affected individuals. These measures included, but were not limited to, the third-party platform's remediation of the coding flaw, access control enhancements by MGM (MGM Resorts International) (e.g., expanding MGM (MGM Resorts International)'s use of multi-factor authentication, prohibiting MGM (MGM Resorts International) software developers from using personal email addresses for MGM (MGM Resorts International)-related work, and ensuring accounts are provisioned on the principle of least privilege) and offering credit monitoring to affected individuals.
8. Given the potential impact on Canadians whose government identifiers were affected (but had not yet been notified of the breach), and considering the significant passage of time between MGM (MGM Resorts International)'s confirmation of the breach and MGM (MGM Resorts International)'s assessment of the breach with respect to Canadians, the Commissioner initiated a complaint to investigate [5](#fn5) whether MGM (MGM Resorts International) had adequately complied with its mandatory breach reporting obligations under PIPEDA (Personal Information Protection and Electronic Documents Act). [6](#fn6) Our investigation focused on the impact on Canadians.
9. We note that MGM (MGM Resorts International) submitted a breach report to the OPC (Office of the Privacy Commissioner of Canada), and commenced notifying affected Canadians, on 3 June 2020. MGM (MGM Resorts International) completed notifying affected Canadians on 17 July 2020.

Analysis

Issue: Whether MGM (MGM Resorts International) had the obligation to report the breach to the OPC (Office of the Privacy Commissioner of Canada) and notify affected Canadians and if so, whether it did so as soon as feasible

10. To ensure that the Privacy Commissioner of Canada and all affected individuals are aware of, and receive consistent information about, data breaches that pose a real risk of significant harm, PIPEDA (Personal Information Protection and Electronic Documents Act) provides for mandatory breach reporting, under section 10.1, for organizations that experience a data breach (referred to in PIPEDA (Personal Information Protection and Electronic Documents Act) as a "breach of security safeguards"). [7](#fn7)
11. Where an organization has experienced a breach of its security safeguards, it will need to assess whether that breach creates a real risk of significant harm ("RROSH") to any affected individual. If it is reasonable to believe in the circumstances that the breach poses a RROSH (real risk of significant harm) to an individual, PIPEDA (Personal Information Protection and Electronic Documents Act) requires the organization to report that breach to the Privacy Commissioner. [8](#fn8) Additionally, the organization must notify any affected individual of the breach, unless otherwise prohibited by law, in order to allow these individuals to take steps, if any are possible, to reduce or mitigate the risk of harm that could result from the breach. [9](#fn9) In both cases, the organization must report and notify of the breach as soon as feasible after the organization determines that the breach has occurred. [10](#fn10)
12. Considering the above, our analysis focused on whether the breach sustained by MGM (MGM Resorts International) in 2019 met the RROSH (real risk of significant harm) threshold, and whether MGM (MGM Resorts International) reported the breach to the OPC (Office of the Privacy Commissioner of Canada) and notified affected Canadians as soon as feasible.

Sub-Issue 1: Whether the MGM (MGM Resorts International) breach met the RROSH (real risk of significant harm) reporting and notification threshold

13. Pursuant to subsection 10.1(8) of PIPEDA (Personal Information Protection and Electronic Documents Act), the RROSH (real risk of significant harm) assessment must consider the sensitivity of the personal information involved in the breach, and the probability that the personal information has been, is being, or will be, misused. In our view, as detailed below, the information at issue is sensitive and the probability of its misuse in the circumstances of the breach is sufficiently high, such that the breach meets the RROSH (real risk of significant harm) threshold.

Sensitivity of the personal information

14. The first RROSH (real risk of significant harm) assessment factor is the sensitivity of the personal information involved in the breach. While PIPEDA (Personal Information Protection and Electronic Documents Act) does not define sensitivity, Principle 4.3.4 of PIPEDA (Personal Information Protection and Electronic Documents Act) states that "[a]lthough some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context." In this case, we found the personal information involved in the breach to be sensitive.
15. In response to the OPC (Office of the Privacy Commissioner of Canada)'s request for information about its risk assessment, MGM (MGM Resorts International) submitted that there was no RROSH (real risk of significant harm) to affected Canadian residents, given "the poor and disorganized state of the data, the possibility of the relevant information being expired or invalid, and the non-sensitive nature (with the exception of government-issued ID numbers) of the data in the affected records".
16. First, the government-issued identifiers for 5,635 affected Canadians represent sensitive information, as these can be very useful in the context of fraud and identity theft.
17. As for the remaining personal information involved in the breach, these details (names, dates of birth, phone number, email address, and full/partial residence address) may not be sensitive in isolation. However, in our view, they can hold a higher level of sensitivity when combined with other personal information and/or when the circumstances of a breach increase the potential for the information to be used in a manner that could cause harm to affected individuals.
18. In this case, the sensitivity of the remaining personal information is heightened when attached to a government-issued identifier. Additionally, we note that the information was posted for sale to malicious actors on a hacking forum on the dark web, which could result in misuse of the information for harmful activities such as identity fraud, financial harm, and phishing. [11](#fn11)
19. We therefore consider the Canadian personal information breached to be sensitive.

Probability of misuse

20. The second RROSH (real risk of significant harm) assessment factor is the probability that the personal information has been, is being, or will be, misused. In this case, we are of the view that the probability of misuse further supports a finding that there is RROSH (real risk of significant harm) to affected individuals.
21. According to the OPC (Office of the Privacy Commissioner of Canada)'s guidance, [12](#fn12) it is important to consider factors such as the following when assessing this probability of misuse:
    a. who accessed (or who could have accessed) the information,
    b. how long the personal information was exposed,
    c. whether there is any evidence of malicious intent (e.g. theft, hacking),
    d. whether the risk of misuse is raised due to a number of pieces of personal information being breached,
    e. whether the information was exposed to individuals/entities who are unknown or to a large number of individuals (where certain individuals might use or share the information in a way that would cause harm),
    f. whether harm has materialized for any affected individuals,
    g. whether the personal information has been recovered, and
    h. whether the personal information was easily accessible (e.g. protected by adequate encryption or anonymization).

22. In this case, the unauthorized actor demonstrated malicious intent by hacking into MGM (MGM Resorts International)'s external cloud server, ex-filtrating MGM (MGM Resorts International) guest data, and attempting to profit from that data by posting it for sale in a hacking forum on the dark web. In this process, the data was exposed to an unknown number of other malicious actors whose purpose for purchasing the data would likely be to misuse the information for harmful activities (e.g., through identity fraud or a phishing attack, as noted earlier in this report).
23. We further note a significant number of pieces of personal information were breached, for millions of individuals, increasing the value of that information and the likelihood that it could be misused.
24. With respect to the accessibility of the information breached, MGM (MGM Resorts International) advised that "the state of the data set was such that it would be extremely challenging for someone without knowledge of the source systems and expertise in data reconstruction to make meaningful use of the data set". In its view, knowledge of MGM (MGM Resorts International)'s source systems was required to understand the information breached.
25. However, based on the OPC (Office of the Privacy Commissioner of Canada)'s technical analysis of a sample of the data set provided by MGM (MGM Resorts International), we found that it would be possible for a malicious actor to, without significant time or effort, organize the data into a form that allows identification of the personal information contained therein. In fact, our Office's own technical analysts were able to do so. As such, we found the information to be reasonably accessible.
26. While MGM (MGM Resorts International) advised that it had no evidence to suggest harm had materialized for any of the affected individuals, the data could have been misused in a way that MGM (MGM Resorts International) has not yet detected or could be misused in future. Notably, while MGM (MGM Resorts International) obtained a copy of the data set in July 2019, on the understanding that the online posting would be removed, the data set reappeared for sale on the dark web in February 2020.
27. Given the sensitivity of the information in question, and the potential for it to be misused by malicious actors, we find that this breach created a RROSH (real risk of significant harm) to affected Canadians, such that MGM (MGM Resorts International) was required to report the breach to our Office, and notify affected individuals in Canada.

Sub-Issue 2: Whether MGM (MGM Resorts International) notified the OPC (Office of the Privacy Commissioner of Canada) and affected Canadians as soon as feasible

28. MGM (MGM Resorts International) advised that on 4 August 2019, following reconstruction of the data set, it was able to identify specific information in the affected records. MGM (MGM Resorts International) began notifying certain affected U.S. (United States) guests and privacy regulators on 5 September 2019.
29. However, MGM (MGM Resorts International) did not commence reconstruction and analysis of the affected data set, with respect to data of Canadians, until 28 February 2020. MGM (MGM Resorts International) then reported the breach to our Office on 3 June 2020, and commenced notifying affected Canadians on the same day, almost 11 months after MGM (MGM Resorts International) had become aware of the breach. MGM (MGM Resorts International) confirmed that it completed notifying affected Canadian residents on 17 July 2020. In our view, it would have been feasible for MGM (MGM Resorts International) to act sooner.
30. The OPC (Office of the Privacy Commissioner of Canada) acknowledges that it can often take weeks or months to completely investigate and confirm the scope of a breach. However, this case is not a question of whether MGM (MGM Resorts International) took too long to analyze the data, determine that 1.9 million Canadians were affected and conduct its RROSH (real risk of significant harm) assessment. MGM (MGM Resorts International) did not even start any such assessment until almost six months after it began notifying affected U.S. (United States) guests and privacy regulators; and this was only after the OPC (Office of the Privacy Commissioner of Canada) contacted MGM (MGM Resorts International) about media reports regarding the breach. In our view, MGM (MGM Resorts International) should have commenced analysis of the data vis-à-vis impact on Canadians concurrent with its analysis in relation to its U.S. (United States) guests.
31. If MGM (MGM Resorts International) had commenced its analysis of the data vis-à-vis Canadians immediately, as it did with respect to Americans, it could have conducted its RROSH (real risk of significant harm) analysis

sooner, and been in a position to notify affected Canadians many months earlier than June-July 2020. We therefore find MGM (MGM Resorts International) to have been in contravention of section 10.1 of PIPEDA (Personal Information Protection and Electronic Documents Act) in that MGM (MGM Resorts International) did not report the 2019 breach to the OPC (Office of the Privacy Commissioner of Canada) and did not notify affected Canadian residents as soon as feasible.

Recommendations

32. In response to a recommendation by our Office, and with a view to complying with its obligations under Section 10.1 of PIPEDA (Personal Information Protection and Electronic Documents Act), MGM (MGM Resorts International) committed to, by 30 June 2022, amend its privacy breach response framework to ensure that in circumstances where MGM (MGM Resorts International) learns of a breach that may involve personal information of Canadian residents:
    a. MGM (MGM Resorts International) will promptly conduct an appropriate assessment as to whether such breach gives rise to a RROSH (real risk of significant harm), consistent with applicable published guidance of the OPC (Office of the Privacy Commissioner of Canada); [13](#fn13) and
    b. if MGM (MGM Resorts International) determines that such breach gives rise to a RROSH (real risk of significant harm), MGM (MGM Resorts International) will, in accordance with s. 10.1 of PIPEDA (Personal Information Protection and Electronic Documents Act):
        i. provide a report, as soon as feasible, to the Privacy Commissioner of Canada; and,
        ii. notify, as soon as feasible, the relevant individuals affected by such breach.
33. We also recommended, and MGM (MGM Resorts International) agreed, to provide, by 30 June 2022 a report and associated documentary evidence to our Office to establish that it has complied with its commitment to amend its privacy breach response framework.

Conclusion

34. Given that MGM (MGM Resorts International) has now reported the breach and notified affected Canadians, and considering MGM (MGM Resorts International)'s commitments as detailed above, we consider this matter to be **well-founded and conditionally resolved** (/en/opc-actions-and-decisions/investigations/def-cf/).

Footnotes

1 Under subsection 11(2) of PIPEDA (Personal Information Protection and Electronic Documents Act), the Commissioner may initiate a complaint if he is satisfied that there are reasonable grounds to investigate a matter under Part 1 of PIPEDA (Personal Information Protection and Electronic Documents Act).

2 PIPEDA (Personal Information Protection and Electronic Documents Act) s (section) 10.1

3 ZDNet, *Exclusive: Details of 10.6 million MGM (MGM Resorts International) hotel guests posted on a hacking forum*, February 19, 2020; The New York Times, *MGM Resorts Says Data Breach Exposed Some Guests' Personal Information*, February 19, 2020

4 As discussed later in the report, the posting was removed from the hacker forum but later reappeared for sale on the dark web.

5 Under subsection 11(2) of PIPEDA (Personal Information Protection and Electronic Documents Act), the Commissioner may initiate a complaint if he is satisfied that there are reasonable grounds to investigate a matter under Part 1 of PIPEDA (Personal Information Protection and Electronic Documents Act).

6 PIPEDA (Personal Information Protection and Electronic Documents Act) s (section) 10.1.

7 *Breach of Security Safeguards Regulations*: SOR/2018-64.

8 PIPEDA (Personal Information Protection and Electronic Documents Act) s (section) 10.1(1).

9 PIPEDA (Personal Information Protection and Electronic Documents Act) s (section) 10.1(3).

10 PIPEDA (Personal Information Protection and Electronic Documents Act) s (section) 10.1(2) and s (section) 10.1(6).

11 An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts. See the Canadian Centre for Cyber Security's glossary

12 OPC (Office of the Privacy Commissioner of Canada), *What you need to know about mandatory reporting of breaches of security safeguards* (October 2018)

13 Examples of OPC (Office of the Privacy Commissioner of Canada)'s published guidance: OPC (Office of the Privacy Commissioner of Canada), *What you need to know about mandatory reporting of breaches of security safeguards* (October 2018); and OPC (Office of the Privacy Commissioner of Canada), *2019 Breach record inspections* (September 2020)

Date modified:

2022-09-29