LAW OFFICE OF
FRANCIS J. FLYNN, JR.
Francis J. "Casey" Flynn, Jr., SBN 304712
422 S. Curson Avenue
Los Angeles, California 90036
Tele: 314-662-2836
Email: casey@lawofficeflynn.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis*
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505
Facsimile: (813) 223-5402
jyanchunis@forthepeople.com

* to seek *pro hac vice* admission

Attorneys for Plaintiff and the putative class

UNITED STATES DISTRICT COURT
CERNTRAL DISTRICT OF CALIFORNIA

JOHN BAKER ORANGE on behalf of himself and all others similarly situated,

Plaintiff

v.

RING LLC and AMAZON.COM, INC.

Defendant.

CASE NO.: 2:19-cv-10899

CLASS ACTION

COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY, AND INJUNCTIVE RELIEF FOR:

(1) NEGLIGENCE
(2) INVASION OF PRIVACY
(3) BREACH OF THE IMPLIED WARRANTY OF MERCHANTABILITY
(4) BREACH OF IMPLIED CONTRACT
(5) UNJUST ENRICHMENT
(6) VIOLATION OF THE UNFAIR COMPETITION

LAW ("UCL") CAL. BUS. PROF. CODE § 17200

DEMAND FOR JURY TRIAL

Plaintiff John Baker Orange ("Plaintiff"), individually, by and through his undersigned counsel, brings this class action lawsuit against Ring LLC and Amazon.com, Inc. (collectively, "Defendants," or "Ring"), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of his counsel as follows:

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because (a) the aggregated claims of putative class members exceeds $5 million, exclusive of interest and costs; (b) there are at least hundreds of putative class members; and (c) at least one of the members of the putative class is a citizen of a different state than Defendants.

2. This Court has personal jurisdiction over Defendants because Defendants, directly or through their agents, conduct business in the State of California and within this District. Specifically, Defendant Ring maintains headquarters in this District and operate in this District. Through their business operations in this District, Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

3. Through its business operations in this District, Defendants intentionally availed themselves of the markets within this District and have sufficient minimum contacts with this State to render the exercise of jurisdiction by this Court just and proper.

4. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this

District and Ring is headquartered in this District.

INTRODUCTION

5. Ring is a security and safety company which manufactures, markets and sells alarms, video doorbells, security systems, and cameras. At its core, Ring's products are designed to promote the safety of its customers and to protect their privacy.

6. Wi-Fi cameras are among Ring's most popular offerings. They are designed to be strategically placed throughout a property, enabling authorized users to see covered areas in high definition and to communicate directly with occupants via a two-way speaker-microphone system.

7. Ring promises its customers "peace of mind" with its Wi-Fi enabled smart security systems. Unfortunately, Ring's cameras fail to deliver on its most basic promise. Lax security standards and protocols render its camera systems vulnerable to cyber-attack. Indeed, over the past several months numerous Ring customers reported that their camera systems had been hacked by malicious third parties who gained access to the video and two-way speaker-microphone system which they used to invade the privacy of customers' homes and terrorize unsuspecting occupants, many of whom are children.

8. While Ring quickly attempted to distance itself from liability by blaming customers for failing to create strong security passwords, it is Ring who failed to provide sufficiently robust security measures such as two-factor authentication and other protocols necessary to maintain the integrity and inviolability of its cameras. As a result of Ring's defective design, and its failure to imbue its Wi-Fi cameras with sufficient security protocols, its customers' most basic privacy rights were violated along with the security and sanctity of their homes.

9. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, invasion of privacy, breach of implied contract, breach of implied

warranty and unjust enrichment. In addition, Plaintiff seeks damages, injunctive and declaratory relief.

PARTIES

10. Plaintiff John Baker Orange is a resident of Jefferson County Alabama. He purchased a Ring outdoor camera for his house in July 2019 for approximately $249.00. The Ring camera was installed over his garage with a view of the driveway. Mr. Orange purchased the Ring camera to provide additional security for him and his family which include his wife and three children aged 7, 9, and 10. Recently, Mr. Orange's children were playing basketball when a voice came on through the camera's two-way speaker system. An unknown person engaged with Mr. Orange's children commenting on their basketball play and encouraging them to get closer to the camera. Once Mr. Orange learned of the incident, he changed the password on the Ring camera and enabled two-factor authentication. Prior to changing his password, Mr. Orange protected his Ring camera with a medium-strong password.

11. Prior to the recent hacking incidents, Mr. Orange was unaware of and believes that Ring did not provide users the ability to secure their systems with two-factor authentication.

12. Defendant Ring LLC is a home security and smart home company that manufactures a range of home security products including Wi-Fi enabled smart cameras. Ring LLC is a wholly owned subsidiary of Amazon.com with its place of business located at 1523 26th St, Santa Monica, California 90404.

13. Defendant Amazon.com Inc. is a Delaware corporation headquartered at 410 Terry Avenue North Seattle, Washington 98109-5210. Ring was acquired by Amazon in February 2018 for an estimated value of between $1.2 billion and $1.8 billion.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class

Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are thousands of putative class members, and at least some of whom have a different citizenship from Defendants.

15. This Court has jurisdiction over the Defendants which operate in this District. Through their business operations in this District, Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and Ring is headquartered in this District.

STATEMENT OF FACTS

A. Ring Products and Wi-Fi Connectivity

17. Ring offers a variety of Wi-Fi enabled security and safety devices, most notably video doorbells and cameras. The Ring video doorbell is the company's flagship product. It is a smart doorbell that contains a high-definition camera, a motion sensor, a microphone and speaker for two-way audio communication. It integrates with an associated mobile app, which allows users to view real-time video from the camera, receive notifications when the doorbell is rung, and communicate with visitors at the door via the integrated speaker.

18. In 2015, Ring released the first of its internal wireless IP cameras. Like the video doorbell, the cameras provide high definition video and microphone-speaker functionality for two-way communication. Since 2015, Ring has expanded its selection to include a range of indoor and outdoor cameras, each with video and two-way audio communication. [1]

19. Ring products are designed to operate through a users' Wi-Fi network.

[1] https://support.ring.com/hc/en-us/sections/360006380112-Indoor-Cam

Once connected, the cameras enable users to see a high definition video stream in the camera's range and listen to and/or communicate with nearby occupants.

20. Creating a Ring account to fully enable the system involves a 4 step process: (1) download the Ring App; (2) Launch the app and click on the Setup Device button; (3) Create an Account at the bottom of the screen; (4) Enter your first and last name, email address and password.

21. Ring cameras are relatively affordable, easy to install, simple to use, and heavily marketed by Amazon, making them one of the best-selling home security and surveillance devices on the market.

22. In addition to their own direct-to-consumer marketing efforts, Ring has signed partnership agreements with hundreds of police departments around the country, many of which have marketed and sold Ring devices on the company's behalf.

23. Ring promises its customers "peace of mind" with "smart security here, there, everywhere."[2]

> At the core of Ring, and guiding every action we take, is respect for the privacy and security of our neighbors (what we call our customers). This includes giving our neighbors effective, easy-to-use and affordable products and services to help protect their homes. It also means taking extremely seriously the privacy, security and control of their devices and personal information. Below you will find Ring's guiding principles.
>
> We know you have many options to choose from so protecting your privacy and data security is a job we take seriously. We know that you place a huge amount of trust in us and we have every intention of continuing to earn that trust.[3]

---

[2] https://shop.ring.com/pages/security-cameras

[3] https://shop.ring.com/pages/privacy

24. Unfortunately, Ring does not fulfill its core promise of providing privacy and security for its customers, as its camera systems are fatally flawed. The Ring system is Wi-Fi enabled, meaning that it will not work without internet connectivity. Once connected, however, any internet device can be seen by the on-line community, making it incumbent upon its manufacturer to design the device such that it can be properly secured for only intended use. This obligation is even more critical in instances where the device, like the Ring camera, is related to the safety and security of person and property.

25. Ring failed to meet this most basic obligation by not ensuring its Wi-Fi enabled cameras were protected against cyber-attack. Notably, Ring only required users enter a basic password and did not offer or did not compel two-factor authentication.

26. Dual factor or two-factor authentication ("2FA") is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. 2FA provides a higher level of assurance than authentication methods that depend on single-factor authentication, in which the user provides only one factor -- typically a password. 2FA adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who have stolen a password database or used phishing campaigns to obtain user passwords.[4]

27. Ring was certainly aware of the infirmity of its cameras and the necessity

[4] https://searchsecurity.techtarget.com/definition/two-factor-authentication

to employ good security practices which included, at a minimum, insistence on robust passwords and dual factor authentication.

B. Hacking Incidents

28. Over the past several weeks, news media has been inundated with reports of hackers gaining unauthorized access to homes across the country via insecure Ring devices. Once in, hackers routinely terrorizing occupants, invade their privacy and undermine their sense of safety and security. While the dramatic nature of these hacking incidents, which involved interactions between the hackers and occupants of the home, many of whom were children, caught the attention of mainstream media, the insecurity of the cameras poses an additional and more looming threat. Hackers who choose not to interact with occupants have gone unnoticed for days, month and even years during which time they spied on occupants and their homes, gathering an array of private which can subsequently be sold and used for a host of nefarious purposes:

(a) Mississippi Incident

Pedophile Hacker Hacked 8yo Girl's Room – Told Her That He Is Santa Claus

> Parents will do anything to keep their child safe. This includes installing a CCTV inside the child's room so that they can monitor their child while at work. However, for a couple in US, this move has caused their 8-year-old daughter to be harassed by a hacker.
>
> The mother, Ashley LeMay told CNN that she installed the camera so that she could make sure that they are OK while she's at the overnight shift but four days after the camera was installed, a hacker managed to get through the system.
>
> From the CCTV footage, it can be seen that their daughter went into her room after hearing song being played from inside her room. Alyssa went on to ask who was playing the song and a voice came through the speaker of the camera. He said, "I'm your best friend.

I'm Santa Claus. Don't you want to be my best friend?"

When the couple's 8-year-old daughter, Alyssa, checked on the music and turned on the lights, a man started speaking to her, repeatedly calling her a racial slur and saying he was Santa Claus. She screamed for her mother. [5]

"She won't even sleep in her room," Ms. LeMay said on Saturday. "She actually spent the night with a friend the other night because she didn't want to be here." "I did a lot of research on these before I got them. You know, I really felt like it was safe,"

A big part of Ring's marketing strategy revolves around making customers feel like their own homes are unsafe, so that they'll turn to surveillance devices to ease those fears. [6]

(b) **Waterbury, Connecticut Incident**

Ed Slaughter told NBC Connecticut last week that he felt "violated" after a hacker started yelling obscenities and woke up his mother-in-law, who had been sleeping in the basement where he had installed a Ring camera. [7]

(c) Cape Coral, Florida Incident

Josefine Brown told NBC 2 that she was frightened by an episode in which a hacker could be heard in footage from a Ring security camera provided to the station asking the interracial couple if their son was a "baboon."

In an email on Sunday, Ms. Brown said: "We are very

---

[5] How Hackers Are Breaking Into Ring Cameras, Vice, December 11, 2009, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras

[6] https://www.worldofbuzz.com/pedophile-hacker-hacked-8yo-girls-room-cctv-in-the-us-told-her-that-he-is-santa-claus/ (December 15, 2019)

[7] Somebody's Watching: Hackers Breach Ring Home Security Cameras, NY Times, December 15, 2019, https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html.

concerned about our safety and privacy because we thought having a security camera will keep us safe. We don't know how long someone has been watching us. It is very scary." *Id.*

(d) Staten Island, New York Incident

Gina Scarlato's 13-year-old son, was terrorized by a hacker who followed the boy from camera to camera throughout the house. [8]

(e) North Texas Incident

"The first thing that they heard was like a siren that went off," said Lue Mayora of Forney. Wednesday night, while Mayora and her husband were coming home from work, someone hacked into their Ring cameras.

They were shouting profanities, racial slurs and threats at their 9-year-old and 11-year-old children who they said ran out of the house in terror.

"I heard real, real screaming and I came out and said what's going on," Mayora's neighbor Johnny Davila said. "They said someone is in house yelling they're going to kill us."

Mayora's neighbor got his gun and ran next door thinking someone was inside the home.

As he heard the voice coming from the camera, he eventually realized it had been hacked.

"It made me so mad that they're targeting our kids," he said. "They don't want to sleep by themselves," Mayora said. "They don't want to be in the house." Mayora has now deactivated her Ring cameras and said she will be getting rid

[8] Staten Island Family's Ring Camera Hacked, CBS News NY, December 14, 2019, https://newyork.cbslocal.com/video/4236747-staten-island-familys-ring-camera-hacked/

of them this weekend.[9]

(f) Georgia Incident

A Georgia woman was given a terrifying wake-up call by a man who hacked into her Ring security camera and began speaking to her in the middle of the night.

The woman was in bed when an unidentified man called to her through the camera, which she and her boyfriend installed to keep an eye on their new puppy, Beau, during working hours.

In footage of the encounter, which a friend of the woman's shared on Twitter, the stranger can be heard clapping, calling to the puppy and telling the woman to "wake up!"

"Hello? Hello? Come here, puppy," he shouts.

"Hello? Hello?" he says after multiple ignored commands. "I can see you in the bed, come on, wake the f*** up."[10]

(g) Texas Incident

Ring hackers demand $350,000 in Bitcoin from Texas Couple

One of the most bizarre recent reports comes from Grand Prairie, Texas, where a couple says they awoke in the middle of the night to an alarm coming from their Ring camera. But that's not all they heard; After the couple came to investigate, a voice over the Ring's built-in speaker claimed that the couple's Ring account had been terminated, and that they themselves would be "terminated" if they didn't fork over a hefty haul of cryptocurrency.

---

[9] North Texas Family Furious After Ring Camera Hacker Terrorizes Their Children, https://texasbreakingnews.com/breaking/texas-family-furious-ring-camera-hacker-terrorizes-children/

[10] Yahoo, December 13, 2019, https://www.yahoo.com/now/woman-horrified-as-stranger-wakes-her-through-ring-security-camera-200838818.html

> The "hackers" demanded a whopping 50 bitcoins. Going by the current conversion rate, that's over $350,000.
>
> * * *
>
> [W]hat makes this whole thing scary is that they also gained control over the home's Ring doorbell. They used their access to the doorbell to spoof their presence outside of the couple's home, making the homeowners believe that someone was actually stalking their property while demanding the ransom.[11]

C. Ring's Response

29. In response to the swath of hacking incidents across the country, Ring said only that it takes the security of its devices seriously, and then proceeded to blame Ring users for the hacking.

> "Our security team has investigated this incident and we have no evidence of an unauthorized intrusion or compromise of Ring's systems or network," the statement said. "Recently, we were made aware of an incident where malicious actors obtained some Ring users' account credentials (e.g., username and password) from a separate, external, non-Ring service and reused them to log in to some Ring accounts."[12]

30. According to Ring, the hacked cameras were accessed when unauthorized third parties were able to login as authentic users with a proper password. Ring places the blame squarely on its customers suggesting these hacks are possible because people are using weak passwords that have previously been

---

[11] Ring hackers demand $350,000 in Bitcoin from Texas couple, but something so simple ruined their plot, BGR, December 12, 2019, https://bgr.com/2019/12/12/ring-hackers-texas-bitcoin-privacy-security/

[12] Somebody's Watching: Hackers Breach Ring Home Security Cameras, NY Times, December 15, 2019

compromised.[13]

31. By so doing, however, Ring ignores the fact that it allows its products – whose very purpose is to provide customers with safety and security – to be setup in a manner that makes it unreasonably susceptible to hacking.

32. Although Ring is in the business of home security and was certainly aware that its Wi-Fi enabled product, was vulnerable to attack, it took no steps to "require camera owners to use two-factor authentication, which could help prevent these types of attacks…"[14] Moreover, it knew, or should have known, in an era of pervasive data breaches, that logging in with user emails instead of unique account names, and not requiring at least 2FA, put its Wi-Fi enabled product at an unreasonable risk of being compromised.

33. Not only was Ring aware that its cameras were inadequately secured, it was also aware of the existence of "online forums where hackers discussed how to break into Ring accounts connected to the cameras." [15]

34. According to *Motherboard*,

> Ring was aware that the hacking community developed dedicated software for breaking into Ring security cameras. [16] Indeed, several posts on different crime forums where hackers discuss creating tools for breaking into the Ring accounts which are connected to cameras.

---

[13] https://www.theguardian.com/technology/2019/dec/13/ring-hackers-reportedly-watching-talking-strangers-in-home-cameras

[14] Hackers are getting really good at hacking Ring cameras and the results are terrifying, Mashable, December 15, 2019, https://mashable.com/article/ring-cameras-easily-hacked-and-its-terrifying/

[15] https://www.theguardian.com/technology/2019/dec/13/ring-hackers-reportedly-watching-talking-strangers-in-home-cameras

[16] How Hackers Are Breaking Into Ring Cameras, Vice, December 11, 2009, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras

> 'Ring Video Doorbell Config,' one thread on a hacking forum reads. A config is a file use to drive special software for rapidly churning through usernames or email addresses and passwords and trying to use them to log into accounts. Hackers have developed configs for a wide variety of websites and online services, from Uber to Facebook.
>
> The thread title adds that the config has a "High CPM," or high "check per minute," meaning it can test if a username and password allows access to a Ring camera quickly. In a different thread, one hacker is offering a Ring.com checker for $6.[17]

35. Sadly, Ring hacking events have become so common place that there is even a podcast dedicated to live and recorded hacking events wherein malevolent third parties take control of Ring devices and terrorize occupants for entertainment.[18] "The NulledCast is a podcast livestreamed to Discord.[19] It's a show in which hackers take over people's Ring and Nest smart home cameras and use their speakers to talk to and harass their unsuspecting owners." [20] "'Sit back and relax to over 45 minutes of

---

[17] How Hackers Are Breaking Into Ring Cameras, Vice, December 11, 2009, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras

[18] Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers-bitcoin-ransom-security.html

[19] Discord is a proprietary freeware voice over internet protocol application and digital distribution platform designed for video gaming communities, that specializes in text, image, video and audio communication between users in a chat channel. As of July 2019, there are over 250 million unique users of the software. https://en.wikipedia.org/wiki/Discord_(software)

[20] Inside the Podcast that Hacks Ring Camera Owners Live on Air, Vice, December 13, 2019, https://www.vice.com/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast.

entertainment,' an advertisement for the podcast posted to a hacking forum called Nulled reads. 'Join us as we go on completely random tangents such as; Ring & Nest Trolling, telling shelter owners we killed a kitten, Nulled drama, and more ridiculous topics. Be sure to join our Discord to watch the shows live.'" [21] As reported in Slashgear:

> Reality [] has taken on a frightening turn for owners of Ring security cameras who suddenly find virtual intruders in their homes, thanks to hackers who break into the security system and live stream their harassment for the entertainment of a few.
>
> The irony is probably lost on no one that the very devices that are supposed to keep homes and their owners safe have become the very vehicle for violations of their privacy. Tools to hack Ring security cameras have unfortunately become widespread enough to become almost common. And to show off their abilities and get a few kicks, some of these hackers have taken to live streaming their activities in bold defiance to authorities. [22]

36. The podcast and other online hacker forums even feature software specifically designed to hack Ring cameras. The software churns through previously compromised email addresses and passwords to break into Ring cameras at scale. *Id.*

37. Despite active knowledge of such forums Ring continued to blame these hacking incidents on poor security practices by users. Ring contends that in each of the hacking incidents, "credentials stolen during a data breach are sold on the black

---

[21] Nulledcast: a podcast where hackers play live audio of themselves breaking into Ring cameras and tormenting their owners, BoingBoing, December 13, 2019, https://boingboing.net/2019/12/13/nulledcast.html

[22] Ring camera hacking has become entertainment for some people, Slashgear, December 12, 2019, https://www.slashgear.com/ring-camera-hacking-has-become-entertainment-for-some-people-12603149/

market and used for hacking into accounts…. Due to the fact that customers often use the same username and password for their various accounts and subscriptions, bad actors often re-use credentials stolen or leaked from one service on other services." Ring's explanation, however, neither eliminates its responsibility, nor accurately attributes the fault. As one hacking victim, Tania Amador, explained, her Ring password is 21 characters long and only used for that account. [23]

38. Moreover, "Ring's status as a maker of home security cameras makes it much more sensitive than most accounts. Ring could probably do more to encourage users to choose strong passwords and set up two-factor authentication. For example, Google-owned Nest recently switches to Google logins, which have industry-leading security features. It also pesters people in the app to configure two-factor if they haven't already."[24]

39. "Additionally, Ring does not alert users of attempted log-in from an unknown IP address, or tell users how many others are logged into an account at one time. Because of this, there is no obvious way to know whether any bad actors have logged into people's compromised Ring accounts without their consent."[25]

40. Ring's failure to employ good security practices in the design and implementation of its camera systems has directly resulted in the unlawful exposure of Plaintiff and Class Members' person and property and has damaged them thereby.

---

[23] Hackers are taking Control of Ring Cameras and using them to taunt both adults and children, Inc., https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers-bitcoin-ransom-security.html

[24] https://www.extremetech.com/internet/303296-hackers-openly-peddle-tools-to-hack-ring-cameras

[25] https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users

D. Plaintiff and Class Members Suffered Damages

41. The ramifications of Defendant's failure to properly secure their cameras and attendant access protocols may be felt for years to come. While the immediate in terrorem effects resulting from unauthorized access may be assuaged by disconnecting the camera, hackers have had access to information derived from those cameras for years, including but not limited to intimate details of household members, work schedules, and property contents. This information can be sold and used for a host of nefarious purposes.

42. The hacking was a direct and proximate result of Ring's failure to: (a) properly secure its camera systems in order to prevent, or at least minimize, the ability of unauthorized third parties to gain access; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of their cameras; and (c) protect against reasonably foreseeable threats to the security or integrity of such cameras.

43. Defendant had the resources necessary to properly secure its cameras but neglected to do so. Had Defendant taken such steps and adopted basic security measures (e.g. 2FA), it would have prevented the intrusions suffered by Plaintiff and Class Members.

44. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from malicious third parties who gained unauthorized access to their homes and highly sensitive details of their lives.

45. As a result of the Defendants' actions, Plaintiff and Class Members have been damages and can no longer trust the integrity of the Ring cameras or believe in security it claims to provide.

CLASS ACTION ALLEGATIONS

46. Plaintiff seeks relief on behalf of herself and as representatives of all

others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons in the United States whose purchased a Ring camera within the applicable statute of limitations periods (the "Class").[26]

47. Excluded from the Class are Ring and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

48. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

49. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

50. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. Ring sells tens of thousands of cameras throughout the United States every year. Ring has physical and/or email addresses for Class Members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

51. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

---

[26] Ring cameras include the Ring Indoor Cam, Stick Up Cam, Spotlight Cam, and Floodlight Cam

a. Whether Ring knew or should have known of the susceptibility of its camera systems to hacking;

b. Whether Ring's security measures to protect their camera systems were reasonable;

c. Whether Ring was negligent in failing to implement reasonable and adequate security procedures and practices;

d. Whether Ring's failure to implement adequate security measures rendered its camera systems subject to hacking;

e. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Ring's failure to reasonably secure its camera systems; and;

f. Whether Plaintiff and Class members are entitled to relief.

52. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a purchaser of a Ring camera. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class. The claims of the Plaintiff and the respective Class are based on the same legal theories and arise from the same unlawful and willful conduct of Defendants, resulting in the same injury to the Plaintiff and the respective Class. Plaintiff and all members of the Class are similarly affected by Defendants' wrongful conduct and were damaged in the same way. Plaintiff's interests coincide with, and are not antagonistic to, those of the other Class members. Plaintiff have been damaged by the same wrongdoing set forth in this Complaint. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

53. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class he seeks to represent; is committed to pursuing this matter against Ring to

obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

54. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Ring, and thus, individual litigation to redress Ring's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

55. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

56. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

57. **Ascertainability.** Finally, all members of the proposed Classes are readily ascertainable. Ring has access to customer names and addresses. Additionally, Ring videos contain hidden geographic coordinates, including latitude and longitude with up to six decimal points of precision.[27] Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE

58. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

59. Defendants had full knowledge of the purpose for which its security cameras were being used and the sensitivity of the people and things the cameras were designed to secure and protect. Defendants also knew the types of harm that Plaintiff and Class Members could and would suffer if the integrity of the cameras were compromised.

60. Defendants had a duty to exercise reasonable care in ensuring their cameras were secure, safe to use and inviolable by unauthorized parties. This duty includes, among other things, ensuring that reasonable and proper protocols and safeguards are in place, so that the Wi-Fi enabled cameras are not easily compromised by unauthorized users.

61. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks of allowing Ring cameras to be set up and used without adequate security protocols and safeguards.

62. Defendants' own actions and inactions created a foreseeable risk of harm

---

[27] *See*, https://www.dailymail.co.uk/news/article-7785293/Sprawling-map-shows-homeowners-Ring-police-access-data.html

to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, its failure to sell cameras with sufficiently robust security protocols to prevent unauthorized users from gaining access to the cameras and to provide users with sufficient instructions and tools to properly secure their Wi-Fi enabled cameras.

63. Plaintiff and the Class Members had no idea Ring cameras were vulnerable to misappropriated and therefore had not ability to properly protect their cameras from unauthorized use.

64. In contrast, Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members and had a duty to do so.

65. Defendants, through their actions, unlawfully breached their duty to Plaintiff and Class Members by failing to ensure their cameras and set up procedures were sufficiently robust to protect against unauthorized use.

66. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' would not have used or purchased a product that is so readily compromised.

67. As a result of Defendants' negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: the cost of replacement cameras; cost of additional surveillance and protective devices and services; time spent monitoring, addressing the current and future consequences of the exposure enabled by Ring; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY

68. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

69. Plaintiff and Class Members had a legitimate expectation of privacy with respect to the people, location and subject matter of what their Ring cameras were

observing and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

70. Defendants owed a duty to their customers, including Plaintiff and Class Members, and the general public to ensure that its cameras and the data they observed and recorded remained confidential and secure.

71. The failure to ensure the cameras had sufficiently robust security features and were accompanied by sufficient security practices is highly offensive to a reasonable person.

72. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members purchased and used Ring cameras with the expectation that people, places and information seen and heard by the camera would be private and would not be subject to disclosure without their authorization.

73. The failure to ensure the camera and its setup features provided adequate security constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

74. Defendants acted with a knowing state of mind when they permitted the cameras to be marketed and sold in such a fashion because they knew their security practices were inadequate.

75. Acting with this knowledge, Defendants had notice and knew that their inadequate security practices would cause injury to Plaintiff and Class Members.

76. As a proximate result of Defendants' acts and omissions, Plaintiff's and Class Members' privacy was violated causing Plaintiff and Class Members to suffer damages.

77. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members.

78. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF THE IMPLIED WARRANTY OF MERCHANTABILITY

79. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

80. Defendants are in the business of manufacturing, designing, supplying, marketing, advertising, warranting, and selling security cameras. Defendants impliedly warranted to Plaintiff and Class Members that the Product was of a certain quality, free from defects, fit for the ordinary purpose of observing and recording events for the purpose of securing property and maintaining safety of its residents.

81. The Ring cameras were and are unfit for ordinary use and not of merchantable quality as warranted by Defendants because the Products are defective in that they are not secure and can easily be hacked by unauthorized third parties. Before purchase, Plaintiff and Class Members could not have readily discovered that the cameras were not merchantable for use to protect their homes and occupants.

82. Defendants have failed to provide adequate remedies under their limited warranty, which have caused that warranty to fail of its essential purpose, thereby permitting remedies under these implied warranties.

83. Defendants had unequal bargaining power and misrepresented the Products' reliability and performance properties, and the limited remedies unreasonably favor Defendants and fail Plaintiff's reasonable expectations for product performance.

84. As a direct and proximate result of the breaches of these implied warranties, Plaintiff and Class Members suffered damages, injuries in fact and

ascertainable losses in an amount to be determined at trial, including repair and replacement costs and damages to other property.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

85. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

86. Defendants sold Ring cameras to Plaintiff and Members of the Class for which they received a benefit in the form of monetary payment.

87. Defendants have acknowledged the benefit and accepted or retained the benefit conferred.

88. Implicit in the agreement between the Defendants and Plaintiff and Class Members was to provide cameras that were suitable for their purpose and not designed with flaws that render them vulnerable to hacking resulting in the compromise of user safety and security.

89. Without such implied contracts, Plaintiff and Class Members would not have paid for and conferred a benefit upon Defendants, but rather chosen one of the numerous alternative cameras that were available to them and which did not present a hidden safety risk.

90. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants, however, Defendants did not.

91. Defendants breached the implied contracts with Plaintiff and Class Members by failing to acknowledge the inherent vulnerability in their cameras. These circumstances are such that it would be inequitable for Defendants to retain the benefit received.

92. As a direct and proximate result of Defendants' breach of their implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: the cost of replacement

cameras; the cost of additional surveillance and protective devices and services; and time spent monitoring, addressing the current and future consequences of the exposure enabled by Ring.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT

93. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

94. As the intended and expected result of their conscious wrongdoing, Defendants have profited and benefited from the purchase of the Product by Plaintiff and the Class.

95. Defendants have voluntarily accepted and retained these profits and benefits, with full knowledge and awareness that, as a result of Defendants' misconduct, Plaintiff and the Class did not receive Product of the quality, nature, fitness, or value that had been represented by Defendants, and that reasonable consumers expected.

96. Defendants have been unjustly enriched by their fraudulent and deceptive withholding of benefits to Plaintiff and the Class at the expense of these parties.

97. Equity and good conscience militate against permitting Defendants to retain these profits and benefits.

As a direct and proximate result of Defendants' unjust enrichment, Plaintiff and Class Members suffered injury and seek an order directing Defendants' disgorgement and the return to Plaintiffs and the classes of the amount each improperly paid to Defendants.

SIXTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. Prof. Code § 17200

98. Plaintiff realleges and incorporates by reference each preceding paragraph as though set forth at length herein.

99. Plaintiff has standing to pursue this cause of action as Plaintiff has suffered injury in fact and has lost money or property as a result of Defendants' actions as delineated herein.

100. The UCL defines unfair business competition to include any "unlawful, unfair or fraudulent" act or practice, as well as any "unfair, deceptive, untrue or misleading" advertising. Cal. Bus. Prof. Code § 17200.

101. A business act or practice is "unlawful" if it violates any established state or federal law.

102. Defendants' business practices, as alleged herein, violate the "unlawful" prong by:

(a) breaching implied warranty of merchantability as to purchasers of the Ring camera;

(b) By engaging in negligent acts and practices by failing to take one or more acts when it should have acted or by taking one or more affirmative actions that it should not have taken as described herein;

(c) By violating the Privacy Policy available at https://shop.ring.com/pages/privacy-notice and/or engaging in misrepresentations and/or omissions of fact;

(d) By violating the FTC;

(e) By being unjustly enriched;

(f) By knowingly and intentionally concealing from Plaintiff and the Class material information; and/or

(g) By breaching an implied contract (e.g., Privacy Policy available at https://shop.ring.com/pages/privacy-notice)

(h) By violating other common or statutory law.

103. Defendants' business practices, as alleged herein, violate the "unfair" prong of California Business & Professions Code §§ 17200, *et seq*. Defendants' business practices are unfair business practice under the UCL because they "either 'offend[] an established public policy' or [are] 'immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.'" *Evenchik v. Avis Rent A Car Sys., LLC*, 2012 WL 4111382, at *8 (S.D. Cal. Sept. 17, 2012) *(quoting McDonald v. Coldwell Banker,* 543 F.3d 498, 506 (9th Cir.2008) (quoting *People v. Casa Blanca Convalescent Homes, Inc.,* 159 Cal.App.3d 509, 530, 206 Cal.Rptr. 164 (1984)).

104. A business act or practice is also, "unfair" under the Unfair Competition Law if the reasons, justifications, and motives of the alleged wrongdoer are outweighed by the gravity of the harm to the alleged victims. The injury resulting from Defendants' acts and practices is substantial, not outweighed by any countervailing benefits to consumers or to competition, and not an injury that the consumers themselves could reasonably have avoided.

105. Defendants' business practices, as alleged herein, also violate the "unfair" prong of the UCL because Defendant (a) misrepresented the source, sponsorship, approval, or certification of goods or services; (b) represented that goods or services have sponsorship, approval, characteristics, ingredients, uses, quantities that they did not have or that a person has a sponsorship, approval, status, affiliation, or connection that he or she does not have; (c) representing that goods or services are of a particular standard, quality, or grade […] if they are of another; (d) advertising goods or services with intent not to sell them as advertised; (e) representing that a transaction confers or involves rights, remedies, or obligations that it does not involve, or that are prohibited by law; (f) representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not; and/or (g) inserting an unconscionable provision in a contract.

106. As a direct and proximate result of Defendants' unlawful and unfair,

business practices, Plaintiff and the Class have suffered injury in fact and lost money or property.

107. The basis for Plaintiff's claims emanated from California as one or more decisions regarding security regarding the Ring cameras occurred at the Ring Headquarters. Additionally, Ri*ng LLC claims that "if you have any questions about this Privacy Notice, or if you would like us to update information we have about you, change your preferences or exercise other applicable data protection rights, please contact us by e-mail at privacy@ring.com or write to us at: Ring LLC 1523 26th Street Santa Monica, CA 90404."

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;
b. An Order appointing Plaintiff as the class representative;
c. An Order appointing undersigned counsel as class counsel;
d. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;
e. An award of damages;
f. An award of costs and expenses;
g. An award of attorneys' fees; and
h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: December 26, 2019

Respectfully submitted,

/s/ Francis J. Flynn, Jr.

LAW OFFICE OF
FRANCIS J. FLYNN, JR.
Francis J. "Casey" Flynn, Jr., SBN 304712
422 S. Curson Avenue
Los Angeles, California 90036
Tele: 314-662-2836
Email: casey@lawofficeflynn.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (FL Bar No. 324681) *
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-2434
jyanchunis@forthepeople.com

* to seek *pro hac vice* admission

Attorneys for Plaintiff and the Putative Class