Bulletin | Cybersecurity, Privacy and Data Protection

November 2022

Privacy Commissioner decision provides guidance for parties to M&A transactions

The Privacy Commissioner of Canada's decision regarding the Starwood/Marriott data security breach provides important guidance for parties to M&A transactions and for all organizations that handle personal information.

The M&A transaction and the data breach

Marriott International ("Marriott") acquired Starwood Hotels ("Starwood") through a share purchase transaction in September 2016. Marriott assessed Starwood's IT practices as part of the transaction due diligence. After the transaction, the Starwood and Marriott computer networks were kept separate, and Marriott implemented measures to improve the security of the Starwood network until it could be decommissioned. Marriott planned to integrate aspects of the networks within 18 months, but the integration was not completed until December 2018.

In September 2018, Marriott discovered a breach of the Starwood network involving unauthorized access to a Starwood guest reservation database of up to approximately 339 million customer records (including up to 12.8 million records of Canadian individuals) that included guest profiles and contact details, account and reservation information, and for some individuals passport details (which in some cases was unencrypted) and encrypted payment card details. The breach occurred over four years – from July 2014 until September 2018. The unknown attacker took steps to prepare to exfiltrate data from the Starwood network, but Marriott was unable to determine whether the attacker had successfully done so.

In November 2018, Marriott publicly announced the breach and reported the breach to the Office of the Privacy Commissioner of Canada ("OPC"). Marriott contained and investigated the breach, gave affected individuals direct and indirect notice of the breach, decommissioned the Starwood database, and enhanced the security safeguards of its systems based on lessons learned from the breach. Class action lawsuits relating to the breach were commenced against Marriott in Canada and the United States, and the United Kingdom Information Commissioner's Office investigated the breach.

The OPC investigation

The OPC investigated Marriott's personal information practices relevant to the breach. The OPC's decision, published in September 2022, details the OPC's findings that Marriott contravened the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") regarding personal information in the compromised Starwood database. The OPC's findings are generally consistent with an October 2020 Penalty Notice issued by the United Kingdom Information Commissioner's Office, which imposed an £18.4 million penalty on Marriott for violations of the European Union *General Data Protection Regulation*. Following is a summary of the OPC's key findings and guidance.

Responsibility

Marriott's acquisition of Starwood gave Marriott control over and responsibility for the Starwood network. Consequently, Marriott became accountable for implementing policies and practices for protecting personal information in the Starwood network. The OPC explained:

> "When acquiring new systems and databases that handle personal information, the acquiring organizations should take action to identify whether there are any security requirements for their acquisitions. This should be performed, where practicable, before the organization receives control of the information system or database, and certainly before using and integrating the data into existing systems. These actions should include various forms of testing, such as a network testing and an audit against recognized industry standards, a security assessment, or a threat risk analysis. The performance of such testing is important because if done properly, it can ensure the early identification of compromised assets and the measures that an organization needs to take (e.g. system improvements, updates, the implementation of new safeguards or processes, or malware removal) to resolve any areas of compromise or ensure newly acquired systems are adequately protected."

Security safeguards

The Starwood network had various levels of security, including measures implemented by Marriott after the acquisition transaction, some of which were validated by regular independent testing as part of Starwood's compliance with the Payment Card Industry Data Security Standard and supported by qualified independent service providers. Nevertheless, the OPC found that the security safeguards were not sufficient, given the sensitive information in the Starwood database (including customer account information and passport numbers) and the possibility that the information could be used to harm individuals through phishing, fraud and identity theft, particularly regarding: (1) access controls; (2) anti-virus software; (3) logging and monitoring; and (4) information storage. The OPC found that Marriott could have detected the breach sooner and minimized the attacker's activities if Marriott had more comprehensive logging and monitoring measures in place and adequately applied multi-factor authentication access controls. The OPC also found that Marriott could have reduced the scale or impact of the breach if all sensitive personal information in the Starwood network had been encrypted and timely deleted.

Accountability

Marriott assessed Starwood's data security practices as part of the acquisition transaction due diligence, and after the transaction implemented measures to improve the security of the Starwood network until it could be decommissioned. Nevertheless, the OPC found that Marriott failed to perform ongoing assessment and revision of the security safeguards for the Starwood database in breach of the PIPEDA requirement to implement appropriate policies and practices to protect personal information under Marriott's control. The OPC explained:

> "In order to properly protect privacy and meet legal obligations, organizations must monitor, assess and revise their privacy framework periodically to ensure it remains relevant and effective. This practice extends to security safeguards, including testing and monitoring activities. Evaluating security safeguards periodically is critical. It is not sufficient for an organization to have the right tools in place – the tools must be implemented properly, their warnings must be heeded, and they should be under continuous assessment with regular reviews and updates (e.g. for corrections and/or maintenance)."

The OPC found that Marriott could have detected the breach sooner and minimized the attacker's activities if Marriott had adequate measures in place to ensure the ongoing assessment and revision of the security safeguards.

Information retention

The Starwood database included personal information retained longer than required by Starwood's data retention policy or for compliance with legal requirements. Consequently, the OPC found that Marriott retained the personal information in contravention of the PIPEDA requirement that organizations retain personal information only as long as necessary for the purposes for which it was collected, except with the consent of relevant individuals or as required by law. In addition, the OPC found that Marriott could have reduced the scale or impact of the breach if information in the Starwood network had been timely deleted.

Mitigation measures

Marriott offered affected Canadians one year of free web monitoring through a commercial service that monitors internet sites where personal information is unlawfully shared and generates an alert to an individual if evidence of their personal information is found. Marriott did not offer credit-monitoring services, which can mitigate the risk of harm from fraudulent activities involving identity theft or phishing attacks. The OPC expressed concern that the web monitoring offered by Marriott was only effective for one year because the OPC "would typically expect an organization to offer protections (such as web monitoring or credit monitoring) for an extended period" in case a malicious actor waits until after the monitoring period to misuse personal information. Nevertheless, the OPC found that in the circumstances, including no substantiated claim of financial loss or evidence of phishing or other information misuse arising from the breach, Marriott's additional mitigation measures were "minimally sufficient".

Remediation/lessons learned

Marriott enhanced the security safeguards of its systems based on lessons learned from the breach, and agreed to an independent assessment of its security practices and ongoing assessments and regular reviews of its privacy framework, information security program, information security controls, incident response capabilities, and due diligence process for acquired assets. The OPC explained that those actions "will provide further assurances that Marriott has taken measures to ensure the protection of its customer's personal information in compliance with" PIPEDA.

Comments/recommendations

Data security risks are an important consideration regarding almost all M&A transactions. Data security risks can affect the viability and value of an M&A transaction, influence the nature and terms of a transaction, and in some circumstances cause the parties to abandon a transaction. In addition, parties to an M&A transaction and their directors and officers (if applicable) might be legally obligated to address data security risks in connection with the transaction or incur potentially significant liabilities if they fail to do so. See BLG bulletins *Managing cyber risks in M&A transactions* and *Cyber risk management guidance for Canadian corporate directors*.

As explained by the OPC, the Starwood/Marriott data security breach "highlights the importance of accountability and security safeguard measures that organizations should apply, particularly with respect to information systems and databases that they are acquiring or taking control over. In particular, it is vital that organizations perform various forms of testing when acquiring new systems, to ensure that they can identify and (where needed) enhance security safeguards".

Following are some key takeaways from the OPC's decision:

- An M&A transaction can result in the purchaser acquiring control over and responsibility for personal information held by the seller. In those circumstances, the purchaser must comply with personal information protection laws regarding the handling of the personal information.
- If an M&A transaction involves the purchaser's acquisition of systems and databases that handle personal information, the purchaser should conduct a thorough and timely data security assessment and implement appropriate security measures for the personal information.
- The measures used to protect the security of personal information should be appropriate for the volume and sensitivity of the personal information. Information that is less sensitive in isolation can be more sensitive if combined with other information.
- Compliance with information security obligations is not a one-time event. Organizations must periodically evaluate and revise their information security practices.

- Organizations should delete or anonymize personal information in a timely manner for compliance with personal information protection laws and as a security measure to reduce the potential scope or effect of a data breach.
- The required mitigation measures for individuals affected by a personal information breach will depend on the circumstances, including whether there is evidence of financial loss or information misuse.
- Organizations should learn lessons from each data security incident and make appropriate changes to their information security practices. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.