February 3, 2020

Ring LLC Faces a Proposed Class Action Alleging Camera Doorbells Should Incorporate Enhanced Cybersecurity Features

On December 26, 2019, Amazon and Ring LLC were named as defendants in a putative class action filed in the U.S. District Court for the Central District of California by plaintiffs alleging claims of over $5 million. While there are myriad counts and allegations in the complaint, the central allegation appears to be that Ring should have required users to utilize the option of two-factor authentication to access their accounts and connected devices—an option that is available on Ring systems but not required when setting up an account. The case raises important questions about whether litigation of this kind will lead companies that handle sensitive personal information to require users to utilize security mechanisms such as two-factor authentication and complex passwords.

Background

Ring is a home security and smart home company. According to the complaint, Ring's flagship product is a video doorbell that contains a high-definition camera, a motion sensor, and a microphone and speaker for two-way audio communication. The smart doorbell integrates with an associated mobile app that enables its users to view real-time video from the camera, receive notifications and communicate with visitors. In addition to the video doorbell, Ring also sells other home security products, including a complete home alarm system as well as a variety of security cameras. Ring was acquired by Amazon in February 2018 for an estimated value of over $1 billion and is now a wholly owned subsidiary of Amazon. On January 9, 2020, Plaintiffs voluntarily dismissed their claims against Amazon, leaving Ring as the only defendant in the case.

The complaint alleges that John Baker Orange, the lead plaintiff, bought a Ring outdoor camera in July 2019 for approximately $249 to provide additional home security. Orange alleges that one day, while his children were playing basketball outside, a voice came through the camera's two-way speaker commenting on their game and encouraging them to get closer to the camera. Plaintiffs allege that this was just one of a number of examples of Ring video doorbells and cameras being compromised, and Plaintiffs allege that Ring knew about the system's security vulnerabilities.[1] Plaintiffs allege that Ring failed to

[1] There have been several recent press reports of bad actors hijacking Ring accounts. *Stranger spews racial slurs over family's hacked Ring camera*, NBC-2 (Dec. 9, 2019), https://www.nbc-2.com/story/41428183/stranger-spews-racial-slurs-over-familys-hacked-ring-camera (updated Dec. 11, 2019); Jessica Holley, *Family says hackers accessed a Ring camera in their 8-year-old daughter's room*, WMC Action News 5 (Dec. 10, 2019), https://www.wmcactionnews5.com/2019/12/11/family-says-hackers-accessed-ring-camera-their-year-old-daughters-room/ (updated Dec. 12, 2019); Matt Howerton, *Hacker says, 'pay bitcoin ransom or get terminated,' through couple's Ring security cameras*, WFAA 8 (Dec. 11, 2019) https://www.wfaa.com/article/news/hacker-says-pay-bitcoin-ransom-or-get-terminated-through-couples-ring-security-cameras/287-226c535c-c765-4b29-91b6-d849fb315e94.

enhance security features and, instead, blamed hacking incidents on poor security practices by users, such as using the same username and password for multiple accounts and services.

Plaintiffs claim that Ring has failed to fulfill its promise to provide privacy and security for its customers, in part because Ring failed to require users to rely on strong passwords and utilize two-factor authentication, and that it failed to alert users of attempted logins from unknown IP addresses. Plaintiffs assert causes of action under common law tort theories, including negligence and invasion of privacy; contract theories, such as breach of the implied warranty of merchantability, breach of implied contract and unjust enrichment; and for violations of California's Unfair Competition Law.

Implications

The case against Ring raises important questions about the standard of care that is required of companies that handle sensitive personal data, including whether in certain circumstances companies are required to both put in place mechanisms like two-factor authentication and the use of strong passwords and then require users to utilize those mechanisms—as opposed to just recommending or offering these options. As "smart devices" and the "Internet of Things" ("IoT") are increasingly part of everyday life, the answers to these questions could have significant implications. Companies that offer smart devices and IoT, and their associated services, may do well to pay close attention to how these issues develop, so that they can adopt practices that will protect them from potential liability. In the meantime, companies engaged in online services should stay up-to-date on security standards and enhancements, routinely update their security systems, and consider having users take steps to reduce the risk of a compromise, such as creating passwords with certain levels of complexity.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Jonathan S. Kanter
+1-202-223-7317
jkanter@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

Jeannie S. Rhee
+1-202-223-7566
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Daniel J. Klein and Apeksha S. Vora contributed to this Client Alert.