Blogs
November 07, 2024
FTC and State Coalition Settle Data Breach Cases with Marriott

The Federal Trade Commission (FTC) announced a complaint and proposed consent order against Marriott International Inc. and its subsidiary, Starwood Hotels & Resorts Worldwide LLC, on October 9, 2024, concerning three alleged data breaches that occurred between 2014 and 2020. In a concurrent settlement regarding the same incidents, a coalition of 49 states (all except California) and the District of Columbia obtained relief that includes a $52 million payment from Marriott.

The Marriott and Starwood Security Incidents

In 2018, Marriott announced a data breach affecting its Starwood reservation system, thought at the time to have affected up to 500 million people worldwide. These settlements arise from that incident, as well as two smaller incidents that also affected Starwood and Marriott. The FTC alleges these incidents exposed payment card information, unencrypted passport numbers, and loyalty account information, along with other information like names, dates of birth, and contact information.

First Breach: June 2014 – Starwood. The first breach allegedly affected Starwood's network over a 14-month period beginning in June 2014. The complaint alleges that a malicious actor exploited vulnerabilities to gain remote access to Starwood's network, installed malware into computer systems at more than 100 hotel properties, and leveraged this malware to access payment card information of 40,000 consumers. According to the FTC, a forensic examination determined that inadequate firewalls and network segmentation, inadequate access controls, use of outdated and unsupported software, and lack of multifactor authentication (MFA) contributed to the breach. Although this incident occurred before Marriott acquired Starwood, the complaint alleges that while closing the acquisition between November 2015 and September 2016, Marriott "reviewed and evaluated Starwood's information security program to understand the state of Starwood's computer networks, systems, and their vulnerabilities, including the information security failures that led to the [breach]." Compl. ¶ 10.

Second Breach: July 2014 – Starwood. The second breach also affected Starwood's systems and originated before Marriott acquired Starwood, then continued after the acquisition. According to the complaint, forensic examiners determined that in July 2014, malicious actors compromised Starwood's external-facing webserver, installed malware on its network, and over the next four years compromised the personal information of 339 million consumer records, including more than 5.25 million unencrypted passport numbers along with payment card numbers, loyalty program numbers, and other personal information. According to the FTC, forensic examiners attributed the breach to similar causes as the first breach, including inadequate firewall controls, unencrypted payment card information stored outside of the secure cardholder data environment, lack of MFA, and inadequate monitoring and logging practices.

Third Breach: September 2018 – Marriott. The complaint alleges that the third breach affected Marriott's own systems, originating when malicious actors compromised credentials of employees at a Marriott franchise property. From there, over periods in 2018 and 2020, the malicious actors allegedly gained access to Marriott's network and accessed more than 5.2 million guest records, including many types of basic personal information along with loyalty account information, with the apparent goal of identifying accounts with loyalty points that could be used or redeemed.

The FTC's Claims and Proposed Order

In the complaint, the FTC alleges that Marriott and Starwood engaged in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). The complaint asserts two counts:

- **Deceptive Security Statements:** The FTC alleges that Marriott and Starwood deceived consumers by representing in the privacy policies on their respective websites that they used appropriate data security safeguards. Specifically, Marriott said it used "reasonable organizational, technical and administrative measures to protect Personal Data" and Starwood said it would "safeguard your information using appropriate administrative, procedural and technical safeguards," including password controls and firewalls.
- **Unfair Information Security Practices:** The FTC alleges that the security practices of Marriott and Starwood were unfair because they failed to implement reasonable security measures to protect consumers' information, including failures to:
    - Implement appropriate password controls, resulting in employees using default, blank, or weak passwords;
    - Timely patch outdated software and systems, including because Starwood's cardholder environment used operating systems so outdated that they were no longer supported and patches were not available;
    - Adequately monitor and log network environments, which limited the companies' ability to timely detect malicious actors;
    - Employ appropriate access controls, for example by failing to terminate the accounts of former employees;
    - Implement appropriate firewall controls;
    - Establish appropriate network segmentation between hotel property and corporate systems; and
    - Utilize MFA to safeguard sensitive information.

The FTC alleged that these deficiencies caused or were likely to cause substantial injury to consumers. For example, the complaint alleged the third breach "enabled malicious actors to fraudulently make purchases by redeeming loyalty points," that identity thieves were likely to take over loyalty accounts for future use, and that loyalty accounts are more susceptible to fraud than payment cards due to their value, static account numbers, and relative lack of monitoring by consumers. Compl. ¶ 29. Additionally, the FTC alleged the second breach

enabled malicious actors to create sophisticated phishing schemes by combining the exposed unencrypted passport numbers with other personal information in the affected records. Compl. ¶ 30.

Requirements in the FTC Proposed Consent Order

The proposed consent order includes a few new and noteworthy requirements for an FTC data security settlement:

- **Loyalty Rewards Program Account Review:** Marriott and Starwood must develop a method for consumers to request a review of their account for unauthorized account activity. If it is determined that a security incident resulted in the loss of rewards points, the companies must restore the points.
- **Data Deletion/Minimization:** Marriott and Starwood must post a clear and conspicuous link on their websites where consumers can request deletion of their personal information. The companies must further maintain a policy to retain personal information only as long as is reasonably necessary for the companies to fulfill the purpose for which the information was collected, a requirement similar to the one found in the consent order recently entered against Blackbaud.

The proposed consent order also includes longstanding standard provisions of FTC data security consent orders, including (1) a prohibition on misrepresentations relating to how Marriott and Starwood collect, maintain, use, delete, or disclose data and the extent to which they protect personal information; (2) a requirement that the companies report additional breaches to the FTC; and (3) a mandatory information security program subject to third-party independent biennial assessments. Continuing a trend of increased specificity in mandatory information security programs, the required program in the consent order includes as a component several required controls, including as related to training, a documented incident response plan, logging and monitoring, data access controls, multi-factor authentication or its equivalent, configuration standards, encryption, scanning for personal information, vulnerability and patch management processes, and timely investigation and remediation of security events.

Multistate Settlement Agreement

The multistate agreement resolves allegations that Marriott's data security practices violated state consumer protection laws, personal information protection laws, and, in some cases, breach notification laws, all relating to the breach of Starwood's guest reservation network between 2014 and 2018. In addition to the $52 million payment, Marriott has agreed to implement a comprehensive information security program that includes an annual risk assessment along with biennial independent third-party assessments. The multistate agreement also contains data minimization and deletion requirements, and a similar loyalty rewards program account review as in the FTC order.

Takeaways

- The FTC appears to be continuing its trend of including more substantive requirements and prohibitions in addition to the process-based obligations (primarily information security programs and regular assessments) that have long been included in data security orders. Most notably, the settlement in this case obligates Marriott and Starwood to provide consumers deletion rights and prominently link to the deletion request process from their websites and apps, a requirement now common in state privacy laws but novel for an FTC order.
- The settlement is also a cautionary tale about possible liability to a parent entity for a subsidiary's conduct and liability that can arise from failures that occurred in whole or in part prior to acquisition. The Starwood breaches began—and the first breach ended—before Marriott acquired Starwood. In alleging that Marriott is liable for Starwood's data security practices, even those that occurred before the acquisition, the FTC cites the fact that Marriott reviewed and evaluated Starwood's information security

program as part of the acquisition process and failed to detect the second, ongoing breach after the acquisition. While the complaint also concerns Marriott's own, unrelated breach, none of the alleged security failures are directly linked to that last incident and it is unclear whether it would have drawn scrutiny absent the two earlier incidents. Thus, the FTC's allegation of Marriott's liability for the first breach in particular appears particularly aggressive and may suggest that the agency will scrutinize privacy and data security incidents that occur both before and after an acquisition if the same or similar offending conduct persists post-acquisition.
- One potential explanation for highlighting the third breach, however, is the involvement of loyalty reward accounts. Although the FTC does not highlight any specific examples reflecting actual misuse of loyalty rewards following the third breach, the novel provisions in the order discussed above and extensive description of potential harms in the complaint indicate the issue is on the FTC's radar and of particular concern.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response