CYBERSECURITY AND DATA PRIVACY

INFORMATION MEMO

OCTOBER 10, 2024

Marriott's Wake Up Call: FTC Fines Hotel Company $52 Million for Delinquent Cybersecurity Practices

In a settlement with Marriott International and its subsidiary Starwood hotels and Resorts Worldwide, the FTC will require Marriott to implement a new comprehensive data security program. The settlement stems from a series of data breaches spanning from 2014 – 2020 in which the FTC alleges bad actors accessed over 339 million consumer records, including names, unencrypted passport numbers and payment card information. In a separate settlement with attorney's general from 49 states and the District of Columbia, Marriott resolved to pay a $52 million fine related to the breaches.

The First Breach

In November 2015, Marriott announced that it would acquire Starwood for $12.2 billion. Four days after the announcement, Starwood notified customers that it had experienced a 14-month long data breach of its computer network, in which malicious actors gained access to payment card information for over 40,000 consumers.

The Second Breach

According to the FTC, Marriott failed to identify an ongoing breach within the Starwood network that continued undetected for nearly two years after the acquisition. Due to this second breach, malicious actors obtained the personal information of 339 million consumer records globally, including more than 5.25 million unencrypted passport numbers.

The Third Breach

Marriott announced in March 2020 that malicious actors had compromised the credentials of employees at a Marriott-franchised property to gain access to Marriott's own network. These intruders accessed more than 5.2 million guest records, including 1.8 million records related to U.S. consumers, that contained significant amounts of personal information.

Delinquent Data Security Practices

According to the FTC, Marriott failed to provide reasonable or appropriate security for the personal information that it collected and maintained. These lax security practices included: a failure to implement appropriate password controls; failure to patch outdated software; failure to adequately monitor network environments; failure to implement access controls; failure to implement appropriate firewall controls; and failure to apply appropriate multifactor authentication to protect sensitive information.

Notably, the FTC alleged that Starwood failed to comply with contractual obligations and internal policies requiring multifactor authentication.

Mandated Modifications of Marriott's Information Security Program

As part of the settlement, the FTC is requiring Marriott to overhaul its information security program. In addition to implementing a new comprehensive data security system, Marriott is required to have a third party assess its security system every two years for the next 20 years. Marriott will also have to provide a conspicuous link on its website and mobile apps that permits customers to request that Marriott delete their personal information.

Bond attorneys regularly assist and advise clients on drafting data privacy and cybersecurity policies. For more information regarding data privacy matters, please contact Jessica Copeland, CIPP/US, Jackson Somes or any attorney in Bond's cybersecurity and data privacy practice.