

1 Hassan A. Zavareei (State Bar No. 181547)

2 Katherine M. Aizpuru*

3 **TYCKO & ZAVAREEI LLP**

4 1828 L Street NW, Suite 1000

5 Washington, D.C. 20036

6 Telephone: (202) 973-0900

7 Facsimile: (202) 973-0950

8 hzavareei@tzlegal.com

9 kaizpuru@tzlegal.com

10 Annick M. Persinger (State Bar No. 272996)

11 **TYCKO & ZAVAREEI LLP**

12 1970 Broadway, Suite 1070

13 Oakland, CA 94612

14 Telephone: (510) 254-6807

15 Facsimile: (202) 973-0950

16 apersinger@tzlegal.com

17 Norman E. Siegel*

18 Barrett J. Vahle*

19 J. Austin Moore*

20 **STUEVE SIEGEL HANSON LLP**

21 460 Nichols Road, Suite 200

22 Kansas City, MO 64112

23 Tel: 816-714-7100

24 siegel@stuevesiegel.com

25 vahle@stuevesiegel.com

26 moore@stuevesiegel.com

27 *Counsel for Plaintiffs and the Class*

18 **UNITED STATES DISTRICT COURT**
19 **CENTRAL DISTRICT OF CALIFORNIA**

20 ASHLEY LEMAY, DYLAN BLAKELEY,
21 TANIA AMADOR, and TODD CRAIG,

22 *On Behalf of Themselves and All Others*
23 *Similarly Situated,*

24 Plaintiffs,

25 v.

26 RING LLC,

27 Defendant.

Case No. 2:20-cv-074

**CLASS ACTION COMPLAINT
FOR DAMAGES, EQUITABLE,
INJUNCTIVE, and DECLARATORY
RELIEF**

- (1) NEGLIGENCE
- (2) VIOLATION OF CAL. BUS. & PROF. CODE § 17200
- (3) BREACH OF IMPLIED CONTRACT
- (4) UNJUST ENRICHMENT
- (5) INTRUSION UPON SECLUSION
- (6) PUBLIC DISCLOSURE OF PRIVATE FACTS

JURY TRIAL DEMANDED

1 Plaintiffs Ashley LeMay, Dylan Blakeley, Todd Craig, and Tania Amador (collectively,
2 “Plaintiffs”), on behalf of themselves and all persons similarly situated, bring this complaint
3 against Defendant Ring LLC (“Defendant” or “Ring”).

4 **I. INTRODUCTION**

5 1. Ring markets and sells home security devices. Intended for use inside the
6 home, Ring’s devices feature motion-activated cameras; a “live view” that allows users to
7 “check in on” their homes remotely; and a two-way talk feature that allows users to
8 communicate through the devices. According to Ring, its home security devices offer “smart
9 security here, there, everywhere.” Ring promises users that it takes security seriously and
10 will safeguard users’ private information.

11 2. But instead of helping families protect their homes, Ring security devices have
12 had the opposite effect by permitting hackers to exploit security vulnerabilities in the Ring
13 system to spy on and harass Ring customers inside their own homes.

14 3. That is exactly what happened to Ashley LeMay and her husband Dylan
15 Blakeley (“the Blakeleys”), as well as Todd Craig and his girlfriend Tania Amador. Plaintiffs
16 purchased Ring indoor security cameras to try to protect their homes and feel safer. Instead,
17 the Ring devices created a living nightmare by allowing intruders to come into their homes
18 and harass them and their families.

19 4. The Blakeleys purchased two of Ring’s security devices on November 29, 2019,
20 as part of a Black Friday sale. They installed the devices in their home so that Ms. LeMay
21 could check in on their four daughters during Ms. LeMay’s overnight shifts at a nearby
22 hospital. They also hoped the devices would notify them if their middle daughter, who suffers
23 from seizures, began to experience a seizure while Ms. LeMay was not home. At first, the
24 cameras gave the Blakeleys peace of mind, and helped their children feel safe.

25 5. That sense of security disappeared on December 4, 2019. Shortly after 8 p.m.,
26 both of the Ring cameras installed in the Blakeleys’ home began live-streaming, and the Tiny
27 Tim cover of “Tiptoe Through the Tulips,” a song that appeared in a scene from the 2020
28

1 horror film “Insidious,” began to play through the two-way talk feature. At the time, Ms.
2 LeMay was out running errands, but Mr. Blakeley was at home with their children.

3 6. Intrigued by the music, the Blakeleys’ eight-year-old daughter, A., went to the
4 room she shares with two of her younger sisters to investigate. But the room was empty. As
5 A. wandered the room, looking for the source of the music, the song abruptly stopped, and a
6 man’s voice rang out: “Hello there.”

7 7. It was a stranger—an unknown hacker, who had taken over the Blakeleys’
8 account and had the ability to see, hear, and speak to A. inside her own room. In a chilling
9 exchange captured on the device’s video recording, the hacker began shouting racial slurs at
10 A. and encouraging her to misbehave. The encounter ended only after a frightened A. left the
11 room to find her father, who disabled the device.

12 8. To this day, Ring has not disclosed the identity of this unknown hacker to the
13 Blakeleys, who have no way of knowing the motives of the digital intruder or whether he still
14 poses a threat to the safety of their family.

15 9. Only a few days later, the same thing happened to Mr. Craig and Ms. Amador
16 when an unauthorized hacker took control of the Ring system that they share in their home.

17 10. On December 9, 2019, Mr. Craig and Ms. Amador were interrupted by a voice
18 laughing and shouting, “Ring support! Ring support!” Ms. Amador, who was napping, was
19 awakened by the noise. Mr. Craig was standing in front of his indoor camera at the time of
20 the breach, and jumped at the sound, at first believing Ms. Amador was playing a joke on
21 him. But this was no joke. A stranger had hacked Mr. Craig’s Ring system and was spying on
22 the couple inside their home.

23 11. The hacker then accessed the couple’s doorbell camera and told them, “I’m
24 outside your front door.”

25 12. The voice also threatened the couple with “termination” if they did not pay a
26 ransom of 50 bitcoin.

27 13. Ring still has not disclosed the identity of the hacker who threatened Mr. Craig
28 and Ms. Amador. And while Ring initially told Mr. Craig that the account was hacked via Ms.

1 Amador’s account, it later walked back that statement and has since refused to confirm how
2 the intrusion occurred.

3 14. Reports of similar hacks have surfaced across the country, including in Florida,
4 Michigan, Georgia, Kansas, and Texas. *Vice News* recently reported on an incident in which
5 a hacker took over a Ring camera located in Florida. The hacker played a “blaring siren” into
6 the Ring camera, then announced, “It’s your boy Chance on Nulled. How you doing?”
7 “Chance” then blared noises and shouted racist comments at the Florida family who owned
8 the device.

9 15. “Chance” was participating in a widely livestreamed podcast, NulledCast,
10 which features live footage of hackers taking over peoples’ Ring smart-home cameras and
11 using the two-way communication function to talk to and harass their owners.

12 16. It is well known that Ring devices are vulnerable to hacking; hackers casually
13 share software to hack Ring cameras online, including through the Discord forum.

14 17. Despite the existence of the NulledCast podcast and the widespread
15 dissemination for tips and tricks on hacking Ring devices, Ring has refused to implement
16 even the most basic security precautions to secure their customers’ accounts.

17 18. Ring does not require users to implement two-factor authentication. It does
18 not double-check whether someone logging in from an unknown IP address is the legitimate
19 user. It does not offer users a way to view how many users are logged in. It offers no
20 protection from brute-force entries—mechanisms by which hackers can try an endless loop
21 of combinations of letters and numbers until they land on the correct password to unlock
22 account. Even though these basic precautions are common and unexceptional security
23 measures across a wealth of online services, Ring does not utilize them for its services.

24 19. Breaking into a Ring account grants access to exceptionally intimate and
25 private parts of someone’s life: the inside of their homes, sometimes their bedrooms. It can
26 put the user’s physical safety, or the safety of their families, at risk. It also exposes Ring
27 customers to the imminent risk of all manner of financial fraud, identify theft, extortion,
28

1 blackmail, or burglary. Ring's failure to take basic security precautions breached its duty to
2 safeguard the highly sensitive information to which their users entrusted them.

3 20. Ring's failure to properly safeguard access to user accounts is even more
4 egregious in light of the presence of hacking forums and podcasts dedicated to hacking Ring
5 devices.

6 21. Yet even in light of widespread reports of hacks and unauthorized access to
7 devices, Ring has refused to take responsibility for the security of its own home security
8 devices, and its role in compromising the privacy of its customers. Even as its customers are
9 repeatedly hacked, spied on, and harassed by unauthorized third parties, Ring has made the
10 non-credible assertions that it has not suffered any data breaches and that there are no
11 problems with the privacy and security of its devices.

12 22. Plaintiffs bring this lawsuit to hold Ring responsible for its defective devices
13 and systems, require that Ring take all necessary measures to secure the privacy of user
14 accounts and devices, and compensate Plaintiffs and the Class members for the damage that
15 its acts and omissions have caused.

16 **II. PARTIES**

17 23. Plaintiffs Ashley LeMay and Dylan Blakeley are residents of Mississippi.

18 24. Plaintiffs Todd Craig and Tania Amador are residents of Texas.

19 25. Defendant Ring LLC is a Delaware corporation with its principal place of
20 business in Santa Monica, California.

21 **III. JURISDICTION AND VENUE**

22 26. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). The
23 matter in controversy, exclusive of interest and costs, exceeds the sum or value of
24 \$5,000,000, and members of the Class are citizens of different states from Defendant.

25 27. This Court has personal jurisdiction over Defendant because it maintains
26 headquarters in this District and operates in this District. Through its business operations
27 in this District, Defendant intentionally avails itself of the markets within this District to
28 render the exercise of jurisdiction by this Court just and proper.

1 28. Venue is proper in this Court under 28 U.S.C. § 1391 because significant events
2 giving rise to this case took place in this District, and because Defendant is authorized to
3 conduct business in this District, has intentionally availed itself of the laws and markets
4 within this District, does substantial business in this District, and is subject to personal
5 jurisdiction in this District.

6 **IV. FACTUAL ALLEGATIONS**

7 **Ring’s Devices and Claims About the Security of Its Devices**

8 23. Ring markets and sells home security devices, including a number of models
9 intended for use inside the home. It claims that its indoor security cameras offer “smart
10 security here, there, everywhere.” Ring promises users that it takes security seriously and
11 will safeguard consumers’ private information.

12 24. Ring’s entire brand is built on the perception that its products increase the
13 safety and security of consumers’ homes. Ring’s stated mission is “to reduce crime in
14 neighborhoods.”¹ Indeed, according to Ring, that mission “drives our team and our strategy
15 throughout every decision.”²

16 Our Mission: To Reduce Crime in
17 Neighborhoods

18
19 This mission drives our team and strategy throughout every decision. It's the statement we live by
20 when we design and engineer not only the products you see today, but the future features and
21 innovations that we will deliver for a long time to come. It also makes the late nights and seemingly
22 impossible tasks more bearable as we know our hard work will create happy customers and make a
positive impact on our homes, our communities, and the world.

23 25. Ring started off as a little-known company called DoorBot, which sold video
24 doorbells intended to make company’s founder, Jamie Siminoff, “feel safer.”³ After raising

25
26
27 ¹ <https://shop.ring.com/pages/about>

² <https://shop.ring.com/pages/about>

³ Kim Wetzel, From Sharks to Shaq: Ring CEO Jamie Siminoff’s Unusual Road to Success, Digital Trends (Sept. 29, 2018), <https://www.digitaltrends.com/home/ring-ceo-jamie-siminoff-unusual-road-to-success/>.

1 several million dollars in 2014, DoorBot relaunched as Ring, selling a sleek, elegant Wi-Fi
2 connected video doorbell system.

3 26. Amazon acquired Ring in 2018 for \$1 billion. The acquisition allowed Ring to
4 expand beyond Wi-Fi doorbells to a full range of Wi-Fi connected home security systems.

5 27. Today, Ring sells a number of home security cameras for use both inside and
6 outside the home. Ring's cameras feature motion-activated sensors; notifications sent to the
7 user's phone, tablet, or PC; and two-way talk features that allow a user to see, hear, and speak
8 to the person on the other side of the lens. Its models include:

- 9 a. Video doorbells;
- 10 b. Indoor security cameras ("Indoor Cams");
- 11 c. Indoor/outdoor security cameras ("Stick Up Cams"); and
- 12 d. Outdoor spotlight and floodlight cameras ("Spotlight Cams").

13 28. Ring also markets and sells other home security devices, including motion-
14 sensor-activated outdoor lighting and home alarm systems.

15 29. Ring's indoor cameras operate through users' Wi-Fi networks. Once
16 connected, users can view the video stream and operate the two-way talk feature.

17 30. Ring's claims that it deters or reduces crime have helped Ring cultivate a
18 surveillance network round the country, assisted by dozens of taxpayer-funded camera
19 discount programs and over 600 police partnerships.⁴

20 31. On its website, Ring boasts that it has worked with the National Center for
21 Missing and Exploited Children to reunite missing children with their families⁵ and worked
22
23


24
25 ⁴ Caroline Haskins, How Ring Went from Shark Tank Reject to One of America's Scariest
26 Surveillance Companies, Slate (Dec. 3, 2019),
[https://www.vice.com/en_us/article/zmjp53/how-ring-went-from-shark-tank-reject-to-
americas-scariest-surveillance-company](https://www.vice.com/en_us/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company).

27 ⁵ Eric Kuhn, Ring and the National Center for Missing & Exploited Children Come
28 Together to Bring Missing Kids Home, Ring (Dec. 18, 2019),
[https://blog.ring.com/2019/12/18/ring-and-the-national-center-for-missing-and-
exploited-children-come-together-to-bring-home-missing-kids/](https://blog.ring.com/2019/12/18/ring-and-the-national-center-for-missing-and-exploited-children-come-together-to-bring-home-missing-kids/).

1 with law enforcement and communities to “achieve amazing results” like “getting stolen guns
2 off the streets” and “helping families keep their children safe.”⁶

3 32. Ring’s marketing and sales materials are infused with the idea that installing a
4 Ring product in one’s home will make the home safer. Ring provides the comforting message
5 that its products are watching over American families.

6 33. For example, an advertisement for Ring’s “Indoor Cams” invites users to “start
7 protecting your home, and family, with a small, sleek, and discreet Indoor Cam by Ring.”⁷
8 Ring claims that the “Indoor Cam” allows users to “bring security indoors” to achieve “piece
9 of mind”⁸:

10 

11 **Indoor Cam**

12 \$59.99

13 Bring security indoors with a compact
14 camera that lets you check in on home
15 at anytime. Plug it into standard outlets
16 for nonstop power and peace of mind.



25 ⁶ Jamie Siminoff, Building Better Communities Together: How Ring Connects
26 Communities and Law Enforcement Through the Neighbors App, Ring (Aug. 2, 2019),
27 <https://blog.ring.com/2019/08/02/building-better-communities-together/> .

28 ⁷ The All-New Indoor Ring Cam,
https://www.youtube.com/channel/UCSDG3Moe2mGX9_qtHEtzj2Q.

⁸ <https://shop.ring.com/collections/security-cams/products/mini-indoor-security-camera>.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

34. Ring also claims that the Indoor Cam allows users to “bring protection inside”:

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.

35. Similarly, Ring claims that the Stick Up Cam lets users “add security anywhere they need it”⁹:

Indoor/Outdoor Camera

Add security anywhere you need it – inside or out – with the flexible Stick Up Cam. Featuring several power choices and countless placement options, our most versatile camera gives you endless possibilities.



Stick Up Cam

Shop Now

⁹ <https://shop.ring.com/pages/security-cameras>

1 36. Ring invites users to “add security anywhere you need it,” “protect your home,”
2 and “watch over home” with the Stick Up Cam:

3

4

5

6

7

8

9

10

11

12

13

14

15

16

Product Name	Price	Description
Stick Up Cam Battery	\$99.99	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.
Stick Up Cam Plug-In	\$99.99	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.
Stick Up Cam Solar	\$148.99	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.

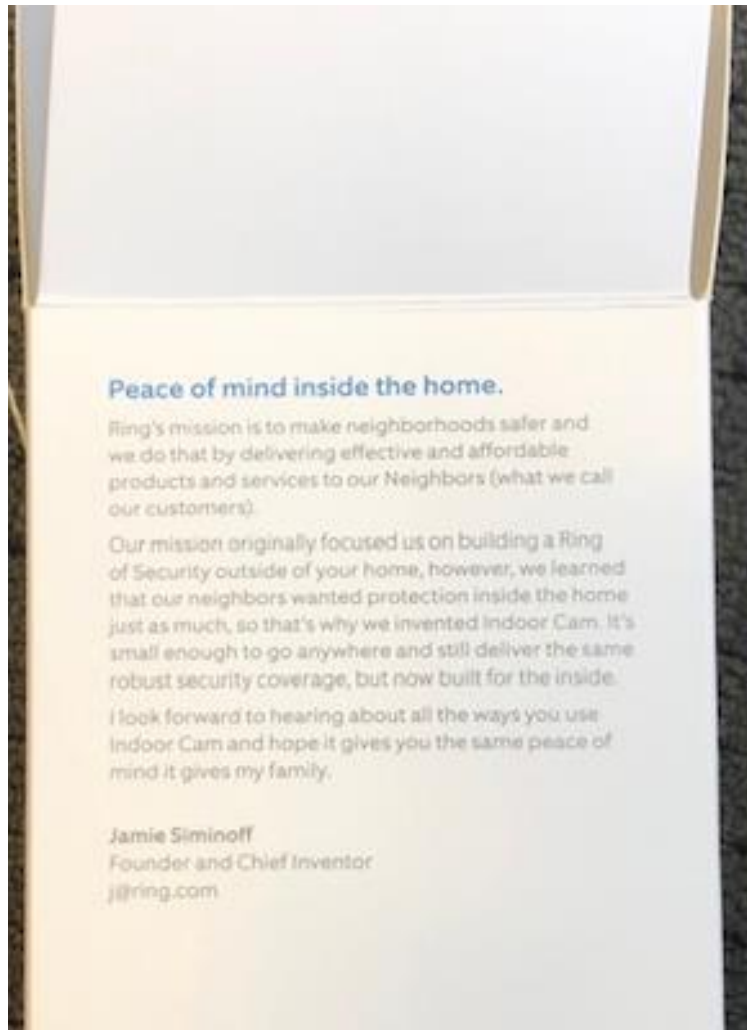
17

18 37. Even Ring’s packaging sends the message that Ring is synonymous with
19 security, stating on the outside of the box: “**Peace of mind inside the home.** Ring’s
20 mission is to make neighborhood safer and we do that by delivering effective and affordable
21 products and services to our Neighbors (what we call our customers). Our mission originally
22 focused on us building a Ring of Security outside your home, however, we learned that our
23 neighbors wanted protection inside the home just as much, so that’s why we invented Indoor
24 Cam. It’s small enough to go anywhere and still deliver the same robust security coverage,
25 but now built for the inside. I look forward to hearing about all the ways you use Indoor Cam
26 and hope it gives you the same peace of mind it gives my family.”

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Ring actually offers poor security and easy access for hackers

38. But in contrast to its public promises, Ring has failed to implement even basic cybersecurity protections to guard their customers' devices from unwanted access and intrusion by third parties.

39. Ring's indoor security cameras use Wi-Fi connections to connect to users' smartphones and tablets via users' Ring accounts and deliver their camera feeds.

40. When a user sets up one of Ring's indoor security cameras, the Ring website prompts the user to download the Ring app and create a username and password. The username and password is linked to the user's device and grants access to the security camera feed.

1 41. If a Ring user chooses to subscribe to one of its plans, they use the same
2 username and password for their subscription plan. But a user does not need to subscribe to
3 a plan to create a Ring account and access the devices via their smartphone or tablet.

4 42. Unlike other companies that use online accounts, Ring does not require basic,
5 industry-standard measures to protect the security of users' accounts.

6 43. For example, two-factor (or dual factor) authentication is a common, industry-
7 standard security feature in which the user provides two different authentication factors to
8 verify themselves to better protect the user's credentials. Two-factor authentication provides
9 higher security than single-factor authentication, in which a user can provide only a
10 password to access an account. Although Ring offers two-factor authentication, it does not
11 require it. And new Ring users are not prompted to enable two-factor authentication at the
12 time they create an account—virtually assuring that the vast majority of users will never
13 enable it.

14 44. Additionally, Ring does not have security protocols in place to notify users
15 when someone logs into their account from a new device or an unrecognized IP address.
16 Whereas most companies request confirmation from the accountholder before allowing a
17 suspicious sign-in to occur, Ring lets it happen no questions asked.

18 45. Ring also does not provide users with a way to see how many users are
19 currently logged in, which could identify whether an unknown party is logged in and
20 watching a user's camera feed. In fact, Ring does not check for concurrent sessions, such as
21 monitoring whether a user is simultaneously logged in from two places at once. Ring also
22 does not provide users with a list of previous login attempts, making it difficult—if not
23 impossible—to tell whether an unauthorized user has accessed a user's account.

24 46. Recently, security professionals from the website Motherboard tested Ring's
25 security procedures.¹⁰ The testers logged into the Ring app from the United States, United
26

27
28 ¹⁰ Joseph Cox, We Tested Ring's Security. It's Awful, Vice (Dec. 17, 2019),
https://www.vice.com/en_us/article/epg4xm/amazon-ring-camera-security.

1 Kingdom, Spain, and Singapore, in some cases simultaneously and from various devices and
2 browsers that had never been used to log into the platform before. At no point did Ring
3 trigger any alert, such as an email notification or text message, to the accountholder to alert
4 them of suspicious logins or check whether the logins were legitimate.

5 47. This is in stark contrast to the protections used by other internet-based
6 companies, even those not in the business of security. For example, social media companies
7 like Twitter, Facebook, and Instagram, email providers like Yahoo! and Gmail, and even
8 streaming services such as Netflix notify accountholders when they detect a suspicious login
9 attempt, or any login attempt, from a new browser, location, or device.

10 48. Ring also offers no protection against repeated, automated attempts to login
11 to its services. It is well known across the industry that hackers can use software to rapidly
12 check whether email and password combinations will grant access to a Ring account.
13 Hackers typically use lists of already compromised combinations from other services.
14 Standard security measures would include a procedure for preventing someone from using
15 software to rapidly check these account combinations after too many incorrect requests to
16 login, by, for example, temporarily blocking access; marking their IP address as suspicious;
17 or presenting a captcha check to ensure that the user is a human rather than an automated
18 program. But Ring does not offer these standard measures.

19 49. Ring also offers no protection against repeated attempts to try new password
20 combinations with known email addresses, sometimes called “brute force entry.” It is well
21 known across the industry that hackers can use bots or other software to rapidly enter
22 combinations of letters, numbers, and symbols into the password field, essentially guessing
23 at an endless string of attempted passwords. Most online accounts will lockout a user after
24 three to five incorrect password attempts. But Ring allows hackers (and hacker software) to
25 try as many passwords as they want without locking them out.

26 50. According to a December 18, 2019, article by *Newsweek* entitled “WHY RING
27 SECURITY CAMERAS ARE SO EASY TO HACK”— password-cracking software used to
28 break into Ring user accounts was offered for sale on a crime forum for just \$6.00. According

1 to the article, a source claiming to have knowledge of the Ring hacks told *Newsweek* that
2 accounts were accessed by a “very basic attack” known as credential stuffing, a brute force
3 method that tries to access an account using a list of compromised login details. The source
4 stated that, “The amount of accounts that are exposed [is] insane. The purpose of Ring is to
5 have security but they leave all their users exposed.”¹¹

6 51. On a desktop web browser, someone who is logged in can watch historical,
7 archived footage, meaning that if a hacker gains access to a user’s account, the hacker can
8 watch live and historical footage of a family inside their home without providing any
9 additional identity verification.

10 52. Despite this, Ring does not offer any way to alert a user via his or her mobile
11 phone or tablet of a suspicious login via an untrusted web browser.

12 53. Ring’s security failures are contrary to its public representations regarding
13 security and constitutes a breach of the duty that Ring owes its customers. Ring persuaded
14 its customers to install its products inside their homes by promising security, protection, and
15 peace of mind. Ring asks its customers to trust Ring with the safety of themselves and their
16 families, in their most intimate spaces. By failing to adequately safeguard access to users’
17 Ring accounts, Ring violated the duty it owes its customers to keep that private information
18 secure.

19 **Hacks of Ring’s indoor security cameras**

20 54. In just the last several weeks, dozens of news outlets have reported multiple
21 instances of hackers gaining unauthorized access to Ring’s indoor security cameras. Hackers
22 have been recorded spying on and harassing homeowners via their Ring indoor cameras.

23 55. In Brookhaven, Georgia, a stranger hacked into a family’s Ring camera and
24 harassed a woman while she lay in bed.¹²

25 _____
26
27 ¹¹ Jason Murdock, WHY RING SECURITY CAMERAS ARE SO EASY TO HACK, *Newsweek*
(Dec. 18, 2019), [https://www.newsweek.com/ring-amazon-cameras-cybersecurity-
passwords-easy-hacking-internet-connected-1477442](https://www.newsweek.com/ring-amazon-cameras-cybersecurity-passwords-easy-hacking-internet-connected-1477442).

28 ¹² Michael Seidan, “I can see you in bed. Wake up!” Woman says stranger hacked Ring
camera, WSB-2 Atlanta (Dec. 11, 2019), <https://www.wsbtv.com/news/local/dekalb->

1 56. In Chesterfield, Virginia, a hacker took over a family’s Ring camera, accessed
2 her live camera, and spoke to her six-year-old daughter.¹³

3 57. A family in Michigan was interrupted while watching TV by a hacker who took
4 over the Ring camera in their living room.¹⁴

5 58. A California woman reported that a hacker took over the Ring security camera
6 in her bedroom and set off her home alarm system.¹⁵

7 59. A hacker began speaking to a family in Wichita, Kansas, through their indoor
8 security camera while they were preparing dinner. He even went so far as to send a pizza to
9 the family’s home.¹⁶

10 60. A hacker demanded that a Waterbury, Connecticut woman “come here” while
11 he hacked into multiple cameras in multiple rooms.¹⁷

12 61. A family in Cape Coral was taunted with racial slurs by a hacker who accessed
13 their Ring indoor camera, including asking whether the family’s interracial son was a
14 “baboon.”¹⁸

15
16
17
18
19 [county/-wake-up-woman-says-someone-hacked-surveillance-system-yelled-at-her-dog/1017442073/.](#)

20 ¹³ Ezo Domingo, Hacker talks to Chesterfield family through Ring doorbell, NBC 12 (Dec.
21 12, 2019), [https://www.nbc12.com/2019/12/12/hacker-talks-chesterfield-family-through-ring-doorbell/.](https://www.nbc12.com/2019/12/12/hacker-talks-chesterfield-family-through-ring-doorbell/)

22 ¹⁴ Michigan family harassed by Ring hacker, Erie News Now (Dec. 12, 2019),
23 [https://www.erienewsnw.com/story/41446500/michigan-family-harassed-by-ring-hacker.](https://www.erienewsnw.com/story/41446500/michigan-family-harassed-by-ring-hacker)

24 ¹⁵ Allison Matyus, Man hacks Ring camera in woman’s home to make explicit comments,
25 Digital Trends (Dec. 17, 2019), [https://www.digitaltrends.com/home/man-hacks-ring-camera-in-womans-home-to-make-explicit-comments/.](https://www.digitaltrends.com/home/man-hacks-ring-camera-in-womans-home-to-make-explicit-comments/)

26 ¹⁶ Caught on camera: Ring cameras hacked across the country, including Wichita, KWCH12
27 (Dec. 12, 2019), [https://www.kwch.com/content/news/Ring-camera-hacks-raise-alarms-across-US-566153241.html.](https://www.kwch.com/content/news/Ring-camera-hacks-raise-alarms-across-US-566153241.html)

28 ¹⁷ “Come Here!” Woman woken up by Ring camera hacker yelling at her, KRON 4 (Dec. 13,
29 2019), [https://www.kron4.com/video/come-here-woman-woken-up-by-ring-camera-hacker-yelling-at-her/.](https://www.kron4.com/video/come-here-woman-woken-up-by-ring-camera-hacker-yelling-at-her/)

¹⁸ Cristina Mendez, Stranger spews racial slurs over family’s hacked Ring camera, NBC-2
(Dec. 11, 2019), [https://www.nbc-2.com/story/41428183/stranger-spews-racial-slurs-over-familys-hacked-ring-camera.](https://www.nbc-2.com/story/41428183/stranger-spews-racial-slurs-over-familys-hacked-ring-camera)

1 62. In New York, a hacker terrorized a 13-year-old boy by following him from
2 camera to camera throughout his home.¹⁹

3 63. Another family in Texas was harassed by a hacker who shouted profanities and
4 racial slurs at their children.²⁰

5 64. Some of the unauthorized hacks were further publicized via the podcast
6 NulledCast. NulledCast streams on Discord, a widely-used Voice over Internet Protocol
7 (VoIP) application (an application that allows users to make voice calls using an internet
8 connection) and digital distribution platform that is designed to allow video gaming
9 communities to livestream games and chat while gaming.

10 65. On the NulledCast, hackers take over peoples' Ring and Nest smart-home
11 cameras, then use the two-way talk feature to harass their unsuspecting owners.

12 66. For example, in one episode, a hacker who called himself "Chance" blared
13 noises and shouted racist comments at a Florida family.²¹

14 67. The NulledCast advertises itself as "over 45 minutes of entertainment,"
15 including Ring "trolling."

16 68. Hackers share software for hacking Ring cameras widely on the internet,
17 including a program that churns through previously compromised email addresses and
18 passwords to break into Ring cameras.

19 **Ring offers inadequate and seemingly false excuses**

20 69. In response to the numerous hacking incidents across the country, Ring has
21 not taken responsibility, apologized, or outlined any measures it is taking to fix its security
22 deficiencies. Instead, it has placed fault on the victims for its own deficient security features.

23 _____
24
25 ¹⁹ Staten Island Family's Ring Camera Hacked, CBS News NY (Dec, 14, 2019),
<https://newyork.cbslocal.com/video/4236747-staten-island-familys-ring-camera-hacked/>.

26 ²⁰ Erin Jones, North Texas Family Furious After Ring Camera Hacker Terrorizes Their
27 Children (Dec. 13, 2019), <https://texasbreakingnews.com/breaking/texas-family-furious-ring-camera-hacker-terrorizes-children/>.

28 ²¹ Joseph Cox and Jason Koebler, Inside the Podcast that Hacks Ring Users Live on Air,
Vice (Dec.12, 2019), https://www.vice.com/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast.

1 For example, in response to an onslaught of news stories regarding the recent hacks, a Ring
2 spokesperson stated, “Our security team has investigated this incident and we have no
3 evidence of an unauthorized intrusion or compromise of Ring’s systems of network. It is not
4 uncommon for bad actors to harvest data from other company’s data breaches and create
5 lists like this so that other bad actors can attempt to gain access to other services.” Ring also
6 stated that it was “made aware of an incident where malicious actors obtained some Ring
7 users’ account credentials (e.g., user name and password) from a separate, external, non-
8 Ring service and reused them to log in to some Ring accounts. Unfortunately, when people
9 reuse the same username and password on multiple services, it’s possible for bad actors to
10 gain access to many account.”

11 70. In other words, according to Ring, the hacked cameras were accessed when
12 unauthorized individuals were able to use a login and password combination that it obtained
13 from somewhere else. But Ring’s excuses fail to recognize that Ring’s own products are not
14 designed in a manner that would prevent such hacks, even though it could have easily
15 implemented security features designed to do just that.

16 71. Additionally, in contrast to Ring’s claims that it had not suffered any security
17 breaches, in fact, it was recently reported that thousands of Ring users’ credentials were
18 stolen and reposted to the internet.²² Security professionals told *Buzzfeed News* that the
19 format of the leaked data suggests it was stolen from a company database. This is just
20 another example of Ring’s apathetic approach to data security and failure to protect its
21 customers’ privacy.

22
23
24
25 ²² Carolyn Haskins, A Data Leak Exposed the Personal Information of Over 3,000 Ring
26 Users, *Buzzfeed News* (Dec. 19, 2019),
27 [https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-
data-over-3000-ring-camera-
users?utm_source=twitter&utm_campaign=tw_wirecutter&utm_medium=social](https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users?utm_source=twitter&utm_campaign=tw_wirecutter&utm_medium=social). See also
28 Aaron Mak, There Sure Have Been a Lot of Reasons Not to Buy a Ring Device Recently,
Slate (Dec. 20, 2019), [https://slate.com/technology/2019/12/all-of-the-hacks-and-data-
leaks-afflicting-ring-doorbells.html](https://slate.com/technology/2019/12/all-of-the-hacks-and-data-leaks-afflicting-ring-doorbells.html).

1 **V. NAMED PLAINTIFFS' ALLEGATIONS**

2 **Plaintiffs Ashley LeMay and Dylan Blakeley**

3 72. Plaintiffs Ashley LeMay and Dylan Blakeley are a married couple residing in
4 Nesbit, Mississippi.

5 73. Ms. LeMay works the overnight shift as a medical laboratory scientist at a
6 hospital near her home. She initially began researching indoor security cameras because her
7 four-year-old daughter has a history of seizures. The Blakeleys wanted a way for Ms. LeMay
8 to check on her daughter in case she began to have seizures during the night while Ms. LeMay
9 was at work and Mr. Blakeley was asleep.

10 74. Several of Ms. LeMay's neighbors have Ring doorbell cameras, so Ms. LeMay
11 began to research the company. She ultimately purchased a two-pack of Ring Indoor Cams
12 on November 29, 2019, from Target, as part of a Black Friday sale.

13 75. The Blakeleys installed one of the cameras in the upstairs bedroom where three
14 of their daughters sleep. They installed the second camera in the downstairs bedroom where
15 their fourth daughter, the baby, sleeps. Ms. LeMay created a Ring account username and
16 password. Ring did not prompt her to enable two-factor authentication. Mr. Blakeley also
17 created a Ring account username and password. Ring did not prompt Mr. Blakeley to enable
18 two-factor authentication for his account username and password either.

19 76. For four days, the Blakeleys believed that they had made the right decision by
20 purchasing Ring indoor security cameras. They felt safe knowing that if their daughter began
21 to experience a seizure—or, worse, if there were an intruder—the motion-activated security
22 camera would alert them. When Ms. LeMay went out, the girls would gather in front of the
23 camera to wave at her and say, "Good night Mommy! We love you!"

24 77. All that changed on December 4, 2019. Shortly after 8 p.m., both of the
25 Blakeleys' cameras began live-streaming, and the Tiny Tim cover of "Tiptoe Through the
26 Tulips," a song that appeared in a scene from the 2020 horror film "Insidious," began to play
27 through the two-way talk feature. At the time, Ms. LeMay was out running errands, but Mr.
28 Blakeley was at home with their children.

1 78. Intrigued by the music, the Blakeleys' eight-year-old daughter, A., went to the
2 room she shares with two of her younger sisters to investigate. But the room was empty. A.
3 wandered the room, looking for the source of the music, the song abruptly stopped, and a
4 man's voice rang out: "Hello there."

5 79. A hacker had gained unauthorized access to the Blakeleys' device. He was able
6 to do so because Ring does not utilize ordinary, basic security precautions to secure their
7 users' accounts.

8 80. The hacker could see, hear, and speak to eight-year-old A. He began to shout
9 racial slurs at A., who is white: "N****r! N****r! N****r!" He shouted, "You're a n****r!" and
10 instructed A. to "go tell Mommy you're a n****r!"

11 81. A., confused, asked, "Who is that?" The man responded: "I'm your best friend.
12 I'm Santa Claus. Don't you want to be my best friend?" He told A. that she could do "whatever
13 you want... Mess up your room, break your TV."

14 82. At one point, A. screamed in distress, "Mommy!"

15 83. Finally, A., terrified, left the room to tell her father that someone was "being
16 weird upstairs." At that point, Mr. Blakeley entered the room and disabled the device.

17 84. The Blakeleys changed their passwords immediately, and Ms. LeMay called
18 Ring that day to report that her indoor security camera had been hacked. A Ring
19 representative told her that Ring would look into it. But Ms. LeMay did not receive a
20 response at first.

21 85. The Blakeleys left for a pre-planned cruise. When they returned on December
22 9, they still had not heard back from Ring. Ms. LeMay emailed Ring customer support
23 approximately three more times, then called them again. A representative informed her
24 dismissively that "we have people who are paid to talk about that," and opined that the issue
25 had "probably" been taken care of when Ms. LeMay changed her password. Of course, the
26 issue had *not* been taken care of, because no one had provided any information about why
27 or how this horrific intrusion had occurred or confirmed that it could not happen again.
28

1 86. The representative transferred Ms. LeMay's call to another representative who
2 refused to answer the Blakeleys' questions. He would not tell her whether Ring knew the
3 identity of the hacker, whether a breach of Ring's security could have permitted the hack, or
4 whether Ring had experienced a data breach itself. He would not tell her whether the hacker
5 appeared to be local or far away.

6 87. To this day, Ring has not disclosed the identity of this unknown hacker to the
7 Blakeleys, who have no way of knowing the motives of the digital intruder or whether he
8 could come to their home in person and threaten the physical safety of their family.

9 88. Ring also has not disclosed how the hacker was able to gain access to the
10 Blakeleys' devices. Ring blamed the Blakeleys for failing to enable two-factor authentication.
11 But Ring did not even prompt the Blakeleys to enable two-factor authentication when they
12 set up their accounts, and even if they had enabled it, it would not necessarily have prevented
13 the hacker from accessing their devices.

14 89. Since then, the Blakeleys have been unable to use their indoor security cameras
15 out of fear they will be hacked again. They have also suffered emotional distress, including
16 fear and anxiety. Ms. LeMay has had to take a leave of absence from work because of the
17 emotional distress this incident caused her.

18 90. While the precise mechanics of the hack are known only to the hacker and to
19 Ring, it is clear the hacker was able to access the Blakeleys' account because Ring did not
20 adopt industry-standard security procedures designed to prevent such access.

21 91. The Blakeleys relied on Ring's representations that it offers security and
22 protection to users and their families and homes. Because of Ring's promises about the level
23 of security offered by their products and services, the Blakeleys purchased the Ring indoor
24 security cameras and installed them in their home.

25 92. The Blakeleys had a special relationship with Ring. Ring provided services to
26 the Blakeleys, including the ability to monitor their indoor security cameras via their Ring
27 account. The transaction between Ring and the Blakeleys was intended to benefit the
28

1 Blakeleys by providing them the ability to use the indoor cameras for all of the purposes they
2 expected and which were intended by Ring.

3 93. It was entirely foreseeable to Ring that the Blakeleys would be harmed if Ring
4 failed to adequately safeguard access to their Ring accounts and security cameras.

5 94. There is a close connection between Ring's failure to adequately safeguard
6 access to the Blakeleys' Ring account and the injuries suffered by the Blakeleys. But for Ring's
7 acts and omissions in maintaining deficient and inadequately-protected systems, and
8 allowing hackers to gain access to customer accounts, the Blakeleys' devices would not have
9 been taken over, their home spied on, and their family harassed. They would not have been
10 exposed to an imminent risk of theft or fraud. This close connection is further reinforced by
11 the broader general evidence of other Ring hacks occurring around the same time period as
12 the hack of their devices.

13 95. Ring's conduct also involves moral blame. Ring markets its products as
14 providing safety and security despite knowing that its security protocols are insufficient to
15 protect its customers' privacy.

16 96. Ring owed the Blakeleys a duty to exercise reasonable care in safeguarding and
17 protecting access to their Ring accounts and keeping them from being compromised, lost,
18 stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other
19 things, designing, maintaining, and testing security systems to ensure that users' account
20 information is adequately secured and protected. Ring breached that duty by failing to adopt,
21 implement, and maintain adequate security measures.

22 97. The injuries to the Blakeleys were reasonably foreseeable as a result of Ring's
23 failure to exercise reasonable care in safeguarding their account information.

24 98. Had they known the truth about Ring's substandard data security practices,
25 the Blakeleys would not have purchased products from Ring or would have paid substantially
26 less, and they would not have installed them in their home, created Ring accounts, and used
27 their Ring devices.

28

1 99. If the Blakeleys could be certain that Ring would implement security measures
2 to protect their Ring accounts and devices from intrusion, they would continue to use their
3 accounts and devices going forward.

4 **Plaintiffs Todd Craig and Tania Amador**

5 100. Plaintiffs Todd Craig and Tania Amador reside together in Texas. Mr. Craig
6 maintained a home security system through ADT for years. But when he learned that he
7 could go from paying approximately \$100 per month for ADT to just over \$100 per year for
8 Ring, he decided to make the switch.

9 101. In December of 2018, Mr. Craig installed a Ring camera doorbell. A few
10 months later, in the spring of 2019, he decided to expand his surveillance system. Mr. Craig
11 purchased a Ring Stick Up Cam security camera from Amazon for use in the home that he
12 and Ms. Amador share. He installed it in their living room and kitchen area. Mr. Craig also
13 purchased and installed two outdoor cameras and an alarm system from Ring.

14 102. Based on Ring's representations about the safety and security it offers, and its
15 commitment to protecting its users, Mr. Craig purchased these devices and installed them,
16 and Ms. Amador agreed to the installation and use of the indoor cameras in the home that
17 they share.

18 103. Mr. Craig works in the information technology industry and his ordinary
19 practice is to create unique sixteen-character passwords for each one of his accounts, which
20 he did when he created his Ring account. The Ring website notified Mr. Craig that his
21 password was "very strong."

22 104. Ms. Amador also created a Ring account so that she could access their indoor
23 security cameras. Her password was a unique fourteen-character password that she did not
24 use with other accounts. The Ring website also notified Ms. Amador that her password was
25 "very strong."

26 105. On approximately December 9, 2019, the couple's sense of safety and security
27 was shattered when a hacker intruded into their Ring security system. A loud voice began
28

1 shouting inside the home, “Ring support! Ring support! I would like to notify you that your
2 account has been terminated by a hacker!”

3 106. Ms. Amador was napping at the time, and was awakened by the noise. Mr.
4 Craig was standing in front of his indoor camera at the time of the breach, and jumped at the
5 sound.

6 107. A stranger had hacked the couple’s Ring system and was spying on the inside
7 of their home.

8 108. The hacker blared sirens through the Ring cameras. He threatened, “Pay this
9 50 bitcoin ransom or you will get terminated yourself!”

10 109. When Mr. Craig heard Ms. Amador crying out for him, he initially thought she
11 was joking. But when he heard the threatening voice of the stranger, he realized the intrusion
12 was real.

13 110. Mr. Craig hid behind a kitchen pillar to listen to what the hacker was saying.
14 After the hacker stopped talking, Mr. Craig pulled the battery out of the camera to disable
15 the device.

16 111. The hacker then accessed the couple’s doorbell camera and told them, “I’m
17 outside your front door.”

18 112. Mr. Craig contacted Ring that day. The representative that he spoke to told him
19 that an unauthorized person had accessed his security cameras through Ms. Amador’s
20 account.

21 113. After Mr. Craig spoke with the first Ring representative, another Ring
22 representative sent him an email addressed to the wrong person. The email stated that
23 someone would reach out in three days.

24 114. Mr. Craig called Ring again the following day and demanded to speak with
25 someone from Ring’s security department. He ultimately connected with Kevin Zenteno,
26 who said only that Ring would not provide Mr. Craig with a log of the unauthorized access
27 and would not confirm that it had been Ms. Amador’s account that was used. He promised
28

1 to provide Mr. Craig with information that Mr. Craig could share with law enforcement, but
2 never provided such information.

3 115. When Mr. Craig saw that Ring was issuing public statements blaming its
4 customers for failing to enable two-factor authentication, he asked Ring to provide an
5 explanation for how his cameras were accessed, given that he and Ms. Amador had each
6 created unique passwords. Ring responded that while it believed that *some* accounts had
7 been accessed because hackers had re-used already-compromised information from another
8 source, Ring was still investigating.

9 116. Ring still has not disclosed the identity of the hacker who threatened Mr. Craig
10 and Ms. Amador. Nor has Ring confirmed how the unauthorized access occurred or whose
11 account the hacker was able to access.

12 117. Since then, Mr. Craig and Ms. Amador has been unable to use their indoor
13 security cameras out of fear they will be hacked again. They have both suffered emotional
14 distress, including fear and anxiety, and are looking for an alternative home security
15 solution. Ms. Amador has been having difficulty sleeping, is suffering from nightmares, and
16 is afraid to sleep in the couples' bedroom. She is constantly terrified of being spied on, or
17 worse, by the unknown hacker.

18 118. While the precise mechanics of the hack are known only to the hacker and to
19 Ring, it is clear the hacker was able to access Mr. Craig's and/or Ms. Amador's Ring accounts
20 because Ring did not adopt industry-standard security procedures designed to prevent such
21 access.

22 119. Mr. Craig and Ms. Amador relied on Ring's representations that it offers
23 security and protection to users and their families and homes. Because of Ring's promises
24 about the level of security offered by its products and services, Mr. Craig purchased Ring's
25 whole-home security system, including a camera doorbell, outdoor cameras, smoke alarms,
26 motion sensors, window/door sensors, and an indoor camera, and he and Ms. Amador
27 created Ring accounts and installed the devices in their home.

28

1 120. Mr. Craig and Ms. Amador had a special relationship with Ring. Ring provided
2 services to Mr. Craig and Ms. Amador, including the ability to monitor their indoor security
3 camera via their Ring accounts. The transaction between Ring, on the one hand, and Mr.
4 Craig and Ms. Amador, on the other, was intended to benefit Mr. Craig and Ms. Amador by
5 providing them the ability to use the indoor cameras for all of the purposes they expected
6 and which were intended by Ring.

7 121. It was entirely foreseeable to Ring that Mr. Craig and Ms. Amador would be
8 harmed if Ring failed to adequately safeguard access to their Ring accounts and security
9 cameras.

10 122. There is a close connection between Ring's failure to adequately safeguard
11 access to the Ring accounts of Mr. Craig and Ms. Amador, and the injuries they suffered. But
12 for Ring's acts and omissions in maintaining deficient and inadequately-protected systems,
13 and allowing hackers to gain access to customer accounts, their devices would not have been
14 taken over, their home spied on. They would not have been harassed and exposed to an
15 imminent risk of theft or fraud. This close connection is further reinforced by the broader
16 general evidence of other Ring hacks occurring around the same time period as the hack of
17 their devices.

18 123. Ring's conduct also involves moral blame. Ring markets its products as
19 providing safety and security despite knowing that its security protocols are insufficient to
20 protect its customers' privacy.

21 124. Ring owed Mr. Craig and Ms. Amador a duty to exercise reasonable care in
22 safeguarding and protecting access to their Ring accounts and keeping them from being
23 compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty
24 included, among other things, designing, maintaining, and testing security systems to ensure
25 that users' account information is adequately secured and protected. Ring breached that
26 duty by failing to adopt, implement, and maintain adequate security measures.

27 125. The injury to Mr. Craig and Ms. Amador was reasonably foreseeable as a result
28 of Ring's failure to exercise reasonable care in safeguarding their account information.

1 126. Had he known the truth about Ring’s substandard data security practices, Mr.
2 Craig would not have purchased products from Ring or would have paid substantially less,
3 and he and Ms. Amador would not have installed them in their home, created Ring accounts,
4 and used their Ring devices.

5 127. If Mr. Craig and Ms. Amador could be certain that Ring would implement
6 security measures to protect their Ring accounts and devices from intrusion, they would
7 continue to use their accounts and devices going forward.

8 **VI. CLASS ALLEGATIONS**

9 102. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs, individually and on
10 behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a
11 class action on behalf of the following Classes:

12 **Class:** All persons who purchased an indoor security camera²³ from Ring
13 LLC during the applicable limitations period.

14 **Subclass:** All persons who purchased an indoor security camera from Ring
15 LLC during the applicable limitations period and whose Ring account(s)
16 were accessed by an unauthorized third party.

17 103. Excluded from the Classes are any entities, including Defendant, and
18 Defendant’s officers, agents, and employees. Also excluded from the Classes are counsel for
19 Plaintiffs, the judge assigned to this action, and any member of the judge’s immediate family.

20 104. Members of the Classes are so numerous that joinder is impracticable. While
21 the exact number of class members is unknown to Plaintiffs, it is believed that the Classes
22 are comprised of thousands of members.

23 105. Common questions of law and fact exist as to all members of the Classes. These
24 questions predominate over questions that may affect only individual class members
25 because Defendant has acted on grounds generally applicable to the Classes. Such common
26 and legal factual questions include:

27
28 ²³ “Indoor security camera” means the Indoor Cam, the Stick Up Cam, and the Indoor/Outdoor Camera.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- a. Whether Defendant’s acts and practices complained of herein amount to egregious breaches of social norms;
- b. Whether Defendant violated Plaintiffs’ and Class Members’ privacy rights;
- c. Whether Defendant acted negligently;
- d. Whether Plaintiffs and the Class Members were harmed;
- e. Whether Defendant intruded upon Plaintiffs’ and the Class members’ seclusion;
- f. Whether Defendant and Plaintiffs formed implied contracts;
- g. Whether Defendant breached implied contracts with Plaintiffs and the Class Members;
- h. Whether Defendant’s conduct was unfair;
- i. Whether Defendant’s conduct was fraudulent;
- j. Whether Plaintiffs and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and
- k. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

106. Plaintiffs’ claims are typical of the members of the Classes as all members of the Classes are similarly affected by the Defendant’s actionable conduct. Defendant’s conduct that gave rise to the claims of Plaintiffs and members of the Classes is the same for all members of the Classes.

107. Plaintiffs will fairly and adequately protect the interests of the Classes because they have no interests antagonistic to, or in conflict with, the Classes that Plaintiffs seek to represent. Furthermore, Plaintiffs have retained counsel experienced and competent in the prosecution of complex class action litigation, including data privacy litigation.

108. Class action treatment is a superior method for the fair and efficient adjudication of this controversy, in that, among other things, such treatment will permit a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of

1 evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that
2 numerous individual actions would engender. The benefits of the class mechanism,
3 including providing injured persons or entities with a method for obtaining redress on claims
4 that might not be practicable to pursue individually, substantially outweigh any difficulties
5 that may arise in the management of this class action.

6 109. Plaintiffs know of no difficulty to be encountered in the maintenance of this
7 action that would preclude its maintenance as a class action.

8 110. Defendant has acted or refused to act on grounds generally applicable to the
9 Classes, thereby making appropriate final injunctive relief or corresponding declaratory
10 relief with respect to the Classes as a whole.

11 111. Plaintiffs suffer a substantial and imminent risk of repeated injury in the
12 future.

13 112. California law applies to the claims of all Class Members.

14 113. The State of California has sufficient contacts to Defendant's relevant conduct
15 for California law to be uniformly applied to the claims of the Classes. Application of
16 California law to all relevant Class Member transactions comports with the Due Process
17 Clause given the significant aggregation of contacts between Defendant's conduct and
18 California.

19 114. Ring is headquartered and does substantial business in California.

20 115. A significant percentage of the Class Members are located in, and Ring aimed
21 a significant portion of its unlawful conduct at, California.

22 116. The conduct that forms the basis for each Class Member's claims against Ring
23 emanated from Ring's headquarters in Santa Monica, California, including Ring's
24 misrepresentations and omissions regarding security and decisions to implement
25 substandard security practices as alleged herein.

26 117. California has a greater interest than any other state in applying its law to the
27 claims at issue in this case. California has a very strong interest in preventing its resident
28 corporations from engaging in unfair and deceptive conduct and in ensuring that harm

1 inflicted on resident consumers is redressed. California's interest in preventing unlawful
2 corporate behavior occurring in California substantially outweighs any interest of any other
3 state in denying recovery to its residents injured by an out-of-state defendant or in applying
4 its laws to conduct occurring outside its borders. If other states' laws were applied to Class
5 Members' claims, California's interest in deterring resident corporations from committing
6 unfair and deceptive practices would be impaired.

7 **VII. CLAIMS FOR RELIEF**

8 **COUNT I**
9 **Negligence**
10 **(On behalf of Plaintiffs and the Class)**

11 118. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
12 set forth above as if fully written herein.

13 119. As alleged herein, Plaintiffs and the Class Members enjoy a special relationship
14 with Defendant.

15 120. Defendant provided services to Plaintiffs and the Class Members, including the
16 ability to monitor their indoor security cameras via their Ring accounts. The transactions
17 between Defendant and the Class Members are intended to benefit the Plaintiffs and the
18 Class Members by providing them the ability to use the indoor cameras for all of the purposes
19 they expected and which were intended by Defendant.

20 121. It was entirely foreseeable to Defendant that Plaintiffs and the Class Members
21 would be harmed if it failed to adequately safeguard access to their Ring accounts and
22 security cameras. Failure to protect their Ring accounts and access to their security cameras
23 was likely to result in injury to Plaintiffs and the Class Members because hackers could gain
24 unauthorized access to private information about their lives, spy on them, harass them,
25 threaten them, endanger them, and commit financial fraud or theft using information
26 learned through the unauthorized access.

27 122. There is a close connection between Defendant's failure to adequately
28 safeguard access to the Ring accounts of the Class Members and the injuries suffered by
them. But for Defendant's acts and omissions in maintaining inadequate security, and

1 allowing hackers to gain access to customer accounts, Plaintiffs' devices would not have been
2 taken over, their homes spied on, and loved ones harassed. This close connection is further
3 reinforced by the broader general evidence of hacks occurring around the same time period
4 as the hack of Plaintiffs' devices.

5 123. Defendant's conduct also involves moral blame. Aware of the vulnerability of
6 its customers, and the sensitive nature of the information available to anyone who watches
7 an indoor camera security feed, Defendant has not taken sufficient actions to prevent
8 hackers from gaining unauthorized access.

9 124. Defendant owed Plaintiffs and the Class Members a duty to exercise reasonable
10 care in safeguarding and protecting access to their Ring accounts and keeping them from
11 being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This
12 duty included, among other things, designing, maintaining, and testing security systems to
13 ensure that users' account information is adequately secured and protected. Defendant
14 breached that duty by failing to adopt, implement, and maintain adequate security
15 measures.

16 125. Plaintiffs and the Class Members were harmed by Defendant's failure to
17 exercise reasonable care in safeguarding their account information, and that harm was
18 reasonably foreseeable.

19 **COUNT II**
20 **Violation of California Unfair Competition Law ("UCL")**
21 **(On behalf of Plaintiffs and the Class)**

22 126. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
23 set forth above as if fully written herein.

24 127. Plaintiffs have standing to pursue this cause of action because Plaintiffs
25 suffered injury in fact and lost money as a result of Defendant's misconduct described herein.

26 128. As described herein, Defendant advertised their products and services as
27 enhancing security and safety, but in fact provided products and services that were highly
28 vulnerable to hacking and that worsened the safety and security of Plaintiffs and the Class
Members.

1 129. Plaintiffs would continue using their Ring products and services if they could
2 be assured that Defendant would take adequate security measures to protect the security of
3 their accounts and cameras going forward.

4 130. The UCL defines unfair business competition to include any “unlawful, unfair
5 or fraudulent” act or practice, as well as any “unfair, deceptive, untrue or misleading”
6 advertising. Cal. Bus. & Prof. Code § 17200. Defendant has engaged in business acts and
7 practices that, as alleged above, constitute unfair competition in violation of Business and
8 Professions Code section 17200.

9 131. Defendant’s acts, as described herein, are “fraudulent” because they are likely
10 to deceive the general public.

11 132. Defendant’s business practices, as alleged herein, violate the “unfair” prong of
12 the UCL because they offend an established public policy and are immoral, unethical, and
13 unscrupulous or substantially injurious to consumers.

14 133. The reasons, justifications, or motives that Defendant may offer for the acts
15 and omissions described herein are outweighed by the gravity of harm to the victims. The
16 injuries suffered by Plaintiffs and the Class Members are substantial, and are not outweighed
17 by any countervailing benefits to consumers or competition.

18 134. Defendant’s business practices described herein also violate the UCL because
19 Defendant falsely represented that goods or services have characteristics they do not have,
20 namely, good security; falsely represented that its goods or services are of a particular
21 standard when they are of another; advertised its goods and services with intent not to sell
22 them as advertised; represented that the subject of a transaction was supplied in accordance
23 with a previous representation when it was not; and/or made material omissions regarding
24 the security of Ring’s devices.

25 135. As a result of Defendant’s unfair business practices, Plaintiffs and the Class
26 Members suffered injury.

27 136. If Defendant is permitted to continue to engage in the unfair and fraudulent
28 business practices described above, its conduct will engender further injury, expanding the

1 number of injured members of the public beyond its already large size, and will tend to
2 render any judgment at law, by itself, ineffectual. Under such circumstances, Plaintiffs and
3 the Class have no adequate remedy at law in that Defendant will continue to engage in the
4 wrongful conduct alleged herein, thus engendering a multiplicity of judicial proceedings.
5 Plaintiffs and the Class request and are entitled to injunctive relief, enjoining Defendant
6 from engaging in the unfair and fraudulent acts described herein.

7 137. The basis for Plaintiffs' claims emanated from California, where the primary
8 decisions regarding what security measures to implement (or not) into Ring's devices
9 occurred. Ring affirmatively instructs its users to contact Ring at an address in Santa Monica,
10 California, with questions about "data protection."

11 **COUNT III**
12 **Breach of Implied Contract**
13 **(On behalf of Plaintiffs and the Class)**

14 138. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
15 set forth above as if fully written herein.

16 139. Defendant sold Ring cameras to Plaintiffs and the Class Members. In
17 exchange, Defendant received benefits in the form of monetary payments.

18 140. Defendant has acknowledged these benefits and accepted or retained them.

19 141. Implicit in the exchange of the cameras for the monetary payments is an
20 agreement that Defendant would provide cameras suitable for their purpose—providing
21 home security—and not designed with flaws that render them vulnerable to hacking and
22 therefore inadequate to provide safety and security.

23 142. Without such implied contracts, Plaintiffs and the Class Members would not
24 have paid for and conferred benefits on Defendant, but rather would have chosen an
25 alternative security system that did not present such dire hidden safety risks.

26 143. Plaintiffs and the Class Members fully performed their obligations under their
27 implied contracts with Defendant, but Defendant did not.

28 144. Defendant breached its implied contracts with Plaintiffs and the Class
Members by failing to acknowledge and repair the inherent vulnerabilities in their accounts

1 and cameras. These circumstances are such that it would be inequitable for Defendant to
2 retain the benefits received.

3 145. As a direct and proximate result of Defendant's breach of its implied contracts
4 with Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered and
5 will suffer injury.

6 **COUNT IV**
7 **Unjust Enrichment**
8 **(On behalf of Plaintiffs and the Class)**

9 146. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
10 set forth above as if fully written herein, and to the extent necessary, assert this count in the
11 alternative to their breach of implied contract claim.

12 147. Defendant has profited and benefited from the purchase of its indoor security
13 cameras by Plaintiffs and the Class.

14 148. Defendant has voluntarily accepted and retained these profits and benefits
15 with full knowledge and awareness that, as a result of the misconduct and omissions
16 described herein, Plaintiffs and the Class Members did not receive products of the quality,
17 nature, fitness or value represented by Defendant and that reasonable consumers expected.

18 149. Defendant has been unjustly enriched by its withholding of and retention of
19 these benefits, at the expense of Plaintiffs and the Class Members.

20 150. Equity and justice militate against permitting Defendant to retain these profits
21 and benefits.

22 151. Plaintiffs and the Class Members suffered injury as a direct and proximate
23 result of Defendant's unjust enrichment and seek an order directing Defendant to disgorge
24 these benefits and pay restitution to Plaintiffs and the Class Members.

25 **COUNT V**
26 **Invasion of Privacy (Intrusion Upon Seclusion)**
27 **(On behalf of Plaintiffs and the Subclass)**

28 152. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
set forth above as if fully written herein.

153. Plaintiffs and Subclass members have reasonable expectations of privacy in
their homes.

1 154. Plaintiffs' and Subclass members' privacy interest as described herein is legally
2 protected because they have an interest in precluding the dissemination or misuse of
3 sensitive information and an interest in making intimate personal decisions and conducting
4 personal activities without observation, intrusion, or interference.

5 155. Defendant intruded on Plaintiffs' and the Subclass Members' solitude,
6 seclusion, and private affairs when it allowed their Ring account information to be
7 compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

8 156. Defendant declined to adopt ordinary, commonplace security measures and
9 instead adopted dismal security features that permitted hackers to easily access user
10 accounts. As a result of Defendant's acts, hackers have been able to gain access to Ring users'
11 devices and spy on them inside of their homes.

12 157. This intrusion is highly offensive to a reasonable person. Defendant's actions
13 alleged herein are particularly egregious because it represents that it cares about and
14 prioritizes security, is aware of the vulnerability of their customers, and is aware of the
15 sensitive nature of the information available to anyone who watches an indoor camera
16 security feed, and yet it has done nothing to prevent hackers from gaining unauthorized
17 access and has refused to take responsibility. In fact, Defendant chose to implement security
18 measures that were deficient and made it easy for hackers to obtain access to user accounts.

19 158. Plaintiffs and Subclass Members were harmed by the intrusion into their
20 private affairs as detailed herein.

21 159. Defendant's actions and omissions described herein were a substantial factor
22 in causing the harm suffered by Plaintiffs and Subclass Members.

23 160. As a result of Defendant's actions, Plaintiffs and Subclass Members seek
24 damages, including compensatory, nominal, and punitive damages, in an amount to be
25 determined at trial.

26
27
28

COUNT VI

**Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiffs and the Subclass)**

1
2
3 161. Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 117
4 set forth above as if fully written herein.

5 162. Plaintiffs and Subclass members have reasonable expectations of privacy in
6 their homes.

7 163. Plaintiffs' and Subclass members' privacy interest as described herein is legally
8 protected because they have an interest in precluding the dissemination or misuse of
9 sensitive information and an interest in making intimate personal decisions and conducting
10 personal activities without observation, intrusion, or interference.

11 164. Defendant declined to adopt ordinary, commonplace security measures and
12 instead adopted dismal security features that permitted hackers to easily access user
13 accounts. As a result of Defendant's acts and omissions, hackers have been able to gain access
14 to Ring users' devices and spy on them inside of their homes.

15 165. Thus, Defendant's acts and omissions caused the exposure and publicity of
16 intimate details of Plaintiffs' and the Subclass Members' private lives—matters that are of no
17 concern to the public.

18 166. This intrusion is highly offensive to a reasonable person. Defendant's actions
19 alleged herein are particularly egregious because it represents that it cares about and
20 prioritizes security, is aware of the vulnerability of their customers, and is aware of the
21 sensitive nature of the information available to anyone who watches an indoor camera
22 security feed, yet it has done nothing to prevent hackers from gaining unauthorized access
23 and have refused to take responsibility. In fact, Defendant chose to implement security
24 measures that were deficient and made it easy for hackers to obtain access to user accounts.

25 167. Plaintiffs and Subclass Members were harmed by the public disclosure of their
26 private affairs as detailed herein.

27 168. Defendant's actions described herein were a substantial factor in causing the
28 harm suffered by Plaintiffs and Subclass Members.

1 169. As a result of Defendant's actions, Plaintiffs and Subclass Members seek
2 damages, including compensatory, nominal, and punitive damages, in an amount to be
3 determined at trial.

4
5 **VIII. PRAYER FOR RELIEF**

6 WHEREFORE, Plaintiffs, individually and on behalf of the other Class members,
7 respectfully requests that this Court enter a Judgment:

- 8 (a) Certifying the Classes and appointing Plaintiffs as Class Representatives;
9 (b) Finding that Defendant's conduct was unlawful as alleged herein;
10 (c) Awarding Plaintiffs and the Class Members nominal, actual, compensatory,
11 consequential, and punitive damages;
12 (d) Awarding Plaintiffs and the Class Members statutory damages and penalties,
13 as allowed by law;
14 (e) Awarding Plaintiffs and the Class Members pre-judgment and post-judgment
15 interest;
16 (f) Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs,
17 and expenses; and
18 (g) Granting such other relief as the Court deems just and proper.

19
20 **IX. JURY DEMAND**

21 Plaintiffs demand trial by jury on all counts for which a jury trial is permitted.

22
23 Dated: January 3, 2020

Respectfully submitted,

24 /s/ Hassan A. Zavareei

Hassan A. Zavareei (State Bar No. 181547)

Katherine M. Aizpuru*

TYCKO & ZAVAREEI LLP

1828 L Street NW, Suite 1000

Washington, D.C. 20036

Telephone: (202) 973-0900

Facsimile: (202) 973-0950

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Email: hzavareei@tzlegal.com
kaizpuru@tzlegal.com

Annick M. Persinger (State Bar No. 272996)

TYCKO & ZAVAREEI LLP

1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6807
Facsimile: (202) 973-0950
Email: apersinger@tzlegal.com

Norman E. Siegel*

Barrett J. Vahle*

J. Austin Moore*

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

**pro hac vice applications forthcoming*

Counsel for Plaintiffs and the Class