,

600 Pennsylvania Ave., NW
Washington, DC 20580,

,

v.

,

a Delaware limited liability company,
12515 Cerise Ave
Hawthorne, CA 90250,

.

1:23-cv-1549

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), which authorizes the FTC to seek, and the Court to order, permanent injunctive relief and other relief for Defendant's acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

3. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(1), (c)(2), and (d) and 15 U.S.C. § 53(b).

4. The FTC is an independent agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own

attorneys. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. Defendant Ring LLC ("Ring") is a Delaware corporation with its principal place of business at 12515 Cerise Ave, Hawthorne, California, 90250. Ring transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Ring has advertised, marketed, distributed, or sold merchandise to consumers throughout the United States.

6. At all times material to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

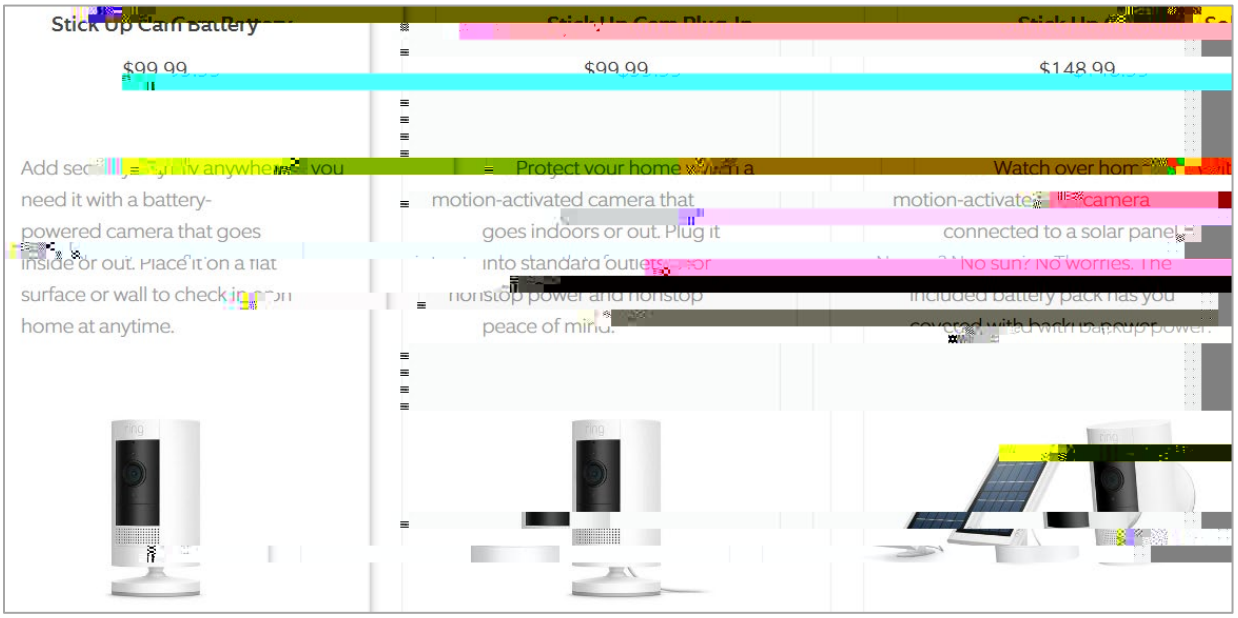
7. Ring advertises, markets, and sells Internet-connected, video-enabled security cameras, doorbells, and related accessories and services to consumers throughout the United States and in other countries. Since 2016, Ring has sold more than a million indoor cameras, including the "Stick Up Cam" (launched in 2016) and the "Indoor Cam" (launched in 2019). Customers routinely use Ring's indoor cameras as baby monitors and to monitor private spaces of the home, including adults' bedrooms, children's bedrooms, and bathrooms.

Increase

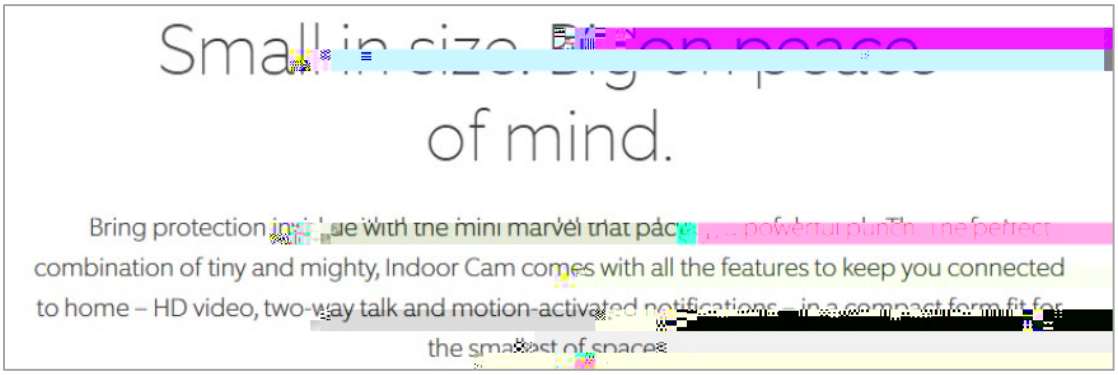
8. Since its founding, Ring has consistently claimed that its products make individuals, families, and children safer and more secure in their homes. For example, Ring's website announces that its "mission" is to "Make Neighborhoods Safer" and, as a 2014 post on

Ring's blog explains, the company's name derives from "the 'ring' of security we create around your home, and then in time your community." The tagline for Ring security cameras is "Smart security here, there, everywhere."

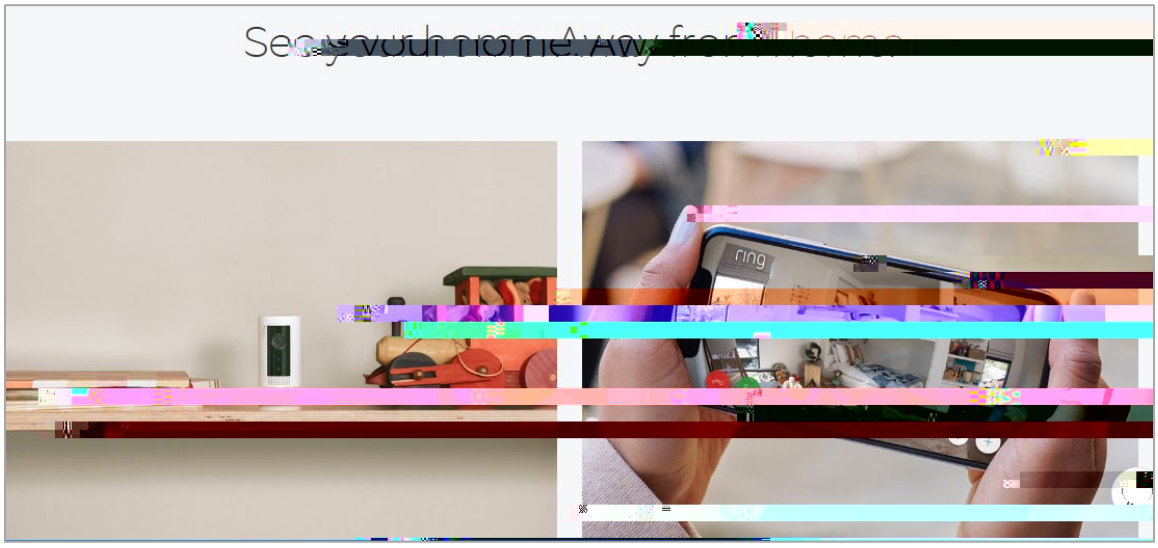
9. Since January 2016, Ring has claimed that its Ring Stick Up Cam enhances users' security within the home. Ring has represented that its Ring Stick Up Cam lets users "[a]dd security anywhere you need it," "[p]rotect your home," and "[w]atch over home."



10. Since September 2019, Ring has marketed the Ring Indoor Cam as "Small in size. Big on peace of mind," and encouraged customers to "[b]ring protection inside with the mini marvel…."



11. With the tagline “See your home. Away from home,” Ring displays pictures on the Ring website of a Ring camera monitoring children’s bedrooms.



12. The claims in Paragraphs 8-11 have implied to reasonable consumers that Ring devices are a secure means to monitor the private spaces of consumers’ homes. Reasonable consumers have understood that Ring’s security claims have implied, in part, a claim of digital security, because a lack of digital security would impede the devices’ basic function: their ability to “protect [the] home,” “[b]ring protection inside,” and allow customers to “[s]ee your home...[a]way from home,” as Ring’s website promises. If, for example, a hacker could readily compromise the device’s digital security and turn off the security camera, the device would have no value as the security monitoring product that the consumer purchased. Moreover, reasonable consumers have understood that Ring’s security claims have implied, in part, a claim of digital security, because a lack of digital security creates the very risk of harm that the device was intended to minimize, such as where a hacker stalks, harasses, or threatens the consumer or her family members through a compromised device.

13.

16. This approach to access meant that Ring's employees and third-party contractors had dangerous—and unnecessary—access to highly sensitive data. For example, although a customer service agent might need access to the video data of a particular customer to troubleshoot a problem, that same customer service agent had unfettered access to videos belonging to thousands of customers who never contacted customer service. Although an engineer working on Ring's floodlight camera might need access to some video data from outdoor devices, that engineer had unrestricted access to footage of the inside of customers' bedrooms.

17. As a result of this dangerously overbroad access and lax attitude toward privacy and security, employees and third-party contractors were able to view, download, and transfer

escalate the report of misconduct. Only at that point did Ring review a portion of the employee's activity and, ultimately, terminate his employment.

19. In September 2017, in response to this incident, Ring narrowed employee access to customers' video data somewhat, so that customer service agents could only access videos with the customers' consent. Despite this narrowing of access for customer service agents, Ring continued to allow others—including hundreds of employees and Ukraine-based third-party contractors—access to all video data, regardless of whether particular engineers actually needed to have access to that data to perform their job function.

20. Granting employees such grossly overbroad and unmonitored access continued to cause harm. In January 2018, a male employee used his broad access rights to spy on a female colleague through her videos. Using her email address as a look-up mechanism, the employee identified his female co-worker's device and watched her stored video recordings without her permission.

21. After this second known instance of employee misconduct related to customers' sensitive video data, Ring belatedly narrowed access to video data. In February 2018—when improving security practices to make Ring more appealing to potential acquirers—Ring finally started limiting the videos used for research and development to videos posted by customers to Ring's Neighbors app, and those for which employees, contractors, and their friends and family had given their written consent for such use. Also in February 2018, as part of this belated clean-up effort, Ring changed access rights so that engineers (both employees and Ukraine-based third-party contractors) could only access customer videos if they had a business need to do so.

22. Despite these changes, Ring's culture of overly broad access to sensitive information continued to result in harm to consumers. First, in February 2018, a Ukraine-based

train algorithms by labeling people or objects, to provide customer service for a particular account), Ring did not adequately notify customers or obtain customers' consent for extensive human review of customers' private video recordings.

26. Before December 2017, Ring's Terms of Service and Privacy Policy did not inform customers that Ring employees and contractors would have the right to review all video recordings for product improvement and development. In the middle of lengthy terms dense with legalese, Ring merely described the company's right to use recordings obtained in connection with Ring's (then called Doorbot's) cloud service for product improvement and development. As a result of this buried half-explanation, customers had no reasonable way of knowing that hundreds of Ring employees and third-party contractors in Ukraine had unfettered access to live streams and stored videos of customers in their Th(D)2 (oor)gh (pl)-2 (oye)4 (e)p33 0 T (t)-2 (,t)-2 (,t)-2 (,t)-2 (,t

36. Knowing this, Ring should have implemented controls to prevent a recurrence of such attacks, especially when available controls (such as requirements for strong and unique passwords) were easy to implement at low cost.

37. Second, Ring received numerous reports of vulnerabilities relevant to credential stuffing and brute force attacks through Ring's "bug bounty" program. This program rewards security researchers and white hat hackers with "bounties" (i.e., payments) in exchange for identifying security vulnerabilities. Between September 2017 and April 2019, the program received four separate bug bounty reports about Ring authentication portals being vulnerable to credential stuffing and brute force attacks, because Ring did not use effective rate limiting. Indeed, one researcher reported in April 2019 that he was able to "guess my own password [to a Ring login] after 1000 tries without getting detected."

38. Third, in December 2018 and April 2019, there were numerous media reports of credential stuffing attacks, including attacks against devices made by Ring competitor Nest. Ring was aware both of reported attacks on Nest and of how susceptible Ring was to similar attacks, based on Ring's lack of key security features.

39. Finally, Ring also received pointed warnings from its own security testing personnel. Specifically, penetration tests conducted by a third-party security firm pointed to the weakness in Ring's password requirements for customer accounts. Rather than requiring strong, complex passwords, Ring permitted users to set very simple passwords for their accounts, such as abcd1234. Permitting users to set easily guessable passwords heightened the risk that any credential stuffing or brute force attack would succeed.

40. The few security measures Ring did implement to address these risks were too little and too late. For example, Ring made two-factor authentication available to customers in

May 2019 (long after this feature had been routine for other companies holding sensitive data), but did not take reasonable steps to encourage its adoption, such as through user-friendly opt-ins for existing customers and default opt-outs for new users. As a result, only a tiny fraction of customers—less than 2%—adopted this optional security feature in 2019.

41. In addition, although Ring implemented some forms of rate limiting before July 2019, not all authentication portals were covered. Moreover, what rate limiting Ring did implement (to prevent multiple login attempts in rapid succession to the same account) did only half the job: Ring failed to block multiple attempts in rapid succession to log into different accounts from the same IP address. As a result of Defendant's failures to act (or to act in full), between January 2019 and March 2020, more than 55,000 U.S. customers suffered from credential stuffing and brute force attacks that compromised Ring devices. Through these attacks, bad actors gained access to hundreds of thousands of videos of the personal spaces of consumers' homes, including their bedrooms and their children's bedrooms—recorded by devices that Ring sold by claiming that they would increase consumers' security.

42. Ring took some short-term steps to correct the problem beginning in July 2019, such as locking accounts, resetting passwords, disconnecting devices, and recommending good password practices and the use of two-factor authentication. Ring also implemented certain new security measures, such as a web application firewall and encrypting video data at rest (which numerous competitors had long before implemented). However, Ring did not take other, more effective measures to prevent the attacks, such as those described in Paragraphs 31-34.

43. Because Ring did not take these measures, the attacks continued to succeed. For example, on December 12, 2019, prominent media outlets began publishing reports about hacked Ring devices, where hackers used access to cameras to harass and threaten children and families.

44.

e. A hack

c. before January 2018, did not restrict engineers' access to consumers' sensitive video data to what the engineers needed to perform their job function;

d. before January 2018, failed to monitor employees' and third-party contractors' access to customers' sensitive video data;

e. before January 2018, failed to obtain customers' consent to review their sensitive video data for research and development and product improvement purposes;

f. before January 2018, failed to detect employees' and third-party contractors' unauthorized access to customers' sensitive video data through technical means;

g. before May 2018, did not provide employees or third-party contractors with any data security training or other training on the proper handling of consumers' sensitive video data;

h. before August 2019, did not encrypt customers' video data at rest, despite the sensitivity of this data; and

i. before January 2020, failed to implement reasonable safeguards to prevent credential stuffing or brute force attacks against cameras sold for use in private spaces of the home, enabling hackers to compromise accounts.

49. Defendant's failures to take reasonable steps to prevent unauthorized access to the live feeds and stored videos of cameras marketed by Ring for use in intimate areas of customers' homes has caused or is likely to cause substantial injury to consumers in the form of, among other things, direct monetary loss. First and foremost, consumers did not receive the benefit of their bargain; they believed they were purchasing reasonably private and secure devices but in fact received devices that compromised their privacy and security. In addition, consumers

suffered other injuries, including time spent remedying the problem (such as filing police reports and research

VIOLATIONS OF SECTION 5 OF THE FTC ACT

53. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

54. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

55. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

56. In numerous instances, in connection with the advertising, marketing, promotion, offering for sale, or sale of home security cameras and related devices and services, Defendant has represented, directly or indirectly, expressly or by implication, that Defendant took reasonable steps to ensure that Ring camera (d)-14 pnt

59. Defendant allowed thousands of employees and contractors to access video recordings of customers' intimate spaces without customers' knowledge or consent.

60. Defendant's actions have caused, cause, or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

61. Therefore, Defendant's acts or practices as set forth in Paragraph 59 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

62. In numerous instances, Defendant has failed to provide reasonable security to prevent unauthorized access to the live feeds and stored videos of its cameras, which Defendant offered to consumers for the purpose of monitoring and securing private areas of their homes.

63. Defendant's actions have caused, cause, or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

64. Therefore, Defendant's acts or practices as set forth in Paragraph 62 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

---

65. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act. Absent injunctive relief by this Court, Defendant are likely to continue to injure consumers and harm the public interest.

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendant; and

B. Award monetary and other relief within the Court's power to grant.

Respectfully submitted,

Dated: 5/31/2023

/s/ Elisa Jillson

ELISA JILLSON
D.C. Bar No. 989763
ANDREW HASTY
D.C. Bar No. 1033981
JULIA HORWITZ
D.C. Bar No. 1018561
Federal Trade Commission
600 Pennsylvania Ave., NW