epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

November 12, 2024

Chair Lina M. Khan
Commissioner Rebecca Kelly Slaughter
Commissioner Alvaro Bedoya
Commissioner Andrew Ferguson
Commissioner Melissa Holyoak
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: *Marriott International Inc., et al.*, FTC File No. 192-3022

Dear Chair Khan and Commissioners Slaughter, Bedoya, Ferguson, and Holyoak,

By notice published October 9, 2024, the Federal Trade Commission (FTC or Commission) announced a proposed consent order with Marriott International Inc, and Starwood Hotels & Resorts, LLC (collectively Marriott), for Marriott's alleged violations of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), prohibiting unfair or deceptive acts or practices.[1] The proposed consent order is the result of the FTC's two count complaint alleging Marriott made deceptive statements concerning their information security practices and failed to reasonably protect consumers' personal and financial information.[2] Additionally, this consent decree was announced in concert with the settlement of a coordinated investigation with 49 state attorneys general and the District of Columbia, which resulted in $52 million to be distributed among all 50 participants.[3]

The Electronic Privacy Information Center (EPIC) submits this letter to recommend approval of the FTC's proposed order as is and to encourage the Commission to continue instituting robust data security practices through enforcement and regulations. EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research,

[1] *See* Agreement Containing Consent Order, In re Marriott Int'l Inc. and Starwood Hotels & Resorts Worldwide, LLC, File No. 1923022 (Rel. Oct. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottacco.pdf [hereinafter Marriott Settlement]; *see also* Marriott Complaint, *In re* Marriott Int'l Inc. and Starwood Hotels & Resorts Worldwide, LLC, File No. 1923022 at ¶36 (Rel. Oct. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottcomplaint.pdf [hereinafter Marriott Complaint].
[2] Marriott Complaint at ¶¶ 33-35.
[3] Elizabeth Benton, *Attorney General Tong Co-Leads $52 Million Multistate Settlement with Marriott for Data breach of Starwood Guest Reservation Database,* Press Release, The Office of the Attorney General, Connecticut (Oct. 9, 2024), https://portal.ct.gov/ag/press-releases/2024-press-releases/multistate-settlement-with-marriott-for-data-breach-of-starwood-guest-reservation-database.

and litigation. EPIC routinely files comments in response to proposed FTC consent orders and complaints regarding business practices that violate privacy rights.[4]

EPIC commends the Commission for its use of Section 5 authority to protect consumers from Marriott's dangerous cybersecurity practices and hopes the Commission will continue to protect consumers in the same way.[5] EPIC also commends the Commission's coordination with state attorneys general, as they can be valuable partners in safeguarding consumer privacy and incentivizing companies to take their data security obligations seriously. Cybersecurity breaches have an outsized impact on consumers; consumers whose data have been lost to a breach are more susceptible to identity theft and financial fraud, and many suffer psychological harms such as anxiety, depression, and PTSD.[6] The breaches of Marriott and Starwood systems between 2014 and 2020 led to the extrication of uniquely sensitive information such as "passport numbers, . . . names . . . payment card numbers . . . telephone numbers, . . . hotel stays and other travel information, . . . number of children travelled with, and hotel stay preferences."[7] The compromise of this data creates a heavy burden for consumers to protect themselves from future harms, such as identity theft. Consumers can spend up to 18 months

[4] *See, e.g.*, Comments of EPIC, Demand Progress, and EFF in re the Federal Trade Commission's Proposed Order & Settlement with X-Mode Social, Inc. (Feb. 20, 2024), https://epic.org/documents/comments-of-epic-demand-progress-and-eff-in-re-the-federal-trade-commissions-proposed-order-settlement-with-x-mode-social-inc/; EPIC, EPIC Commends FTC for Including Data Minimization & Data Rights in Chegg Settlement (Dec. 12, 2022), https://epic.org/epic-commends-ftc-for-including-data-minimization-data-rights-in-chegg-settlement/; EPIC, EPIC Applauds FTC SpyFone Ban, Urges Similar Remedies in Future Privacy Cases (Oct. 8, 2021), https://epic.org/epic-applauds-ftc-spyfone-ban-urges-similar-remedies-in-future-privacy-cases/.

[5] *See, e.g.*, Comments of EPIC, *In re Chegg, Inc.*, FTC File No. 202-3151 (Dec. 12, 2022), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-chegg-inc/ [hereinafter EPIC re Chegg]; Comments of EPIC, *In re Blackbaud, Inc.*, FTC File No. 202-3181 (Mar. 2024), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-blackbaud/ [hereinafter EPIC re Blackbaud]; Comments of EPIC, *In re BetterHelp, Inc.*, FTC File No. 202-3169 (Apr. 12, 2022), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-betterhelp-inc/ [hereinafter EPIC re BetterHelp]; Comments of EPIC, *In re Global Tel*Link*, FTC File No. 212-3012 (Dec. 2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-global-tellink/ [hereinafter EPIC re GTL].

[6] *See, e.g.*, Danielle Citron & Daniel Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, Texas L. Rev. (2018), https://scholarship.law.bu.edu/faculty_scholarship/616/; Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, DOJ, Doc. No. NCJ 306474 at 12 (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf; Ido Kilovaty, "Psychological Data Breach Harms," U.N.C. J. of L. & Tech. (2021), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1432&context=ncjolt; Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA Today (Feb. 24, 2020), https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/; Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, Info. Sec. (Sep. 12, 2016), https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/.

[7] Marriott Complaint at ¶ 16.

to resolve even just the immediate consequences of identity theft.[8] The impacts felt by breaches can become more severe with time, especially when sensitive information is lost to successive breaches.[9]

Marriott and other businesses have no shortage of best practices and regulatory guidance to rely on when it comes to reasonably safeguarding consumers' personal data from breaches. The FTC has been clear about its data security expectations for businesses, including through the Commission's business guidance, the Safeguards Rule, and its case-by-case enforcement. In EPIC's comments on the FTC's Advanced Notice of Public Rulemaking on Commercial Surveillance & Data Security, we noted that the wide range of cybersecurity cases the Commission has brought provides sufficient precedent to establish poor data security as a deceptive trade practice[10] and unfair trade practice.[11] Moreover, there is broad consensus about the core elements of effective data security: the remedies imposed in the FTC's data security cases are very similar to requirements established across multiple cybersecurity frameworks.[12] Companies have enough information to build cost-effective cybersecurity programs that protect consumers.[13]

Several of the deficiencies in Marriott's cybersecurity practices bear striking resemblance to issues this Commission highlighted in its investigation of another hospitality company, Wyndham Worldwide Corporation (Wyndham). The Commission found that Wyndham, "failed to . . . [employ] firewalls . . . failed to remedy known security vulnerabilities on Wyndham-branded hotels' servers . . . [and] failed to adequately restrict third-party vendor's access to [Wyndham's] network."[14] Here, the Commission has alleged that Marriott has, "failed to implement appropriate password controls . . . failed to patch outdated software . . . leaving Starwood's network susceptible to attacks. . . failed to implement appropriate access controls . . . [and] failed to implement firewall controls."[15] In Wyndham,

---

[8] IDShield, *How Long Does it Take to Fix Identity Theft?* (Feb. 21, 2022), https://www.idshield.com/blog/identity-theft/how-many-hours-fix-identity-theft/ (citing to Bureau of Justice Statistics, FTC, Experian, and others).

[9] *See, e.g.*, Brief for Electronic Frontier Foundation and EPIC as Amici Curiae, Supporting Plaintiffs-Appellee, *Peter Maldini v. Marriott International Inc.*, No. 22-1744(L), at 6-9 (Nov. 11, 2022), https://epic.org/documents/peter-maldini-v-marriott-international-inc/.

[10] EPIC, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem (Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security) at 194 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter Disrupting Data Abuse].

[11] Id. at 191.

[12] Id. at 194–97; *see also* Comments of EPIC, *In re Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations (RFI)*, ONCD-2023-0001 at App'x 1 (Oct. 2023), https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/.

[13] *See, e.g.*, FINRA, *Report on Cybersecurity Practices* (Feb 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; NIST, *The NIST Cybersecurity Framework 2.0* (Feb. 26, 2022), *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*; CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.

[14] Complaint, *FTC v. Wyndham Worldwide Corporation*, WL 12372027 at ¶ 24 (D.N.J. 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

[15] Press Release, FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches, FTC (Oct. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches.

the court likened these cybersecurity violations to an egregious failure to clean up banana peels to such an extent that hundreds of thousands of consumers slipped on them.[16]

EPIC is particularly supportive of the order's proposed mandates relating to vendor oversight, working with a third-party auditor, and data minimization.[17] Vendors are prevalent vectors for breaches, so prospectively ensuring Marriott does not entrust consumer data to deficient service providers is a timely preventative measure.[18] Independent auditing is important for accountability because it can be a conflict of interest for companies to evaluate their own cybersecurity compliance ("grade their own homework") after having already been found deficient.[19] Lastly, data minimization is an essential feature of effective data security and mitigates the impact of breaches like this one. The Commission is right to restrict Marriott's retention of personal data to what is reasonably necessary to fulfill the purpose of collection, just as the FTC has imposed data minimization obligations in numerous prior consent decrees.[20] EPIC has consistently supported these provisions, which lead to stronger cybersecurity programs and better outcomes for consumers and companies alike.[21]

EPIC urges the Commission to finalize the proposed Marriott consent order as is. We also encourage the Commission to continue reinforcing its unfairness authority in the data security context and centering data minimization in its enforcement actions and regulations. If there are any questions, please contact Chris Frascella, EPIC Counsel, at [redacted]

Sincerely,

/s/ *John Davisson*
EPIC Director of Litigation &
Senior Counsel

/s/ *Chris Frascella*
EPIC Counsel

/s/ *Matt Contursi*
EPIC IPIOP Clerk

[16] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015) ("[W]ere Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).").
[17] Marriott Settlement at 6, 8, 12.
[18] Disrupting Data Abuse at 204–05.
[19] *Id.* at 208 (citing Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower).
[20] Decision and Order, *In re CafePress*, File No. 1923209 at 6-8 (Jun. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/192%203209%20-%20CafePress%20combined%20package%20without%20signatures.pdf; Decision and Order, *In re Avast Limited*, File No. 2023033 at 9,11 (Feb. 22, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/D%26O-Avast.pdf; Decision and Order, *In re X-mode Social Inc.*, File No. 212-3038 at 8-9 (Apr. 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf; Decision and Order, *In re InMarket Media, LLC.*, File No. 202-3088 at 8-10 (May 1, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/D%26O-InMarketMediaLLC.pdf.
[21] *See generally* EPIC re Chegg; EPIC re Blackbaud; EPIC re GTL; EPIC re BetterHelp.