

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FEDERAL TRADE COMMISSION,
600 Pennsylvania Ave., NW
Washington, DC 20580,

Plaintiff,

v.

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

Defendant.

Case No. 1:23-cv-1549

**COMPLAINT FOR PERMANENT
INJUNCTION AND OTHER RELIEF**

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).

JURISDICTION AND VENUE

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).

PLAINTIFF

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.

DEFENDANT

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.

COMMERCE

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.

DEFENDANT’S BUSINESS ACTIVITIES




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.

Defendant Has Claimed That Its Products *Increase* Customers’ Security

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.”

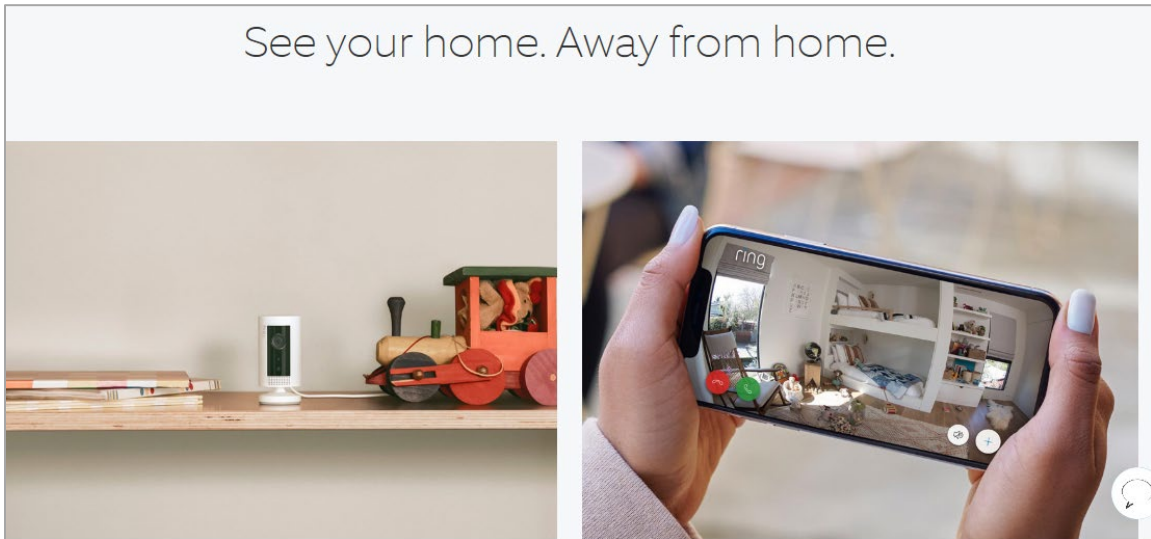
Stick Up Cam Battery	Stick Up Cam Plug-In	Stick Up Cam Solar
\$99.99	\$99.99	\$148.99
Add security anywhere you need it with a battery-powered camera that goes inside or out. Place it on a flat surface or wall to check in on home at anytime.	Protect your home with a motion-activated camera that goes indoors or out. Plug it into standard outlets for nonstop power and nonstop peace of mind.	Watch over home with a motion-activated camera connected to a solar panel. No sun? No worries. The included battery pack has you covered with backup power.
		

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....”

Small in size. Big on peace of mind.

Bring protection inside with the mini marvel that packs a powerful punch. The perfect combination of tiny and mighty, Indoor Cam comes with all the features to keep you connected to home – HD video, two-way talk and motion-activated notifications – in a compact form fit for the smallest of spaces.

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.

Defendant Ring Gave Every Ring Employee and Contractor Unnecessary and Unrestricted Access to Customers' Sensitive Video Data

13. Despite promising greater security as its products' core feature, Ring ignored information security considerations when management believed they would interfere with growth. In pursuit of rapid product development, before September 2017, Ring did not limit access to customers' video data to employees who needed the access to perform their job function (e.g., customer support, improvement of that product, etc.). To the contrary, Ring gave every employee—as well as hundreds of Ukraine-based third-party contractors—full access to every customer video, regardless of whether the employee or contractor actually needed that access to perform his or her job function.

14. Not only could every Ring employee and Ukraine-based third-party contractor access every customer's videos (all of which were stored unencrypted on Ring's network), but they could also readily download any customer's videos and then view, share, or disclose those videos at will. Before July 2017, Ring did not impose any technical or procedural restrictions on employees' ability to download, save, or transfer customers' videos.

15. Ring also did not train employees to handle customers' sensitive video data with care, even though all employees and third-party contractors had this broad access and some were tasked with reviewing customers' video data for various purposes, including customer support, product improvement, and research and development. Ring distributed an employee handbook that prohibited misuse of Ring data and required employees to sign a Proprietary Information and Inventions Agreement that prohibited data misuse. However, despite the fact that Ring was collecting mass quantities of highly sensitive data, Ring did not conduct any training on privacy or data security before May 2018—or otherwise advise employees or third-party contractors that customers' video data was sensitive and should be treated as such.

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 customers’ sensitive video data for their own purposes. For example, between June and August 2017, a Ring employee viewed thousands of video recordings belonging to at least 81 unique female users (including customers and Ring employees) of Ring Stick Up Cams. The employee focused his prurient searches on cameras with names indicating that they surveilled an intimate space, such as “Master Bedroom,” “Master Bathroom,” or “Spy Cam.” On hundreds of occasions during this three-month period, the employee perused female customers’ and employees’ videos, often for an hour or more each day. Undetected by Ring, the employee continued spying for months.

18. Ring failed to detect this inappropriate access through any technical means. By good fortune, in August 2017, an employee discovered her co-worker’s actions and reported the misconduct to her supervisor. Initially, the supervisor discounted the report, telling the female employee that it is “normal” for an engineer to view so many accounts. Only after the supervisor noticed that the male employee was only viewing videos of “pretty girls” did the supervisor

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

third-party contractor created an unauthorized “tunnel” or pathway to Ring services in an attempt to access customer video data. Ring failed to detect this intrusion by any technical means. Only when an employee happened to report the misconduct did Ring remove the Ukrainian team’s ability to create such unauthorized pathways. Second, in May 2018, another employee gave information about a customer’s video recordings to the customer’s ex-husband without the customer’s consent. Third, in August 2020, a whistleblower notified Ring that between March 2018 and September 2019, a former employee had provided Ring devices to numerous individuals and then accessed their videos without their knowledge or consent. When the employee left Ring in September 2019, the whistleblower alleged that he took copies of these videos with him—without the knowledge or consent of his unsuspecting victims and without Ring noticing that anything was amiss.

23. In February 2019, Ring changed its access practices so that most Ring employees or contractors could only access a customer’s private video with that customer’s consent.

24. Importantly, because Ring failed to implement basic measures to monitor and detect inappropriate access before February 2019, Ring has no idea how many instances of inappropriate access to customers’ sensitive video data actually occurred. Indeed, Ring only discovered the incidents described above through the good fortune of employee reporting, despite having given employees zero security training and no responsibility to engage in such reporting. It is highly likely that numerous other incidents of spying, prurient behavior, and other inappropriate access occurred entirely undetected.

Defendant Ring Did Not Adequately Notify or Obtain Customers’ Consent Before Allowing Thousands of Employees and Contractors to Watch Video Recordings of Customers’ Private Spaces

25. Even when Ring employees and third-party contractors may have had a business purpose to access video recordings of customers’ private spaces on particular occasions (e.g., to

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 bedrooms, their bathrooms, their children's nurseries, and elsewhere in and outside their homes.

27. Between December 2017 and January 2018, Ring described its use of device recordings for product improvement and development in its Privacy Policy, but buried this description in dense and lengthy legalese. To obtain customers' "consent" for this invasive review of highly sensitive data, Ring merely required customers to check a box acknowledging that they agreed to Ring's Terms of Service and Privacy Policy.

28. Only in January 2018 did Ring finally begin to take steps to obtain consumers' consent for review of their sensitive video data for research and development purposes. At that point, Ring began limiting research and development to videos publicly posted on the Internet or for which employees, contractors, and their friends and family had given their written consent for such use on a document that clearly informed the consumer of Ring's review of their video data.

29. Ring’s paltry process for informing customers and obtaining their “consent” before January 2018 was especially harmful because, as described in Paragraphs 13-24, Ring allowed hundreds of employees and third-party contractors to access and view customers’ private spaces, rather than limiting access for product improvement and development to a few, well-trained employees whose compliance with reasonable access policies was carefully monitored.

**Defendant Ring Failed to Secure Ring Devices From
Credential Stuffing and Brute Force Attacks**

30. Before January 2020, Ring systematically failed to appreciate and control for the risk of at least two types of well-known online attacks: “credential stuffing” and “brute force.” With a credential stuffing attack, the attacker finds breached login credentials (e.g., usernames and passwords) on the Internet and then uses them to try to access consumers’ accounts on other systems or services not associated with the original breach. If a consumer has reused a breached username and password when creating a Ring account, the bad actor can gain full access to the consumer’s account. Relatedly, a brute force attack involves an automated process of password guessing—for example, by cycling through breached credentials, entering well-known passwords or variations of well-known passwords, etc.—hundreds or thousands of times.

31. Because these are well-known forms of attack, there are many standard security measures for preventing such attacks. For example, requiring a unique password (i.e., one not previously used before) helps prevent credential stuffing, and requiring strong, complex passwords reduces the likelihood that an attacker can use brute force to guess the credential.

32. Another common method of preventing such attacks is to notify users of suspicious logins—that is, when someone logs into their account from a new device or suspicious IP address. A third method is to monitor and notify users of concurrent sessions—e.g., when two devices are simultaneously logged into the same account. A fourth method is called

“rate limiting,” a process of blocking repeated attempts in rapid succession to log into (a) the same account with different passwords or (b) multiple accounts from the same IP address. And a fifth method is to compare passwords that device owners try to set against known compromised credentials to ensure no reuse of breached passwords.

33. Finally, another highly effective method of protecting user accounts is multi-factor authentication, which requires the user to provide at least two different forms of authentication (such as a password plus a code texted to a mobile device). Using multiple factors provides much greater security than a single factor (i.e., a password) alone, because a compromised password, by itself, is not enough to access the account. Companies that hold sensitive consumer information frequently use multi-factor authentication to protect that data. For this reason, many of Ring’s competitors made multi-factor authentication available to their customers long before Ring finally did in May 2019.

34. Indeed, after April 2018, Ring could have used a trust management system called Transaction Risk Management System or “TRMS.” Ring did not adopt TRMS.

35. First, in 2017 and 2018, Ring experienced multiple credential stuffing attacks. In a 2019 document justifying the belated implementation of one security control (a Web Application Firewall or “WAF”), Ring employees wrote of the 2017-2018 attacks: “Unwittingly, we aid and abet those [hackers] who breached the data by not having any mitigations in place.” In this document, the author notes that Ring permitted “thousands of requests [for account access] per second” from a single IP address (i.e., a single user), rather than an appropriate “half dozen per day.” The author notes, “If we can slow the attacker down, they will definitely look elsewhere, as we’ve destroyed their economic model of cheap and fast bulk verification of stolen user account credentials.”

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. During the course of these attacks, approximately 55,000 U.S. customers suffered serious account compromises. For at least 910 U.S. accounts (affecting approximately 1,250 devices), the bad actor not only accessed the accounts, but took additional invasive actions, such as accessing a stored video, accessing a live stream video, or viewing a customer's profile. The bad actors disproportionately targeted indoor cameras. Even though indoor cameras are a relatively small subset of Ring's product offerings, approximately 500 of the 1,250 compromised devices in the U.S. (i.e., approximately 40% of the compromised devices in the U.S.) were Stick Up Cams or Indoor Cams, both of which Defendant markets for indoor use.

45. In many cases, these instances of unauthorized access were not short-lived invasions. In at least 20 instances, for example, the bad actors maintained unauthorized access to the accounts' devices for more than one month.

46. And, in many instances, the bad actors were not just passively viewing customers' sensitive video data. Rather, the bad actors took advantage of the camera's two-way communication functionality to harass, threaten, and insult individuals—including elderly individuals and children—whose rooms were monitored by Ring cameras, and to set off alarms and change important device settings. Examples of the harassment, slurs, and threats that consumers experienced include the following:

- a. Several women lying in bed heard hackers curse at them;
- b. Several children were the objects of hackers' racist slurs;
- c. A teenager was sexually propositioned;
- d. An 87-year old woman in an assisted living facility was sexually propositioned and physically threatened;

- e. A hacker told an individual through her camera that the hacker had killed the individual's mother and then directly threatened the individual: "Tonight you die";
 - f. After a hacker taunted one child in the bedroom she shared with her siblings, the child developed a strong fear of her bedroom and required therapy and physical changes to her room to help her overcome her fear;
 - g. One hacker threatened a family with physical harm if they did not pay a ransom in Bitcoin; and
 - h. A hacker told a woman that her location was being tracked and that her device would self-destruct at the end of his countdown; she disconnected the device before his countdown ended.
47. Consumers whose accounts were hacked told Defendant in emailed complaints that they felt "terrified," "extremely traumatiz[ed]," "appalled," and "fear[ful]."

Defendant Ring's Unreasonable Data Security and Privacy Practices

48. From at least 2016 through January 2020, Ring engaged in a number of unreasonable data security and privacy practices. Among other things, Ring:
- a. before September 2017, gave all employees and third-party contractors access to consumers' sensitive video data, regardless of whether the employee or contractor needed such access to perform his or her job function;
 - b. before July 2017, did not impose any technical restrictions on employees' and third-party contractors' ability to view, download, save or transfer customers' videos;

- 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.

**Defendant Ring's Unreasonable Data Security
and Privacy Practices Harmed Consumers**

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 researching and purchasing more secure devices). Moreover, the exposure of customers' sensitive video data increases the likelihood that consumers or their property will be targeted for theft, stalking, harassment, or other criminal activity. Defendant's failures to provide reasonable security have increased the likelihood that consumers' personal activities and conversations or those of their family members, including young children, will be observed and recorded by strangers over the Internet, and that downloaded or screen-captured copies of these videos would be used by strangers for purposes of extortion, harassment, or public embarrassment. These risks impair consumers' peaceful enjoyment of their homes, increase consumers' susceptibility to physical tracking or stalking, and reduce consumers' ability to control the dissemination of private video feeds.

50. Similarly, Ring's unreasonable review practices have caused or were likely to cause substantial injury. Enabling hundreds of employees and third-party contractors to access private videos taken in intimate areas of consumers' homes placed consumers at risk from the exposure of their personal information. Consumers were also injured by the unwarranted invasion into the peaceful enjoyment of their homes. This surreptitious review of the private details of individual and family life—including images of visitors, children, family interactions, partially undressed individuals, and people engaged in intimate conduct—caused actual consumer harm.

51. Ring's customers had no way of independently knowing about Ring's security and privacy failures and could not reasonably have avoided possible harms from such failures.

52. Ring could have prevented or mitigated these failures through readily available and relatively low-cost measures.

VIOLATIONS 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).

Count I

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 cameras are a secure means to monitor private areas of consumers’ homes.

57. In truth and in fact, in numerous instances in which Defendant has made the representations set forth in Paragraphs 8-11, Defendant did not take reasonable steps to ensure that Ring cameras are a secure means to monitor private areas of consumers’ homes.

58. Therefore, Defendant’s representations as set forth in Paragraph 56 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II

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).

Count III

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).

CONSUMER INJURY

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.

PRAYER FOR RELIEF

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
Mailstop CC-6316
Washington, DC 20580
(202) 326-3001 (voice)
(202) 326-3062 (fax)
Email: ejillson@ftc.gov
Email: ahasty@ftc.gov
Email: jhorwitz@ftc.gov

*Attorneys for Plaintiff
Federal Trade Commission*