Hassan A. Zavareei (SBN 181547)
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
(202) 973-0900; Fax (202) 973-0950
hzavareei@tzlegal.com

Daniel S. Robinson (SBN 244245)
Michael Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
molson@robinsonfirm.com

Tina Wolfson (SBN 174806)
Theodore W. Maya (SBN 223242)
Bradley K. King (SBN 274399)
Rachel R. Johnson (SBN 331351)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585
twolfson@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com
rjohnson@ahdootwolfson.com

Interim Co-Lead Counsel for Plaintiffs and the Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

In re Ring LLC Privacy Litigation

This document relates to: all cases

Case No. 2:19-cv-10899-MWF-RAO

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

(I) Negligence
(II) Violation of Cal. Bus. & Prof. Code § 17200
(III) Breach of Implied Contract
(IV) Unjust Enrichment
(V) Intrusion Upon Seclusion
(VI) Public Disclosure of Private Facts
(VII) Consumers Legal Remedies Act
(VIII) Breach of Implied Warranty of Merchantability
(IX) Negligence
(X) Violation of Cal. Bus. & Prof. Code § 17200
(XI) Unjust Enrichment
(XII) Intrusion Upon Seclusion
(XIII) Public Disclosure of Private Facts

JURY TRIAL DEMANDED

JUDGE: Hon. Michael W. Fitzgerald
CTRM: 5A

Plaintiffs Ashley Lemay (individually and as parent and guardian for her minor daughter A.L.), Todd Craig, Tania Amador, Jason Ball (individually and as parent and guardian for his minor son J.B.), Josefine and Michael Brown, Angela Mako (individually and as parent and guardian for her minor daughter M.M.), Marco Mariutto, Yolanda Martinez, Jeannette Pantoja, Johnny Powell, William and Sherry Slade, Corrina and Jerathen Tillman (individually and as parents and guardians for their minor sons C.T. I and C.T. II), Jacob and Ashley Norris, Maureen and James Butler (individually and as guardians for Phyllis Mckiernan and as parents and guardians for their minor son B.B.), John Baker Orange, John and Jennifer Politi (individually and as parents and guardians for their minor children J.P. I and J.P. II), Abhi Sheth, Lue Mayora (individually and as parent and guardian for her minor children R.M. and A.M.), Richard Cambiano, Jason Caldwell, Megan Skeuse (individually and as parent and guardian for her minor children T.S. and S.S.), and Brandon Hagan (collectively, "Plaintiffs"), on behalf of themselves and all persons similarly situated, bring this Second Amended Consolidated Complaint against Defendant Ring LLC ("Defendant" or "Ring").

The claims of the Purchaser Plaintiffs, as defined in the Court's order granting in part and denying in part Ring's motion to compel arbitration (Dkt. 113; "Arb. Order"), are stayed pending the outcome of their arbitration proceedings. The Non-Purchaser Plaintiffs, as defined in the Arb. Order and as to whom the Court denied Ring's motion to compel arbitration (*see id.* at 13-16), proceed with their claims individually and on behalf of the Non-Purchaser Hacked Families Class. This Second Amended Consolidated Complaint separates the causes of action and classes being pursued by the two separate groups of plaintiffs now before this Court.

I. INTRODUCTION

1. This case addresses Ring's egregious failure to provide the safety and security it ostensibly promises its customers and users of its devices, and its failure to

respect its customers' and their families' fundamental rights to privacy and autonomy—including the right to privacy in one's home.

2. Ring markets and sells home security remote-access cameras and appurtenant software (collectively, "devices"). Intended for use in and around the home, Ring's devices feature motion-activated cameras; a "live view" that allows users to "check in on" their homes remotely; and a two-way talk feature that allows users to communicate through the devices. According to Ring, its home security devices offer "smart security here, there, everywhere." Ring promises users that it takes cyber-security seriously and will safeguard users' private information.

3. Despite Ring expressly promising to provide its customers and their families "peace of mind," and to put its customers' and their families' "security first," its devices actually expose the most intimate areas of customers' homes—and consequently the most private aspects of customers' and their families' lives—to unauthorized third parties through its deliberately inadequate security measures that allow hackers to invade and terrorize their homes. Ring failed to protect Plaintiffs against ill-meaning hackers despite that it was on notice of the inadequacies of its cybersecurity as a result of previous breach incidents.

4. Further, by affirmatively sharing customers' personal information with third parties without the customers' clear, informed consent, Ring unlawfully helps third parties to continuously track consumer activity inside the home and augment consumers' digital "fingerprints." Ring thus places its own profits above the sacred privacy rights of its customers and the very security its devices are supposed to protect.

5. Instead of helping families protect their homes, Ring's devices—plagued with cyber-security vulnerabilities—provided hackers a wide-open back door to enter the very homes the devices were supposed to protect. These simple vulnerabilities, including the failure to require two-factor authentication, permitted vicious criminals to terrorize Ring customers, including their young children, inside their own homes.

6. That is exactly what happened to Plaintiffs Ashley LeMay and her daughter A.L., Todd Craig and Tania Amador, Jason Ball and his son J.B., Josefine and Michael Brown, Angela Mako and her daughter M.M., William and Sherry Slade, Corrina and Jerathen Tillman and their children C.T. I and C.T. II, Jacob and Ashley Norris, Maureen and James Butler as well as Ms. Butler's elderly mother Phyllis McKiernan and the Butlers' minor son, B.B., John Baker Orange, John and Jennifer Politi and their minor children J.P. I and J.P. II, Lue Mayora and her minor children R.M. and A.M., Richard Cambiano, Jason Caldwell, Megan Skeuse and her minor children T.S. and S.S., and Brandon Hagan (collectively, the "Hacked Families"). The Purchaser Plaintiffs, all purchased Ring's indoor security devices intending to protect their homes and feel safer. Instead, the Ring devices allowed intruders into their home to terrify and harass them and their families, including their young children. Plaintiffs who purchased the Ring devices and/or opened Ring accounts bring claims on behalf of themselves and the proposed Purchaser Hacked Families Class. *See infra* ¶¶ 441-541. Their non-purchasing family members bring claims on behalf of themselves and the proposed Non-Purchaser Hacked Families Class. *See infra* ¶¶ 542-592.

7. For example, as further described below in the Factual Allegation section, Plaintiffs who relied on Ring devices to watch their children's bedrooms were faced with the horror of hackers observing and yelling obscenities, sexually explicit vulgarities, and racial slurs at their children through the devices. Hackers verbally threatened other Hacked Families with ransom demands and death threats. The very devices the Hacked Families purchased to protect their homes and families were used as weapons to destroy their privacy and security and traumatize them.

8. In addition to virtual harassment, Ring's cybersecurity failings also have the potential to cause identity theft and even physical harm to its customers. As chatter on the dark web and hacking forums indicates, hackers discussed creating tools for breaking into the Ring accounts, which would allow access to payment information and fraudulent charges. Hackers also discussed the possibility of physically breaking into

the homes, or manipulating entry permissions to the home, by accessing the Ring doorbell device system. Indeed, as described below, a hacker had access to the Norris family's physical address and sent a pizza delivery to the home after he finished harassing them through their Ring device, as if to prove to the Norris family that the hacker had gained knowledge of the Norris' home address.

9. Furthermore, Ring actively shared users' sensitive personal identifying information ("PII") with third parties without first obtaining users' authorization or consent. This sensitive data, combined with data already in the possession of third parties such as Facebook, allows third parties to build comprehensive and unique digital fingerprints to track consumer behavior and engage in surveillance behind the walls of one's private home, further enriching both Ring and the third parties. Plaintiffs Marco Mariutto, Yolanda Martinez, Jeannette Pantoja, Johnny Powell, and Abhi Sheth (collectively, the "Purchaser/Accountholder Plaintiffs") were victims of Ring's unauthorized use and dissemination of their PII and bring claims on behalf of themselves and the proposed Purchaser/Accountholder Class.

10. All Purchaser Plaintiffs purchased Ring's devices based on Ring's misrepresentations and omissions about security, safety, and privacy. They had no way of knowing that the Ring devices were defective and insecure, or that Ring would share their PII with third parties without their consent in violation of their privacy rights.

11. Plaintiffs intend to ask the Court to certify a Class under Rule 23(b)(2) and 23(b)(3) on behalf of all persons in the United States who purchased Ring's defective devices and insecure services and/or created an account for use of such devices (the "Accountholder Class"). Plaintiffs further intend to ask the Court to certify two Classes under Rule 23(c)(4) (the "Purchaser Hacked Families Class" and the "Non-Purchaser Hacked Families Class," or, collectively, the "Hacked Families Classes") to determine that Ring is liable for the horrendous privacy intrusions suffered by the Hacked Families.

12. Ring continues to sell to the public devices that are not secure and are prone to hacking, while promising consumers "peace of mind" and safety despite continuing to affirmatively share its customers' PII with third parties without their clear, informed consent.

13. Plaintiffs bring this lawsuit to hold Ring responsible for selling defective, dangerous devices and proliferating misrepresentations, and to prevent the public from being similarly harmed in the future. Plaintiffs request that the Court order Ring to take all necessary measures to secure the privacy of user accounts and devices, to stop sharing customers' PII with third parties without their clear, informed consent, and to compensate Plaintiffs and the Class members for the damage that Ring's acts and omissions have caused.

II. PARTIES

14. Plaintiffs Jason Ball and his minor son J.B. are residents and citizens of Michigan. Plaintiff Jason Ball is a member of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiff J.B. is a member of the Non-Purchaser Hacked Families Class.[1]

15. Plaintiff John Baker Orange is a resident and citizen of Alabama and is a member of the Accountholder Class and the Purchaser Hacked Families Class.

16. Plaintiffs Josefine and Michael Brown are residents and citizens of Florida and are members of the Accountholder Class and the Purchaser Hacked Families Class.

17. Plaintiffs Maureen and James Butler, Phyllis McKiernan, and the Butlers' minor son B.B., are residents and citizens of Colorado. Plaintiffs Maureen and James Butler are members of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiffs Phyllis McKiernan and B.B. are members of the Non-Purchasers Hacked Families Class.

[1] All Classes are defined in the Class Allegations Section. *See infra* ¶¶ 422-440.

18. Plaintiff Jason Caldwell is a resident and citizen of Michigan and a member of the Accountholder Class and the Purchaser Hacked Families Class.

19. Plaintiff Richard Cambiano is a resident and citizen of Texas and a member of the Accountholder Class and the Purchaser Hacked Families Class.

20. Plaintiffs Todd Craig and Tania Amador are residents and citizens of Texas and are members of the Accountholder Class and the Purchaser Hacked Families Class.

21. Plaintiff Brandon Hagan is a resident and citizen of Indiana and a member of the Accountholder Class and the Purchaser Hacked Families Class.

22. Plaintiffs Ashley LeMay and her minor daughter A.L. are residents and citizens of Washington. Plaintiff Ashley LeMay is a member of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiff A.L. is a member of the Non-Purchaser Hacked Families Class.

23. Plaintiffs Angela Mako and her minor daughter M.M. are residents and citizens of Colorado. Plaintiff Angela Mako is a member of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiff M.M. is a member of the Non-Purchaser Hacked Families Class.

24. Plaintiff Marco Mariutto is a resident and citizen of California and a member of the Accountholder Class.

25. Plaintiff Yolanda Martinez is a resident and citizen of Florida and a member of the Accountholder Class.

26. Plaintiffs Lue Mayora and her minor children R.M. and A.M. are residents and citizens of Texas. Plaintiff Lue Mayora is a member of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiffs R.M. and A.M. are members of the Non-Purchaser Hacked Families Class.

27. Plaintiffs Ashley and Jacob Norris are residents and citizens of Kansas and are members of the Accountholder Class and the Purchaser Hacked Families Class.

28. Plaintiff Jeannette Pantoja is a resident and citizen of Colorado and a member of the Accountholder Class.

29. Plaintiffs John and Jennifer Politi and their minor children J.P. I and J.P. II are residents and citizens of New York. Plaintiffs John and Jennifer Politi are members of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiffs J.P. I and J.P. II are members of the Non-Purchaser Hacked Families Class.

30. Plaintiff Johnny Powell is a resident and citizen of Georgia and a member of the Accountholder Class.

31. Plaintiffs William and Sherry Slade are residents and citizens of Maryland and are members of the Accountholder Class and the Purchaser Hacked Families Class.

32. Plaintiffs Megan Skeuse and her minor children T.S. and S.S. are residents and citizens of Pennsylvania. Plaintiff Megan Skeuse is a member of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiffs T.S. and S.S. are members of the Non-Purchaser Hacked Families Class.

33. Plaintiffs Jerathen and Corrina Tillman and their minor sons C.T. I and C.T. II are residents and citizens of North Carolina. Plaintiffs Jerathen and Corrina Tillman are members of the Accountholder Class and the Purchaser Hacked Families Class. Plaintiffs C.T. I and C.T. II are members of the Non-Purchaser Hacked Families Class.

34. Plaintiff Abhi Sheth is a resident and citizen of Washington and a member of the Accountholder Class.

35. Defendant Ring LLC is a Delaware limited liability company with its principal place of business in Santa Monica, California.

III. JURISDICTION AND VENUE

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

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

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

IV. FACTUAL ALLEGATIONS

A. Ring's deficient security standards and practices resulted in trauma, harm, and damages to families across the country whose devices were hacked.

39. The Hacked Families suffered horrific invasions of their privacy due to Ring's substandard security practices and apathetic approach to protecting consumer privacy. As a result of Ring's actions and omissions, the Hacked Families Class members continue to suffer emotional distress and anxiety, loss of their privacy, and have incurred and continue to incur substantial harm. The Hacked Families Class members would not have incurred these harms and damages but for the acts and omissions of Ring described herein.

The LeMay Family

40. At all times relevant herein, Ms. LeMay resided in Nesbit, Mississippi. In December of 2019, she worked the overnight shift as a medical laboratory scientist at a hospital near her home. She initially began researching indoor security devices so that she could check on her four-year-old daughter who has a history of seizures during the night while she was at work. After conducting some research, on November 29, 2019, Ms. LeMay purchased a "2-Pack Indoor Cam."

41. Ms. LeMay installed one of the devices in the upstairs bedroom where three of her daughters slept. She installed the second device in the downstairs bedroom

where her fourth daughter, the baby, slept. When Ms. LeMay and her husband each created a Ring account username and password, Ring did not prompt either of them to enable two-factor authentication or to use a strong, unique password.

42. On December 4, 2019, shortly after 8 p.m., while Ms. LeMay was running errands, both of the Ring devices began live-streaming. Simultaneously, the Tiny Tim cover of "Tiptoe Through the Tulips," a song that appeared in a scene from the 2020 horror film "Insidious," began to play through the two-way talk feature. Intrigued by the music, Ms. LeMay's eight-year-old daughter, A.L., went to the room she shares with two of her younger sisters to investigate. But the room was empty. As A.L. wandered the room, looking for the source of the music, the song abruptly stopped, and a man's voice rang out: "Hello there."

43. A hacker had gained unauthorized access to Ms. LeMay's Ring device. He was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts. [2]

44. The hacker could see, hear, and speak to eight-year-old A.L. and began to shout racial slurs at A.L.: "N****r! N****r! N****r!" He instructed A.L. to "go tell Mommy you're a n****r!"

[2] The faces on the images contained herein have been pixelated for the protection of the identities of individuals.

45. A.L., confused, asked, "Who is that?" The man responded: "I'm your best friend. You can do whatever you want right now. . . . you can break your TV. You can do whatever you want."

46. The hacker also told A.L., among other things, that he was "Santa Claus" and asked if she wanted to be his "best friend." At one point, A.L. screamed in distress, "Mommy!"

47. Finally, A.L., terrified, left the room to tell her father that someone was "being weird upstairs." At that point, A.L.'s father entered the room and disabled the device.

48. Ms. LeMay and her then-husband changed their passwords immediately, and Ms. LeMay called Ring that day to report that her indoor security device had been hacked. A Ring representative told her that Ring would look into it, but Ms. LeMay did not receive a response.

49. Five days later, on December 9, 2019, Ms. LeMay still had not heard back from Ring. Ms. LeMay emailed Ring customer support approximately three more times, then called them again. A representative informed her dismissively that Ring has people who are 'paid to talk about that' and opined that the issue had 'probably' been

taken care of when Ms. LeMay changed her password. Of course, the issue had not been taken care of, because no one had provided any information about why or how this horrific intrusion had occurred or confirmed that it could not happen again.

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

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

52. Ring also has not disclosed how the hacker was able to gain access to the devices. Ring blamed Ms. LeMay for failing to enable two-factor authentication. But Ring did not even prompt her to enable two-factor authentication when she set up her account, and even if she had enabled it, it would not necessarily have prevented the hacker from accessing their devices.

53. Since then, Ms. LeMay has been unable to use the indoor security devices out of fear she will be hacked again. She and A.L. have suffered severe emotional distress, including fear and anxiety.

54. In addition to the emotional distress and trauma, Ms. LeMay incurred damages as a result of the hacking incident. These include damages in the form of lost time spent contacting Ring on multiple occasions trying to understand the hack, requesting records from Ring, and asking questions of Ring about the hack. She had to miss multiple days of work and take a leave of absence from work. She eventually had to leave her job because of the emotional distress this incident caused her and because of the need to attend doctor's visits and take A.L. to doctor's visits, and spend time caring for A.L. in the aftermath of the hack. She and A.L. have both attended therapy and incurred additional medical bills due to the anxiety and distress that this caused

them.

55. She and A.L. also suffered damages due to the loss of privacy and loss of privacy in their home.

56. Had she known the truth about Ring's substandard security practices and its practice of sharing sensitive PII with third parties, Ms. LeMay would not have purchased products from Ring or would have paid substantially less and would not have installed Ring devices in her home, created Ring accounts, and used her Ring devices and apps.

57. These damages would not have been incurred but for Ring's acts and omissions.

Maureen and James Butler, Phyllis McKiernan, and B.B.

58. Plaintiffs Maureen and James Butler purchased three Ring security devices – one for their home in Colorado, and two to monitor Ms. Butler's mother, Phyllis McKiernan, inside her apartment at an assisted living facility. All three devices were connected to the same account.

59. On the night of July 3, 2019, hackers took control of the device installed in Ms. McKiernan's room at her assisted living facility. Immediately, they began to harass Ms. McKiernan by blaring the device's alarm to wake her and get her attention.

60. Upon her entering the room in view of the device, the hackers identified themselves as "911" and the "NYPD". Visibly confused by what was going on, Ms. McKiernan declared that she was going to bed.

61. The hackers threatened Ms. McKiernan: "Tonight you die."

///

///

///

///

///

///

62. Following this, the hackers told her that they were outside her door. Ms. McKiernan then went out into the hallway, asking "what is happening?" The hackers then began making lewd and bizarre sexual comments to her, including saying "you're pretty sexy, damn", "are you a virgin?", "do you want to make me not a virgin?", and "can you be my first?"

63. Ms. McKiernan, who was 87 years old at the time of the incident, was frightened, confused, and traumatized by what had occurred.

64. Ms. Butler was alerted to what was happening to her mother, and immediately went to the facility to comfort her and disable the devices. She stayed with her that night, and for the next ten nights, because her mother had difficulty sleeping due to anxiety from the event.

65. Within the hour, the hackers moved on to the Ring doorbell device installed at the Butler's home, which was connected to the same account.

66. There, they began harassing the Butlers' minor sixteen-year-old son, B.B. and a group of his friends as they were leaving the house.

67. The hackers again made bizarre sexual comments, telling B.B. he "looks sexy" and asking if he "wants to fuck." They also told him "I almost killed your grandma. I almost killed her." One of the hackers also said, "no one uses Ring guys; it is easy to hack. I cracked it myself, only me."

68. After disabling their doorbell device, the Butlers contacted Ring to report the hack and find out what had happened. They asked that Ring provide them with the video recording of the incidents, and to help them track down the hackers. The Butlers also filed a police report.

69. Though Ring did provide the videos, they did nothing to help the Butlers track down the persons who had hacked the devices. Instead, the company blamed the Butlers for the incident, telling them that the problem was with their password.

70. Since the hack occurred, the Butlers and Ms. McKiernan have suffered emotional distress, including fear and anxiety, due to the breach of security. Ms. McKiernan was particularly traumatized by the event. Prior to her device being hacked, she was living independently and happily at an assisted living facility. But she was shaken by the incident, and became fearful that the hackers may be nearby, and that they might continue to torment her in the future. As a result, to protect her and ease her anxiety, the Butlers moved her out of the facility and into their home.

71. As a consequence, the Butlers suffered damages, including costs associated with remodeling their home to accommodate Ms. McKiernan, costs of

providing an in-home caretaker, and moving expenses. Ms. Butler also quit her job to help care for her mother.

72. The Butlers also hired a cybersecurity firm to find the hackers, though they have not yet been identified.

73. They also suffered harm due to the invasion of privacy and loss of privacy in their home.

74. These damages would not have been incurred but for Ring's acts and omissions.

The Mayora Family

75. Plaintiff Lue Mayora purchased five Ring "Stick Up" devices. One device was placed outside in front of the house above the garage, pointing toward the street. A second device was placed on the right side of house, pointing toward the street and side of the house. A third device was placed on the left side of the house pointing toward the back gate and backyard of the house. A fourth device was placed on the back of the house pointing toward the back door and backyard. A fifth device was placed inside the house in living room area, pointing toward stairs, master bedroom, and overseeing living room.

76. Plaintiff Lue Mayora purchased the devices to provide additional security in her home for her family, which includes her husband and two minor children, R.M. and A.M.

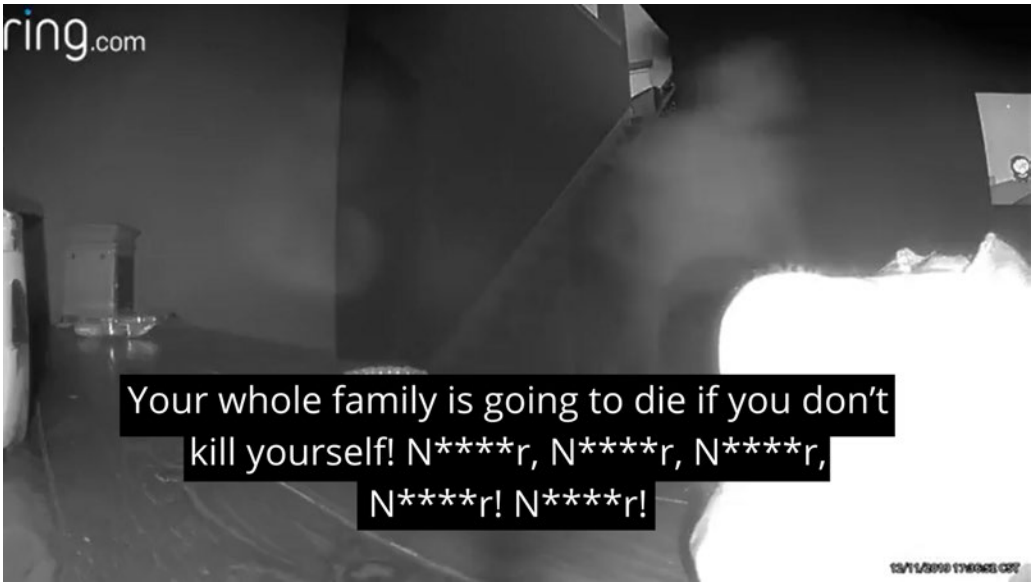
77. When creating a password for her Ring system, Ring told Plaintiff Mayora that her password was strong.

78. On or about December 11, 2019, a hacker gained access to the Ring device system.

79. In the first video, Ms. Mayora's daughter, A.M., is seen in the background of the indoor Ring video.

80. A female voice calls out to A.M.:

> "Your dick is being molested. Say the N word or your family will die! N***r, N***r, N****r, N****r, N****r, N****r, N****r, N****r, N****r, N****r, N****r. Your whole family is going to die if you don't kill yourself! N****r, N****r, N****r, N****r! N****r!"



81. Because of this unrecognizable voice and shocking language, Ms. Mayora's daughter ran off crying.

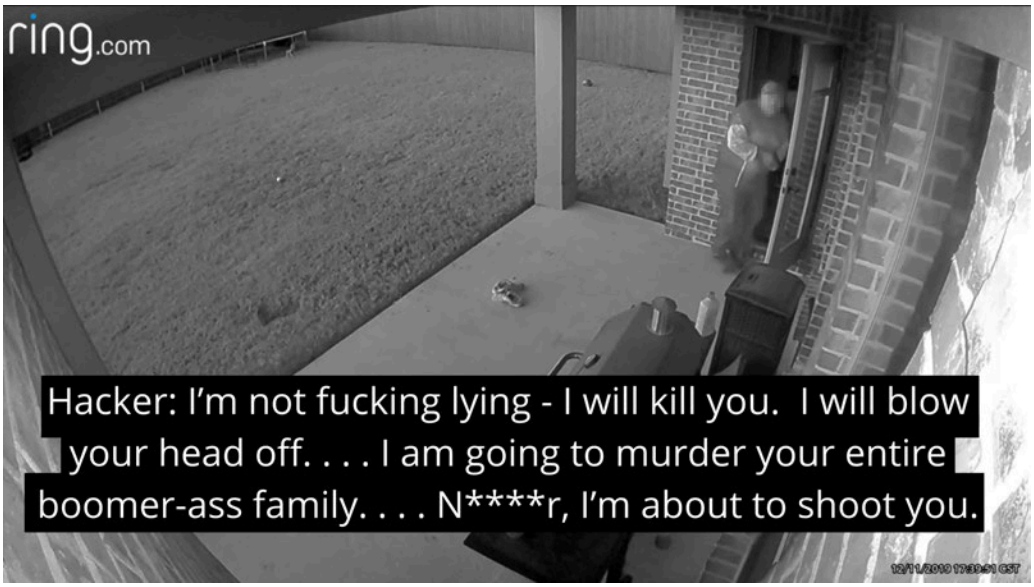
82. In the second video, the video shows Ms. Mayora's children, R.M. and A.M, running outside in the backyard frightened. Ms. Mayora's daughter is extremely upset, crying inconsolably.

83. The female voice comes through the outdoor Ring device, as though following the children, calling out to the children: "You n****r, you should fuck me in the eastside." Then there is a very loud alarm sound and maniacal laughing. At some point the voice then states to the children: "This is fucking hilarious, n****r. I am recording it. Oh fuck, I'm not?"

84. In the third video, the alarm sounds again, and Ms. Mayora's neighbor approaches the house with a gun. He investigates the scene outside and walks inside to do the same.

85. The female voice calls out again from the Ring device:

> "Buddy, you have a fucking gun. I'm not fucking lying - I will kill you. I will blow your head off. I have your d*** to your head. I am going to murder your entire boomer-ass family. N***a, I will [???] you. I have the d**k in you're a*s. I'm about to shoot you. Hello? I'm about the shoot you."



86. The neighbor, carrying a firearm, responds, "Lue, it's me."

87. The hacker, speaking through the video, responds:

> "No. It's not you. We don't recognize you. There is a burglar in the house and you need to call 911. You need to shoot yourself in your head to protect yourself. You need to shoot the camera too. You need to shoot the camera to help the situation. Shoot the camera, you're being soft."

88. Ms. Mayora's neighbor walks out of the scene, prompting the female voice to state:

> "Dude what the the fuck? Dude. You're going to wall bang me? Bro. I'll try to [stage???] on YouTube. . . . Do I talk, Richard? Oh fuck he's driving away on a fucking motorcycle?"

89. The police were contacted soon after the incident.

90. Ms. Mayora received an email on December 12, 2019 entitled "Important Message from Our Security Team" in which Ring misrepresented that "Rest assured this incident is in no way related to a breach or compromise of Ring's security."

91. Ring further instructed Ms. Mayora to activate two-factor authentication and change her password.

92. Ms. Mayora was not aware of the availability of two-factor authentication until after the hacking incident. As soon as Ms. Mayora became aware of the availability of two-factor authentication, she enabled it.

93. As a result of the hack, Ms. Mayora removed the Ring security system from her home. Plaintiff Mayora and her family, including her minor children R.M. and A.M., have suffered emotional distress, including fear and anxiety, due to the breach of security and invasion of their home.

94. In addition to the emotional distress suffered due to the hack, Ms. Mayora incurred other damages. These include damages in the form of lost time of several hours due to managing the fallout of the hack, including: communicating with Ring regarding the hack; attempting to calm and comfort her minor children, R.M. and A.M.; and seeking legal help. R.M. and A.M. have become too frightened to be home alone as a result of the incident, so Ms. Mayora has had to spend additional money for someone to be with R.M. and A.M. after school.

95. Ring did nothing to help Ms. Mayora or her children track down the person(s) who had hacked the devices. Instead, the company blamed Ms. Mayora and her children for the incident, telling them that the incident resulted from the password.

96. Ms. Mayora and her children also suffered harm – and continue to suffer harm – due to the invasion of privacy and loss of privacy in their home.

97. Had Ms. Mayora known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, Ms. Mayora would not have purchased products from Ring or would have paid substantially less, and

would not have installed Ring devices in their family home, created Ring accounts, and used the Ring devices and apps.

98. These damages would not have been incurred but for Ring's acts and omissions.

Todd Craig and Tania Amador

99. Plaintiffs Todd Craig and Tania Amador reside together in Texas. Mr. Craig maintained a home security system through another vendor for years, but after conducting some research, decided to switch to Ring.

100. In December of 2018, Mr. Craig installed a Ring doorbell. A few months later, in the spring of 2019, he decided to expand his surveillance system. Mr. Craig purchased a Ring "Stick Up Cam" security device for use in the home that he and Ms. Amador share. He installed it in their living room and kitchen area. Mr. Craig also purchased and installed two outdoor devices and an alarm system.

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

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

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

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

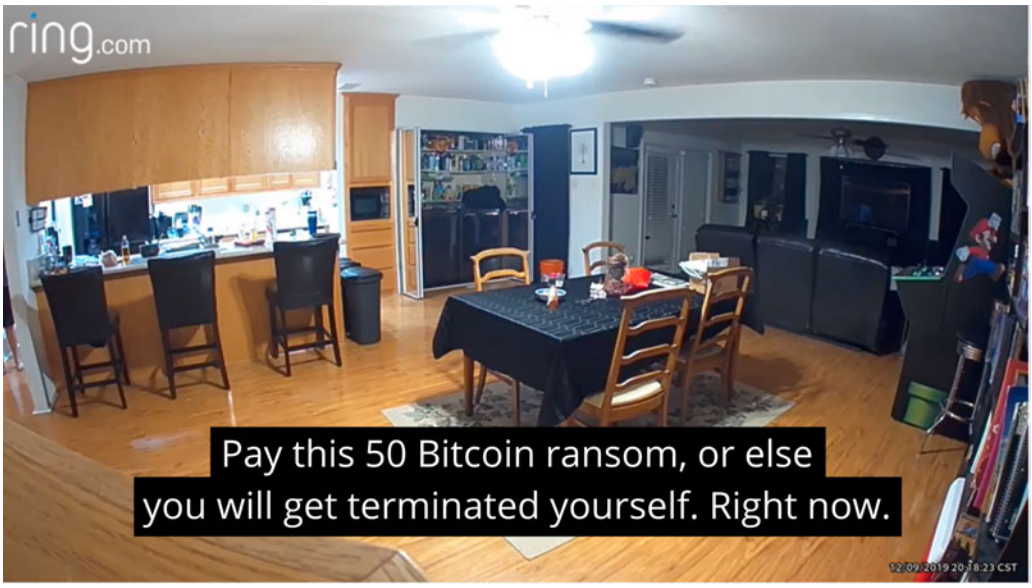
voice began shouting inside the home, "Ring support! Ring support! I would like to notify you that your account has been terminated by a hacker!"

105. Ms. Amador was napping at the time and was awakened by the noise. Mr. Craig was standing in front of his indoor device at the time of the breach and jumped at the sound. When Mr. Craig heard Ms. Amador crying out for him, he initially thought she was joking. But when he heard the threatening voice of the stranger, he realized the intrusion was real.

106. An intruder had hacked the couple's Ring system and was spying on them inside of their home. The intruder was able to do so because Ring did not utilize ordinary, basic security precautions to secure their users' accounts.

107. Mr. Craig hid behind a kitchen pillar to listen to what the hacker was saying.

108. The hacker blared sirens through the Ring devices. He threatened, "Pay this 50 bitcoin ransom, or else you will get terminated yourself. Right now."



109. The hacker then accessed the couple's doorbell device and told them, "I'm outside your front door." After the hacker stopped talking, Mr. Craig pulled the battery out of the device to disable the device.

110. Mr. Craig contacted Ring that day. The representative that he spoke to told him that an unauthorized person had accessed his security devices through Ms. Amador's account.

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

112. Mr. Craig called Ring again the following day and demanded to speak with someone from Ring's security department. He was ultimately connected to Kevin Zenteno, who said only that Ring would not provide Mr. Craig with a log of the unauthorized access and would not confirm that it had been Ms. Amador's account that was used. He promised to provide Mr. Craig with information that Mr. Craig could share with law enforcement, but never provided such information.

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

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

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

116. In addition to the emotional distress suffered due to the hack, Mr. Craig and Ms. Amador incurred damages as a result. These include damages in the form of lost time contacting Ring to report and inquire about the hack and requesting their records from Ring. They also incurred damages due to lost time spent completely overhauling their security system due to the breach, and spent time creating a home invasion plan, realizing that it was necessary after their personal information was accessed by unauthorized users with malicious intentions. Mr. Craig attended therapy sessions and incurred medical expenses due to the hacks. They purchased home defense firearms to protect themselves from threats since, because of the hacks, they no longer feel safe in their home.

117. They also suffered harm due to the invasion of privacy and loss of their privacy in their home.

118. Had they known the truth about Ring's substandard security system, and its practice of sharing sensitive PII with third parties, Mr. Craig and Ms. Amador would not have purchased products from Ring or would have paid substantially less and would not have installed Ring devices in their home, created Ring accounts, and used their Ring devices and apps.

119. These damages would not have been incurred but for Ring's acts and omissions.

The Brown Family

120. Plaintiffs Josefine and Michael Brown purchased Ring's indoor security devices to protect their home in Cape Coral, Florida. Mr. Brown is a retired military member and after years of living on a military base, it was important to the Browns to make sure their home was secure. They spent money on the Ring devices believing Ring's representations about the security of its products.

121. The Browns created a Ring account and paid for a subscription to Ring's services.

122. On December 8, 2019, the Browns were in their living room, video

chatting with their eldest son. Suddenly, a voice began speaking to them through the Ring device. A hacker had accessed their Ring account and was spying on them through the device. He was able to do so because Ring did not utilize ordinary, basic security precautions to secure their customers' accounts.

123. The hacker insulted the Browns and their family with racial slurs. Mr. Brown is African American and Mrs. Brown is white. The hacker said, "Hey, uh, is your son Black or light-skinned or white? I don't know how it came out." He asked if their son was "a baboon" "like the monkey" and if he "looked like an Oreo."

124. The Browns' younger son, a teenager who lives with them, was not in the room at the time, suggesting that the hacker had previously watched him through the device.

125. The hacker shouted for the Browns' attention and turned on the Ring device's siren, which blared across the living room. Then the voice announced, "It's your boy Chance on Nulled. Welcome to the NulledCast. What's going on? How you doing?"

126. The Browns asked who the hacker was, and the hacker again identified himself as "Chance from Nulled."

127. The NulledCast was a podcast that streamed hacks of indoor security devices.

128. The hacker ordered the Browns to "bring, like, a web browser up on your phone and then type in the website that I tell you." The Browns replied, "No," and the hacker said that if they did, he would "leave you and your family alone." Otherwise, he said, he would "do this," and turned the sirens on again.

129. Mr. Brown then disconnected the video device.

130. The Browns filed a police report and contacted Ring.

131. A Ring representative contacted the Browns and blamed them for the hack, stating that it had to do with their username and password.

132. Since the hack, the Browns have suffered emotional distress, including fear and anxiety. Mrs. Brown feels afraid and unsettled because she did not know how long she was being spied on, or how long her teenage son was being spied on. In addition to the emotional distress suffered due to the hack, the Browns incurred damages as a result of the incident. These include damages in the form of lost time when they had to contact Ring to report and understand the hack, file a police report, request their records from Ring, and ask questions of Ring about the hack. The Browns also purchased new security devices since they no longer felt safe using the Ring devices. Mrs. Brown has incurred expenses associated with doctors' visits and anxiety.

133. Had they known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, the Browns would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in their home, created Ring accounts, and used Ring devices and apps

134. They also suffered harm due to the invasion of privacy and loss of their privacy in their home.

135. These damages would not have been incurred but for Ring's acts and omissions.

The Mako Family

136. Plaintiff Angela Mako purchased an indoor Ring device for her home in Colorado, believing that Ring was a reputable and trustworthy company that had done its due diligence on their products' cybersecurity. She installed the camera in her young daughter's room to monitor her as she slept. Her daughter, M.M., is epileptic, and Ms. Mako believed that the Ring device would be a good way for her to observe her daughter in case she suffered from any seizures during the night.

137. Ms. Mako created a Ring account and does not recall being prompted to enable two-factor authentication. She used a strong password to secure the account.

138. Only a few days after installing the camera, on or about December 7, 2019, she heard loud noises from M.M.'s room in the middle of the night. Hackers had taken control of the camera system and were yelling at M.M. to "wake the fuck up."

139. They were able to do so because Ring did not utilize ordinary, basic security precautions to secure their users' accounts.

140. Upon hearing the voices from the device's microphone, Ms. Mako realized that the hackers could see inside her daughter's room. She then went to disconnect the device. As she was doing so, the hackers harassed and cursed at her, calling her a "bitch" and telling her "get your slimy mitts off me."

141. Disgusted by what had happened, Ms. Mako immediately deleted the device from her Ring app and posted the recorded video of what occurred to the Ring Neighbors App, warning others of her experience with the product.

142. Ring quickly removed the video, purportedly on the grounds that it was not related to crime or safety.

143. The next day, Ms. Mako contacted Ring customer service and informed them of the incident.

144. Later, a Ring representative called her back and proceeded to blame her for getting hacked, claiming that it had to do with her password. Ms. Mako used a strong password for her Ring indoor camera and did not share that password with anyone. She had numerous other password-protected electronics, none of which were breached.

145. Ring also initially refused to provide a copy of the video that it had deleted from the Neighbors App, insisting that they "can't delete videos from" her account and that they had "no way to retrieve videos from" her account. After numerous emails and phone calls in which Ring employees gave Ms. Mako the runaround, Ms. Mako informed a customer service agent that she works in electronic security and knows that a company like Ring had the video and would not fool her. Suddenly Ring found the video and sent it to her.

146. Ms. Mako returned the device only a few days after purchasing it.

147. Since the hack, Ms. Mako suffered emotional distress, anxiety, and upset due to the security of her home being violated. M.M. also suffered emotional distress.

148. In addition to the emotional distress suffered due to the hack, Ms. Mako incurred damages in the form of lost time spending many hours contacting Ring trying to understand the hack, requesting records from Ring, and asking questions of Ring about the hack. She also incurred damages in the form of lost time improving her security by changing accounts and passwords and otherwise ensuring that her identity was protected.

149. Ms. Mako also had to find a new way to monitor whether her daughter was having a seizure, so she had to spend additional time researching a new monitoring system. She incurred the expense of purchasing a new baby monitor, and spent time installing it. When traveling for work, she now experiences anxiety to the point where she has requested accommodations at her job to reduce the amount of travel. Ms. Mako would not have had to request that accommodation but for Ring's acts and omissions.

150. She and M.M. also suffered harm due to the invasion of privacy and loss of their privacy in their home.

151. Had she known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, Ms. Mako would not have purchased products from Ring or would have paid substantially less, and would not have installed a Ring device in her home, created Ring accounts, or used her Ring devices and apps.

152. These damages would not have been incurred but for Ring's acts and omissions.

The Tillman Family

153. Plaintiffs Jerathen and Corrina Tillman, a married couple, installed two indoor Ring devices in their North Carolina home. They also have a Ring doorbell device and three outdoor cameras. After researching home security systems, they decided to purchase Ring devices based on Ring's representations about safety and security, and its affiliation with Amazon, a prominent company.

154. They created a Ring account as part of the doorbell setup. The password to their account was strong, including capital letters, lowercase letters, numbers, and symbols. Ring did not prompt them to enable two-factor authentication when they created their account.

155. The Tillmans installed the Ring devices in the bedrooms of their young children C.T. I and C.T. II so that they could keep an eye on them.

156. On December 4, 2019, after 10 p.m., the Tillmans heard their then-three-year-old son C.T. II yelling and the Ring sirens blaring from his room. Mr. Tillman opened the Ring app on his phone and turned on the live view for both their sons' rooms to see what was going on. Both sons were sitting up in bed.

157. The Tillmans ran to C.T. II's room. The light on the Ring device was on, and a man was speaking to the three-year-old through the device. A hacker had gained access to the Tillmans' account and was spying on their toddler through their Ring device. This was possible because Ring did not utilize ordinary, basic security precautions in securing their customers' accounts.

158. Mr. Tillman attempted to turn the device off through the Ring app on his phone, but it did not work. He then reached for the device. The hacker shouted, "don't put your finger in me!"

159. Mr. Tillman removed the batteries from the Ring device.

160. Suddenly, the Tillmans heard the Ring device's sirens blaring in their eight-year-old son C.T. I's room. They ran to his room and found him awake. A woman's voice was saying, "Well, hello there," through the Ring device. Mr. Tillman removed the batteries from that device.

161. The hackers then triggered the outside alarms. The Tillmans were afraid that would-be intruders could be trying to lure them outside, so they called the police. A police escort accompanied the Tillmans to remove their outdoor Ring devices.

162. That night, the Tillmans slept together in the same room with their children. Their eight-year-old son C.T. I was afraid to return to his room.

163. The Tillmans contacted Ring that night and were told that what was happening was "not possible." Later, Ring blamed the Tillmans for the hack, asking if they had shared their passwords with other people.

164. Ring refused to give them information that they needed to provide to law enforcement, and only after repeated requests did Ring provide a list of IP addresses that accessed the account without other information. Ring claimed that because the

Tillmans had removed their indoor devices, Ring could no longer access the videos of the incident in order for the Tillmans to provide a copy to law enforcement.

165. Since they were hacked, the Tillmans have suffered emotional harm, including anxiety and distress. They feel uncomfortable in their own home. Their sons C.T. I and C.T. II have suffered immense anxiety and emotional distress. To this day, they will ask from time to time if there are cameras inside the home, and they can recall what was said to them over the devices that night. The experience with Ring left the Tillmans with a long-lasting fear. They feel they will never again feel completely safe.

166. In addition to the emotional distress suffered due to the hack, the Tillmans incurred damages as a result. These include damages in the form of lost time contacting Ring trying to understand the hack, contacting the police, requesting their records from Ring, and asking questions of Ring about the hack. They also spent time changing passwords for accounts to improve security and monitoring the outdoor area of their home for days and weeks after the hacks. They did not allow their children to play outside for fear of harm from the intruders.

167. They also suffered harm due to the invasion of privacy and loss of their privacy in their home.

168. Had they known the truth about Ring's substandard security system, and its practice of sharing sensitive PII with third parties, the Tillmans would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in their home, created Ring accounts, and used their Ring devices and apps.

169. These damages would not have been incurred but for Ring's acts and omissions.

The Norris Family

170. Plaintiffs Jacob and Ashley Norris installed Ring indoor devices in their Wichita, Kansas home to promote security and peace of mind for themselves and their children.

171. On December 9, 2019, Ms. Norris was cooking dinner when a hacker took control of the device in the family's living room, speaking to her son and commenting on things she was doing and items in the home that could be seen through the device. The hacker was able to take control of the Norris family's devices because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

172. Initially, Ms. Norris thought that these comments were from a FaceTime call on her son's tablet device, or perhaps that her husband, who was not home at the time, was playing a prank.

173. But soon thereafter, Mr. Norris arrived home, and the noises from the device continued. The hackers commented on the Christmas tree in the family's living room. When Mr. Norris went to disable the device, the hacker said, "don't you dare fucking unplug me," and "put me down, I have feelings."

174. Mr. Norris unplugged the device, and then went to examine another Ring indoor device, which was in the downstairs family room. A hacker spoke from that device as well, first telling Mr. Norris that he was from Ring tech support, and then telling him that "I have your address," indicating that he would have a pizza delivered to the Norris' home to demonstrate that he knew where they lived.

175. Later that night, it became clear that the hacker did in fact learn the Norris' address when the pizza arrived.

176. Terrified, the Norris family contacted the police and Ring customer support. But they never received satisfactory answers on what had occurred. Instead, Ring blamed them for the hack, saying that their password was insufficient, when in fact they had used a strong password.

177. Since the hack occurred, the Norris family suffered emotional distress, including fear and anxiety, as a result of the breach of security in their home. Their ten-year-old daughter was particularly frightened and expressed fear and upset for months following the incident.

178. In addition to the emotional distress suffered due to the hack, the Norris family incurred damages in the form of lost time contacting Ring trying to understand the hack, contacting the police, requesting their records from Ring, and asking questions of Ring about the hack.

179. They also suffered harm due to the invasion of privacy and loss of their privacy in their home.

180. These damages would not have been incurred but for Ring's acts and omissions.

William and Sherry Slade

181. Plaintiffs William and Sherry Slade purchased and installed multiple Ring security devices to help protect their home in Maryland. Mr. Slade created an account and added Ms. Slade and their two children. He does not recall being notified whether his password was strong or weak, but he does recall the password being unique.

182. Mr. Slade switched to Ring from a different indoor security system because he believed it would offer better features and he trusted Ring's representations about safety and security.

183. On December 9, 2019, Ms. Slade was home alone doing laundry when the Ring indoor device in her living room was hacked.

184. A group of men was able to take control the devices because Ring does not utilize ordinary, basic security precautions to secure their customers' accounts.

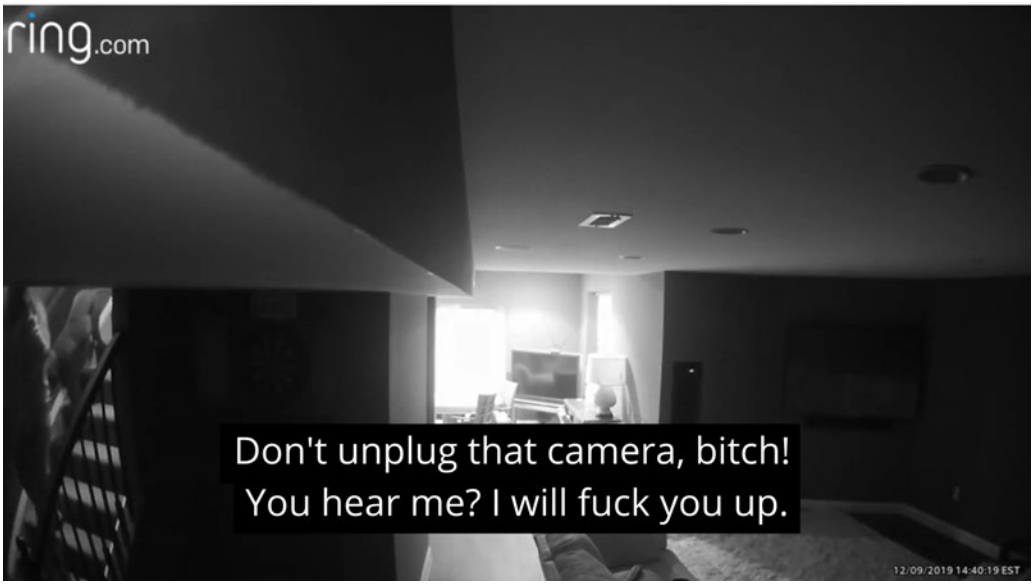
185. The hackers used the devices to harass Ms. Slade by blaring alarm sounds, making "meowing" noises, and shouting vulgarities at her, including "hey, bitch", and "show me them boobies." She disconnected the device.

186. After Ms. Slade disconnected the upstairs device, the hackers moved on to the device in the Slades' basement. They again sounded the device's alarm, and made threatening statements, including "I will fuck you up, don't make me hurt you, girl" to Ms. Slade, before she disabled that device as well.

187. When the Slades contacted Ring customer service to figure out what had happened, which account was hacked, and whether their passwords had been compromised, Ring refused to help. Instead, Ring blamed the Slades for the hack for purportedly using a weak password.

188. Since the hack, Ms. Slade has suffered emotional distress, anxiety, and upset due to the security of her home being violated. The Slades live in a secluded area and Ms. Slade will no longer stay alone in the house because she does not feel safe.

189. Initially, Ms. Slade accused her teenage son and his friends of playing a bad practical joke. Her son, who was not the perpetrator, became highly offended and



it caused family conflict as a result.

190. In addition to the emotional distress suffered due to the hack, the Slades incurred damages in the form of lost time contacting Ring trying to understand the hack, requesting their records from Ring, and asking questions of Ring about the hack. The Slades incurred damages when they purchased a new security system to replace

Ring's system, and lost time spent installing it. Ms. Slade has incurred medical expenses because of the anxiety that she now suffers from.

191. They also suffered harm due to the invasion of privacy and loss of their privacy in their home.

192. Had they known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, the Slades would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in their home, created Ring accounts, and used their Ring devices and apps.

193. These damages would not have been incurred but for Ring's acts and omissions.

John Baker Orange

194. Plaintiff John Baker Orange is a resident of Jefferson County, Alabama. He purchased a Ring outdoor camera device for his house in July 2019. The Ring device was installed over his garage with a view of the driveway.

195. Mr. Orange purchased the Ring device to provide additional security for him and his family, including his wife, and three children—then ages seven, nine, and ten.

196. In or around December 2019, Mr. Orange's children were playing basketball when a voice came on through the device's two-way speaker system.

197. A hacker had obtained unauthorized access to his Ring account and had taken over his device. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

198. The hacker engaged with Mr. Orange's children, commenting on their basketball play and encouraging them to approach the device.

199. When Mr. Orange learned of the incident, he changed the password on the Ring device and enabled two-factor authentication.

200. At the time he created his account, Mr. Orange was not prompted to use two-factor authentication and does not believe users had the ability to do so.

201. Mr. Orange suffered harm due to the invasion of privacy and loss of their privacy in their home.

202. These damages would not have been incurred but for Ring's acts and omissions.

The Ball Family

203. Plaintiff Jason Ball purchased his Ring indoor security system several years ago due to Ring's reputation and messaging around safety and security. He spent hundreds of dollars installing a Ring security system for his home.

204. Mr. Ball is a retired law enforcement officer, and protecting his home is important to him. And in the summer, he often goes to a cottage in northern Michigan. He purchased Ring indoor devices to help keep his home safe at all times.

205. Mr. Ball created a Ring account, but he never was prompted to enable two-factor authentication. He used a password that he did not use for other accounts and that he did not believe could be guessed.

206. On December 8, 2019, Mr. Ball was watching TV with his teenage son J.B. when he began to hear some distorted sounds emanating from the indoor Ring device.

///

///

///

///

///

///

///

///

///

207. Then, Mr. Ball heard a voice coming from the device, saying, "What's goin' on buddy? What are you watching?" The voice claimed he wanted to sell Mr. Ball a Ring upgrade.

208. A hacker had taken control of the device and was watching and speaking to Mr. Ball and J.B. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

209. The hacker began to insult and mock Mr. Ball, saying, "dude, look at the top of your head, what the fuck happened to your hair? You're fucking bald, buddy!"

210. Mr. Ball ran to the device to turn it around so that the hacker could not see him and the inside of his home.

211. The hacker shouted for Mr. Ball, "dude, don't unplug me, man! Don't unplug me! What are you doing? … turn me around!"

212. The hacker told Mr. Ball to meet him in the garage and began speaking through the Ring device in the garage.

213. Terrified and unsure of how to stop the hacker, Mr. Ball deactivated his internet router. He also immediately changed his password.

214. Mr. Ball called Ring that night but was unable to speak to anyone.

215. It took three days for anyone from Ring to speak to Mr. Ball. Ring blamed a third-party hacker and claimed that Mr. Ball's password was not secure.

216. Since the hack, Mr. Ball and his son suffered emotional distress, including fear and anxiety. He lost trust in his home security system.

217. In addition to the emotional distress suffered due to the hack, Mr. Ball incurred damages in the form of lost time contacting Ring trying to understand the hack, requesting records from Ring, and asking questions of Ring about the hack. He has also contacted a security specialist about installing a standalone system at his house and has incurred medical expenses associated with his anxiety. He spent a substantial amount of time changing passwords and reviewing the security of all of his accounts.

218. Mr. Ball and J.B. also suffered harm due to the invasion of privacy and loss of their privacy in their home.

219. Had he known the truth about Ring's substandard security system, and its practice of sharing sensitive PII with third parties, Mr. Ball would not have purchased products from Ring or would have paid substantially less and would not have installed Ring devices in his home, created Ring accounts, and used the Ring devices and apps.

220. These damages would not have been incurred but for Ring's acts and omissions.

Richard Cambiano

221. Plaintiff Richard Cambiano purchased a Ring Outdoor Wi-Fi Cam with Motion Activated Floodlight on or about May 14, 2018; a Spotlight Cam Mount x 3, an Alarm Protection Kit, a Floodlight Cam, a Stick Up Cam Wired, an Alarm Keypad, an Alarm Motion Detector, and Alarm Contact Sensor x 2 on or about January 7, 2019; and a Ring Stick Up IndoorOutdoor 1080p WiFi Wired Security Camera on or about November 16, 2019.

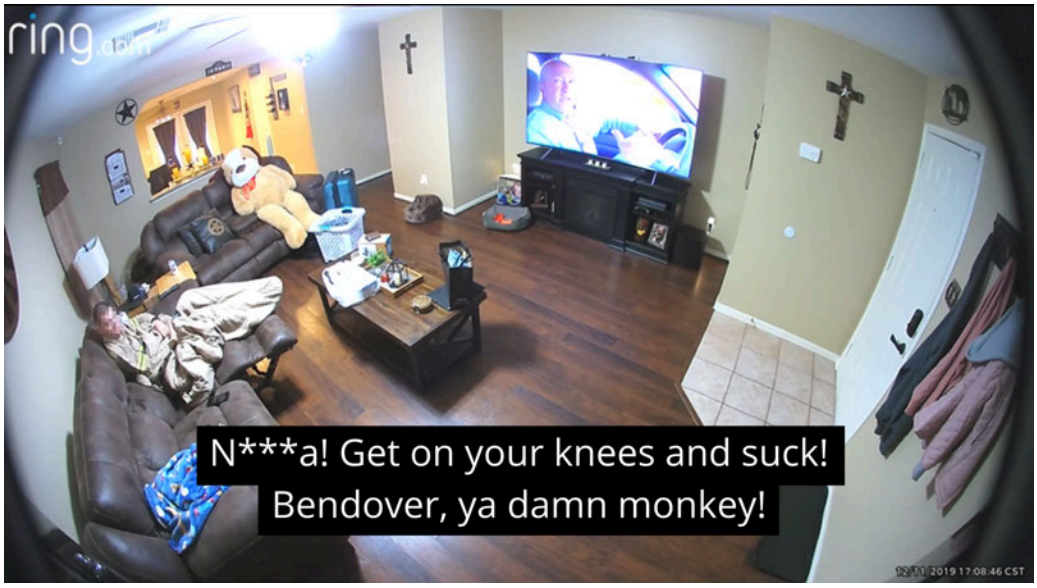
222. Mr. Cambiano purchased a few additional Ring devices as well.

223. Mr. Cambiano purchased the Ring devices to provide additional security for himself and his fiancée, who babysits her young niece and nephews quite often at their home.

224. On or about December 11, 2019, a hacker gained access to the Ring device and began yelling at Mr. Cambiano, including profanities that were sexually explicit and disturbing. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

225. In particular, a voice (which sounds exactly like the voice in the Mayora video from the same date) said the following disturbing things:

> "Hey buddy room – Nice Roomba – Can I have it? . . . Are you a police officer? . . . Please don't rape my whole family. . . . I see you are very sad and you have a teddy bear. . . . Can I, uh . . . Really N***a? . . N***a! Get on your knees and suck. Bend over ya damn monkey."



226. At some point, the hacker set off the sirens on Mr. Cambiano's alarm system.

227. This event was terrifying to Mr. Cambiano and his fiancée.

228. Mr. Cambiano notified Ring of the breach.

229. Within a few hours of reaching out to Ring about the breach, Ring acknowledged the security breach and claimed to have conducted an investigation, however blamed Mr. Cambiano for the hack, stating the following:

> During a recent investigation by our security team, we identified that the email address and password of one of your external accounts was exposed in a data breach. Due to the fact that many people use the same username and password for many different accounts, bad actors often re-use credentials stolen or leaked from one service on other services. We believe that somebody may have used this method to attempt to gain access to your Ring account and we are committed to making sure that you and those you designate are the only people with access to your account. Rest assured this incident is in no way related to a breach or compromise of Ring's security.

230. Upon investigation, Mr. Cambiano learned and subsequently informed Ring that the password used on the Ring Account was never used on any other accounts.

231. Ring then recommended that Mr. Cambiano activate two-factor authentication, change his password, and notify any shared users to do the same.

232. Mr. Cambiano was not aware of the availability of two-factor authentication until after the hacking incident. As soon as he became aware of the availability of two-factor authentication, Mr. Cambiano enabled it.

233. Mr. Cambiano has suffered emotional distress, including fear and anxiety, due to the breach of security. He also worries about how many people had hacked into the system and watched he and his fiancée and other guests, including minors, without saying anything at all. Additionally, Mr. Cambiano has fear regarding the fact that because Ring is part of the whole house alarm system, hackers could have disabled the Ring system, physically entered the house, left the house, and reenabled the security system – all without Mr. Cambiano's knowledge or consent and he would have no idea that it happened.

234. In addition to the emotional distress suffered due to the hack, Mr. Cambiano incurred other damages. These include damages in the form of lost time of

several hours managing the fallout of the hack, including: communicating with Ring regarding the hack; changing passwords and enabling two-factor authentication; attempting to calm and comfort his fiancée who learned about the incident; and seeking legal help.

235. Ring did nothing to help Mr. Cambiano track down the person(s) who hacked the devices. Instead, the company blamed Mr. Cambiano for the incident, telling him that the incident was caused by his password. When Mr. Cambiano asked for Ring to provide him with a record of log-ins so that he could determine how many hacks had occurred, Ring stated that it does not have that information, and that there was no way to find that out.

236. Mr. Cambiano also suffered harm – and continues to suffer harm – due to the invasion of privacy and loss of privacy in his home.

237. Had Mr. Cambiano known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, Mr. Cambiano would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in his home, created Ring accounts, and used the Ring devices and apps.

238. These damages would not have been incurred but for Ring's acts and omissions.

Jason Caldwell

239. Plaintiff Jason Caldwell is a resident of Oakland County, Michigan. Plaintiff Caldwell purchased four Ring camera devices for his house on or about November 18, 2019. One Ring device was installed in Mr. Caldwell's kitchen. The other Ring devices were installed in various places outside the home. Mr. Caldwell purchased the Ring device to provide additional security for him and his family.

240. At approximately 2:13 a.m. on January 2, 2020, a hacker gained access to his Ring device in his kitchen. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

241. First, the hacker said: "Hello? What's up my n***as? n***a, n***a. What's up, my n***a?"

242. Next, the voice started talking to the family dog, making kissing sounds and calling to the dog: "Doggy! Here doggy!"

243. Then, when Mr. Caldwell opened his refrigerator, the voice asked if Plaintiff Caldwell was "Thirsty?"

244. When Mr. Caldwell realized that a voice was coming from the Ring device, he turned the device over. While turning the device over, the voice said "Please don't! Please don't!" Once the device had been turned over, the voice said "Hey that ain't nice – turn me around. I'm the AI guy [???] in your camera."

245. While Mr. Caldwell ran to his office to change his password, the voice started playing music in the background, stopping it at times. The music contained the following lyrics:

> Well, I could be more specific
> Uh, I'm a human, and I just wanted to, you know
> For the sake of all of us earthlings out there
> Just wanted to say:
> We love the Earth, it is our planet
> We love the Earth, it is our home
> We love the Earth, it is our planet
> We love the Earth, it is our home
>
> Hi, I'm a baboon
> I'm like a man, just less advanced and my anus is huge.

Finally, the music stopped, however, the voice began to sing a terrifying song, which is often associated with mass shootings:

> All the other kids with the pumped up kicks **You'd better run, better run, out run my gun.** All the other kids with the pumped up kicks You'd better run, better run, outrun my bullet. All the other kids with the pumped up kicks **You'd better run, better run, out run my gun.**

246. This event was terrifying to Mr. Caldwell and his family.

247. On January 2, 2020, Mr. Caldwell notified Ring of the hacking event. In response, Ring essentially blamed Mr. Caldwell for the hack, stating:

> To protect your Ring account, you should take advantage of two-factor authentication (2FA) available in the account settings of the Ring app. Please consider enabling the 2FA feature in your account today. I also recommend changing your password and making sure it's different than any other password you use; it's the best way to protect your Ring account.

248. Ring did nothing to help Mr. Caldwell track down the person(s) who had hacked the devices. Instead, the company blamed Mr. Caldwell for the incident, telling him that the problem was with his password.

249. As a result of the hack, Mr. Caldwell suffered and continues to suffer emotional distress, including fear and anxiety from the breach of security, hearing terrifying songs through his Ring device, and not knowing how long he was being watched beforehand. As a direct result of the incident, Mr. Caldwell began to have, and continues to have, issues sleeping and suffers from nightmares. Plaintiff was not able to see a therapist or psychologist to work through the trauma of the incident because of

the associated cost to do so and because of insufficient insurance coverage; however, Mr. Caldwell believes it would have been helpful.

250. In addition to the emotional distress Mr. Caldwell suffered due to the hack, he incurred other damages as a result of the incident. These include damages in the form of lost time of approximately 10 plus hours managing the aftermath of the hack, including: communicating with Ring regarding the hack; updating his password; and seeking legal help.

251. Had Mr. Caldwell known the truth about Ring's substandard security system, and its practice of sharing sensitive PII with third parties, he would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in his home, created Ring accounts, and used the Ring devices and apps.

252. These damages would not have been incurred but for Ring's acts and omissions.

The Skeuse Family

253. On or about February 4, 2019, Plaintiff Megan Skeuse and her husband purchased a Ring Camera Deluxe Pro Kit. The Ring camera device was installed in the Skeuses' living room with a view of the living room, kitchen, and hallway to the front door.

254. The Skeuses purchased the Ring camera kit to provide additional security for their family.

255. On or about December 13, 2019 at approximately 7:35 p.m., a hacker accessed the Ring device and began yelling at the Skeuse children, T.S. and S.S., scaring them. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

256. Ring acknowledged the security breach, but has otherwise been unhelpful about the incident.

257. On December 15, 2019, two days after the hacking incident, the Skeuses received an email from Ring with the subject line: "Important Security Update from Ring." The email claimed that Ring's systems were not compromised.

258. On December 16, 2019, Ring Support responded to the Skeuses' complaint in an email entitled "Security Concern," claiming to have investigated the incident, essentially blaming Mrs. Skeuse, and recommending that she enable two-factor authentication.

259. Prior to the hacking incidents, Mrs. Skeuse was unaware of and believes that Ring did not provide customers the ability to secure their systems with two-factor authentication. Had Mrs. Skeuse known that two-factor authentication could have been enabled, Ms. Skeuse would have enabled it. In fact, she did so as soon as she learned about it.

260. As a result of the hack, Mrs. Skeuse and her family, including her minor children, T.S. and S.S., immediately stopped using the Ring system and Mrs. Skeuse deleted the app in fear that she and her family would be hacked again. Mrs. Skeuse and her family have suffered emotional distress, including fear and anxiety, due to the breach of security. Mrs. Skeuse was deeply upset by the event as her youngest child was in the process of potty training during the hacking incident. As part of the training process, the child was walking around the area of the house where hacked Ring camera was installed, naked from the waist down. Mrs. Skeuse still worries about whether the footage was seen by an unauthorized party and captured and circulated on the dark web.

261. In addition to the emotional distress suffered due to the hack, Mrs. Skeuse incurred damages as a result. These include damages in the form of lost time of several hours over multiple days managing the aftermath of the hack, including: communicating with Ring via telephone and email regarding the hack; updating her password; calming and comforting her family; and seeking legal help. Mrs. Skeuse spent additional time and money to purchase a new hard-wired security system because of her fear another hack could occur.

262. Ring did nothing to help Mrs. Skeuse and her family track down the person(s) who hacked the devices. Instead, Ring blamed Mrs. Skeuse and her children for the incident, telling them that the problem was with their password.

263. Mrs. Skeuse and her children also suffered harm due to the invasion of privacy and loss of privacy in their home.

264. Had Mrs. Skeuse known the truth about Ring's substandard security system, and its practice of sharing sensitive PII with third parties, Mrs. Skeuse and her family would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in the family home, created Ring accounts, and used the Ring devices and apps.

265. These damages would not have been incurred but for Ring's acts and omissions.

The Politi Family

266. John and Jennifer Politi and their minor children J.P. I and J.P. II, residents of New Yok, purchased and own various Ring devices including a video doorbell, outdoor video surveillance camera devices, and an indoor video surveillance camera device.

267. On or about December 9, 2019, the Politis' son ran into their room, terrified because a male voice was calling out from the first floor asking if anyone was home.

268. Mr. Politi was unable to find an intruder, so the Politis told their children it must have been coming from a neighbor's house.

269. The next night the Politis were in bed when their children came running into their room again because they heard a male voice downstairs humming a scary tune.

270. Mr. and Ms. Politi then heard what sounded like a siren alarm coming from their first floor.

271. Mr. Politi went downstairs and did not see anyone in the house, but heard a male voice calling out "what's up bro?," asking if Mr. Politi could hear him, and telling Mr. Politi to "come here."

272. At this point, Mr. Politi saw lights displayed on the ring indoor camera device and realized that the voice and siren were coming from it.

273. He quickly unplugged the Ring device.

274. Mr. Politi later discovered that the lights displayed means the camera device is being accessed.

275. He recalls seeing these same lights displayed at times over the past year that they have had the device, meaning unauthorized individuals have watched the Politi family in the past. The unauthorized individuals were able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

276. Mr. Politi called Ring about the shocking privacy invasions, but Ring simply told the Plaintiff to change his password.

277. Since the incident, the Politis have not used the Ring indoor camera device because it is not secure, which means the device that cost the Politis over $100 is currently useless to them.

278. Mr. Politi also posted a notice on Ring's "Ring Neighborhood" social media site to warn other Ring users about the possibility of a hack and the inadequate security measures. However, Mr. Politis' warning post was swiftly removed by Ring.

279. Plaintiffs' children J.P. I and J.P. II were and still are traumatized by the experience. One of the children suffered and still suffers from significant anxiety including headaches, vomiting, and crying. The child also has missed a significant number of days of school, such that it has caused issues with the child's school due to excessive absences. The Politis have also suffered financial loss as a result of the school absences because Mrs. Politi has had to miss a significant number of days at work to stay at home with her son. Mrs. Politi does not receive pay for any days she does not go in to work.

280. The Politi family also suffered harm due to the invasion of privacy and loss of privacy in their home.

281. Had Mr. and Mrs. Politi known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, Mr. and Mrs. Politi would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices in Plaintiff's home, created Ring accounts, and used the Ring devices and apps.

282. These damages would not have been incurred but for Ring's acts and omissions.

Brandon Hagan

283. In July 2019, Mr. Hagan purchased a Ring Stick Up Cam and installed it in the living room of his home.

284. Mr. Hagan purchased the Ring Stick Up Cam so he could monitor workers inside his home while he was at work. He purchased and installed the Ring device based on Ring's representations about the safety and security that its devices provide. Had Mr. Hagan known that his Ring device and account was vulnerable to being compromised, misused, or accessed by unauthorized parties, he would not have purchased the Ring device for any price.

285. When installing the Ring device, Mr. Hagan also created a Ring account and installed the Ring app on his phone. Ring did not prompt him to enable two-factor authentication when he set up his account.

286. In the evening on December 7, 2019, Mr. Hagan and his wife, who was his fiancée at the time, were in his home when his Ring alarm blared loudly. A hacker began talking to Mr. Hagan through the Ring device's two-way talk feature, at first pretending to be from Ring by stating he was responding to a security call and asking Mr. Hagan if he had any concerns. The hacker then began asking Mr. Hagan perverted sexual questions, inquiring if he had any women in the house and using expletives. The hacker was able to do so because Ring does not utilize ordinary, basic security precautions to secure their users' accounts.

287. Mr. Hagan removed the device's battery to stop the man from continuing to speak through the device.

288. That same evening, Mr. Hagan called Ring to report the hacking incident. The Ring representative stated that she would send the video recording of the incident to Ring's security department. She also stated that other customers reported experiencing similar hacking incidents.

289. One week after the incident, on December 15, 2019, Mr. Hagan received an email entitled "Important Message from Our Security Team" in which Ring misrepresented, "Rest assured this incident is in no way related to a breach or compromise of Ring's security."

290. After the incident, Mr. Hagan did not reinstall the battery in his Ring device for several days. He eventually reinstalled the device on the deck outside his home. However, because he bought the device to use inside his home and no longer trusts it for that purpose, he completely stopped using the device.

291. Mr. Hagan does not trust the Ring device or Ring's systems and cannot use the device for the purpose for which it was purchased.

292. Mr. Hagan relied on Ring's representations that it offers security and protection to users and homes. Because of Ring's promises about the level of security offered by its products and services, Mr. Hagan purchased Ring's indoor camera device, created a Ring account, and installed the Ring camera device in his home.

293. Since the hack, Mr. Hagan has suffered emotional distress, fear, and anxiety due to the security of his home being violated. He lost trust in home security systems in general. He and his wife want another home security system but are afraid to purchase or install one for fear of being hacked and invaded again.

294. In addition to the emotional distress suffered due to the hack, Mr. Hagan incurred damages in the form of lost time contacting Ring trying to understand the hack, requesting records from Ring, and asking questions of Ring about the hack. He also spent time changing his password and enabling two-factor authentication for his Ring account.

295. He also suffered harm due to the invasion of privacy and loss of their privacy in his home.

296. Had he known the truth about Ring's substandard security systems, and its practice of sharing sensitive PII with third parties, Mr. Hagan would not have purchased products from Ring, installed a Ring device in his home, created a Ring account, and used this Ring device and apps.

297. These damages would not have been incurred but for Ring's acts and omissions.

B. Ring was on notice that its cybersecurity systems were inadequate and that thousands of Ring customers could be observed in their homes.

298. The Hacked Families Class members were not the only individuals who suffered privacy invasions and harm due to Ring's substandard security practices. Families across the country suffered hacks and privacy breaches of their Ring devices, leading to harassment.[3]

299. Hackers shared software for hacking Ring devices widely on the internet, including for example, "Ring Video Doorbell Config," a program used to drive special software for rapidly churning through usernames or email addresses and passwords to log into accounts and thus break into Ring devices. The hacker stated 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.[4]

[3] *See, e.g.*, 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-county/-wake-up-woman-says-someone-hacked-surveillance-system-yelled-at-her-dog/1017442073/; Ezo Domingo, Hacker talks to Chesterfield family through Ring doorbell, NBC 12 (Dec. 12, 2019); Allison Matyus, Man hacks Ring camera in woman's home to make explicit comments, Digital Trends (Dec. 17, 2019), https://www.digitaltrends.com/home/man-hacks-ring-camera-in-womans-home-to-make-explicit-comments/; "Come Here!" Woman woken up by Ring camera hacker yelling at her, KRON 4 (Dec. 13, 2019), https://www.kron4.com/video/come-here-woman-woken-up-by-ring-camera-hacker-yelling-at-her/; 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/; 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/.

[4] Joseph Cox and Samantha Cole, How Hackers are Breaking into Ring Cameras, Vice (December 11, 2019), https://www.vice.com/en/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

300. Comments on the threads for these programs illustrate the threat posed to Ring customers: "I'd assume you would only use these if you actually we're [*sic*] planning to break into the persons house."[5]

301. Ring effectively ignored attacks on and threats to its customers such as the NulledCast podcast and widespread dissemination for tips and tricks on hacking Ring devices.

302. Contrary to Ring's claims that it had not suffered any security breaches, thousands of Ring's customers' credentials had been stolen and reposted to the internet in 2019.[6] The log-in credentials for thousands of Ring device owners were compromised, allowing access to Ring customer home addresses, telephone numbers, and payment information, including the type of payment card, the payment card's last four digits, and security code. The names people gave to specific Ring cameras also were visible, which names often denote the cameras' locations, such as "bedroom" or "front door." An intruder also could access live video footage from all active Ring devices associated with an account, as well as a 30- to 60-day video history, depending on the customer's cloud storage plan. Security professionals told *Buzzfeed News* that the format of the leaked data, which included personally named Ring devices and time zones of where those Ring devices were located, suggests it was stolen from Ring's database.

303. Hackers stole credentials and dumped them online both for sale and to boost reputation among peers in the hacking community.

---

[5] *Id*.

[6] Caroline Haskins, *A Data Leak Exposed the Personal Information of Over 3,000 Ring Users*, BuzzFeed News (Dec. 19, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-usersv.

304. In yet another leak, reported by *TechCrunch*, security researchers found 1,562 unique email addresses and passwords associated with Ring doorbell accounts on a dark web text-sharing site, commonly used to share stolen passwords and illicit materials. When researchers reported the findings to Amazon, instead of protecting customers, Ring asked that the researcher not discuss their findings publicly.[7] Similar to the credentials reported to *Buzzfeed*, the list was not limited merely to usernames and passwords, but also included information specific to Ring accounts like names of devices and time zones in which the device was located.

305. And also like the leaked credentials reported by *Buzzfeed*, credentials discovered by *TechCrunch* could be used to log into a Ring account and obtain Ring customer addresses, phone numbers and payment information. The credentials also

[7] Zack Whittacker, *Over 1,500 Ring passwords have been found on the dark web*, (December 19, 2019), https://techcrunch.com/2019/12/19/ring-doorbell-passwords-exposed/.

provided access to Ring devices in that home, including access to historical video data if the setting is enabled.

306. As a result of prior hacking incidents, Ring knew its cybersecurity was deficient and that its devices were vulnerable to such attacks.

C. Hacking Incidents Were Broadcasted Over the Internet.

307. Some of the unauthorized hacks were publicized via the podcast "NulledCast" and streamed on Discord. Discord is a messaging and distribution platform where users communicate directly via voice, video, or text, and join "servers" where larger groups interact. Servers are the virtual spaces on Discord.

308. As reported by Vice, hackers advertised the public broadcasts (including live video and audio streaming) of these invasions:

> "Sit back and relax to over 45 minutes of 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."[8]

309. On the NulledCast, hackers commandeered Ring camera devices, then used the two-way talk feature to harass their unsuspecting owners and their families.[9] In addition to harassment, hackers had access to, and could broadcast essentially unlimited visual and audio surveillance of families in their homes. Hackers and their audiences likely observed and learned granular daily schedules and routines, discussions of medical and health conditions, financial and employment information, as well as the utmost private and intimate moments including moments of undress and other compromising situations.

310. Prior to each broadcasted episode of the NulledCast, hacker hosts would confirm valid Ring account credentials, observe families for some time prior to the

[8] Joseph Cox and Jason Koebler, Inside the Podcast that Hacks Ring Users Live on Air, Vice (December 12, 2019), https://www.vice.com/en_us/article/z3bbq4/podcast-livestreams-hacked-ring-cameras-nulledcast (last visited August 13, 2021).
[9] *Id.*

broadcast to learn information about them such as names, addresses, and other personal details, and then orchestrate public observation and harassment of families at numerous locations within their home live on Discord.

311. It is likely that thousands were observed in their homes and were observed without their knowledge. In addition to the 5100+ credentials reported by Buzzfeed and TechCrunch, Ring confirmed to ZDNet that *at least* 4,000 credentials listed on another site were valid. ZDNet also received links to three other instances where hackers had compiled lists of credentials for Ring accounts.[10]

312. At least 200 people were members of the Discord server where hackers broadcasted the NulledCast livestream described above. However, the extent of hackers' surveillance of, and use of information pertaining to, the private lives of individuals through Ring security cameras was greater than, and extended beyond, the NulledCast.

313. Additional hacking incidents have been streamed over the internet, and remain available for viewing at this time.[11] Nearly a year after the NulledCast, in November 2020, other hackers surfaced who claimed to have profited from livestream of security camera hacking by charging "admission" to broadcasting of the invasions. One hacker told police, "I'm watching through four different cameras, I get all entertainment for me and my guys, easy money."[12] At another hacking in Georgia, hackers claimed to have broadcasted at least "a dozen" hacks that day alone.

---

[10] Catalin Cimpanu, *Hackers keep dumping Ring credentials online 'for the giggles,'* ZDNet (December 20, 2019), <https://www.zdnet.com/article/hackers-keep-dumping-ring-credentials-online-for-the-giggles/>.

[11] *See, e.g.* Insidious Ring Camera Hack, available at <https://www.youtube.com/watch?v=d-IGYmg3r58.

[12] Evan Watson, *Swatting in Chesapeake: Hacker makes fake 911 call, uses Ring cameras to talk to police officers,* 13NewsNow (Nov. 24 2020), <https://www.13newsnow.com/article/news/local/13news-now-investigates/swatting-in-chesapeake-hacker-makes-fake-911-call-uses-ring-cameras-to-talk-to-police-officers/291-cb1fbedf-7f71-46c6-a5fa-51b88c543eb6>.

314. In October 2020, another hacking group with nearly 1,000 members on Discord reported to have three terabytes of video footage, some of which was uploaded to pornographic websites as it included intimate situations, mothers breastfeeding, and people in a state of undress. The anonymous group claimed to have footage from over 50,000 hacked cameras and charged $200 from members for access.[13]

D. In response to the horrific hacking incidents, Ring blamed the victims, and offered inadequate responses and spurious explanations.

315. In response to the numerous hacking incidents across the country, including the Hacked Families Class members' experiences, Ring initially did not accept responsibility, apologize, or outline any measures to fix its security deficiencies. Instead, it placed fault on the victims for its own deficient security features.

316. For example, in response to an onslaught of news stories regarding the series of hacking incidents, a Ring spokesperson stated, "Our security team has investigated this incident and we have no evidence of an unauthorized intrusion or compromise of Ring's systems of network. It is not uncommon for bad actors to harvest data from other company's data breaches and create lists like this so that other bad actors can attempt to gain access to other services."[14] Ring also stated that it was "made aware of an incident where malicious actors obtained some Ring users' account credentials (*e.g.*, user names and passwords) from a separate, external, non-Ring service and reused them to log-in to some Ring accounts. Unfortunately, when people

[13] Matt Willie, *50K The number of cameras reportedly hacked by one group,* Input Mag (October 14, 2020), <https://www.inputmag.com/culture/hackers-leaked-tons-of-webcam-home-security-footage-on-porn-sites>.

[14] Jay Peters, *Amazon's Ring has been blaming reused passwords, but now thousands of logins have leaked*, The Verge (Dec. 19, 2019), <https://www.theverge.com/2019/12/19/21030545/ring-leaked-personal-data-amazon-video-doorbell-camera-security-login-credentials>.

reuse the same username and password on multiple services, it's possible for bad actors to gain access to many accounts."[15]

317. Ring's explanation is unsound for multiple reasons, but even if it were remotely logical, Ring's excuses fail to recognize that Ring's own products, marketed and sold as home security devices and systems, are not designed in a manner that would prevent such hacks, even though Ring could have easily implemented security features designed to do just that.

318. Indeed, Ring did in fact have several data breaches of its own that were more likely to be the source of compromised information, contrary to its excuse of "credential stuffing" (a technique where attackers gather usernames and passwords compromised in another data breach and use them to access other apps and websites).

E. Ring's current cybersecurity protocols continue to be inadequate, placing Class Members and future Ring customers and their families at risk of getting hacked.

319. Only after receiving negative press for numerous hacks did Ring announce that it would take some measures to increase the security of its devices, such as requiring two-factor authentication, and creating a "Control Center" where customers could view and remove shared users.

320. But although Ring eventually implemented two-factor authentication, it used a weak form of two-factor authentication, sending a code by text message. Two-factor authentication by text message is the least secure method. These days, hackers can easily exploit weaknesses in phone networks to steal SMS two-factor codes. Because SMS messages aren't encrypted, they can also just leak. More recently, researchers found that this can be done on a massive scale. TechCrunch explains this as "Cybersecurity

[15] Neil Vigor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, The New York Times (Dec. 15, 2019), <https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html>.

101."[16] In June 2017, the National Institute of Standards and Technology ("NIST"), the federal government's technology standards body, released its Digital Authentication Guidelines stating that SMS-based two-factor authentication is strongly discouraged.[17] Text-based two-factor authentication is far less secure than app-based two-factor authentication, where codes are delivered over an encrypted connection to an app on a mobile phone.

321. Any fixes these belated measures provided were and are similarly insufficient to remedy the harm that Ring's acts and omissions have caused, or to compensate purchasers who unknowingly spent money on their defective and insecure devices.

322. Privacy advocacy group Fight for the Future explains Ring's efforts were inadequate to alleviate privacy concerns: "Despite a string of terrifying stories about Ring cameras being accessed in the most grotesque ways, the company doesn't appear to be making any meaningful changes to their product. Instead, they've basically given their app a [cosmetic] redesign [accompanied by a press release] and called it a new feature."[18]

323. To date, Ring's tardy updates are still insufficient to protect their consumers' privacy and security going forward. There is no indication that Ring has addressed gaping security holes like Ring leaving their devices vulnerable to brute force attacks and credential stuffing, failure to limit the number of failed login attempts, or Ring's failure to conduct basic IP detection to warn a customer that someone is

---

[16] Zack Whittacker, Cybersecurity 101: Two-factor authentication can save you from hackers, TechCrunch, December 25, 2018, <https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/>

[17] NIST Special Publication 800-63B, Digital Identity Guidelines, Computer Security, U.S. Department of Commerce, June 2020.

[18] *See* Evan Greer, *Amazon Ring isn't even good at pretending to care about your privacy and safety*, Fight for the Future (Jan. 6, 2020), <https://tumblr.fightforthefuture.org/post/190104161798/amazon-ring-isnt-even-good-at-pretending-to-care>.

attempting to login to their account from multiple different geographic locations at the same time. There is also no indication that Ring plans to require customers to use strong passwords or will prevent them from using passwords that are known to be exposed from previous data breaches.

324. In May 2020, a computer science student at the Florida Institute of Technology discovered that Ring products manifest "systemic design flaws" rendering them vulnerable to intrusion.[19] For example, the student discovered that "the mechanism for removing user accounts does not work as intended on many camera systems because it does not remove active user accounts," which could allow malicious users to retain access to a camera system indefinitely.

325. And in November 2020, news outlets reported at least one additional hacking incident that bore a striking resemblance to the experiences of the Hacked Families Class members. According to media reports, hackers accessed a Ring camera doorbell and placed a prank call to local law enforcement, claiming to be a man "confessing to hoarding explosives and killing his wife."[20] But when authorities arrived at the home, the homeowner was unharmed and did not know who the caller was. The voice speaking through the Ring device then started calling them names.

326. Incidents like these demonstrate that Ring has *not* sufficiently improved its security practices or responded adequately to the ongoing threats its products pose to its customers.

[19] *Student finds privacy flaws in connected security and doorbell cameras*, Florida Institute of Technology (May 27, 2020), <https://techxplore.com/news/2020-05-student-privacy-flaws-doorbell-cameras.html>.

[20] Samir Ferdowsi, *Amazon Ring Doorbell Hacked in Florida Swatting Incident*, Motherboard (Nov. 17, 2020), <https://www.vice.com/en/article/n7vndw/amazon-ring-doorbell-hacked-in-florida-swatting-incident>.

F. Ring violated its customers' privacy by sharing their personal identifying information (PII) with third parties.

327. Not only did Ring fail to protect Plaintiffs' Ring accounts in adopting substandard security and privacy protocols, it also violated their customers' privacy by affirmatively sharing PII with third parties without authorization or consent.

328. After widespread reporting on the Ring hacks, an investigation by the Electronic Frontier Foundation ("EFF"), a nonprofit organization that educates consumers on privacy matters, found that the Ring app integrated multiple third-party trackers including branch.io, mixpanel, appsflyer, and facebook.[21] This unauthorized release further exposed customers to privacy violations by sharing their PII with third parties and increasing the risk of unauthorized access.

329. Among the information shared with these third parties were customers' names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of Ring's customers, including Purchaser Plaintiffs.

330. For instance, Facebook, via its Graph API, is alerted when the Ring app is opened and upon device actions such as app deactivation after screen lock due to inactivity. Information delivered to Facebook (even for those without a Facebook account) includes time zone, device model, language preferences, screen resolution, the advertiser ID (IDFA for Apple and AAID for Android), "custom app events" which collect activity within the app, and a unique identifier, "anonymous id", which persists even if the advertiser ID is reset, and is used by Facebook to build shadow profiles of device owners. Collection of IDs that cannot be reset is intended to completely circumvent an individual's choice to not be tracked (a choice clearly indicated by resetting the advertiser ID on a device).

[21] Bill Budington, *Ring Doorbell App Packed with Third-Party Trackers*, Electronic Frontier Foundation (Jan. 27, 2020), <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers>.

331. Branch, which describes itself as a "deep linking" platform,[22] receives a number of unique identifiers (device_fingerprint_id, hardware_id, identity_id) as well as the device's local IP address, advertising ID, model, screen resolution, and DPI. The fingerprint ID as well as hardware ID cannot be reset. Analytics and advertising companies developed these IDs to precisely track device owner activity and behavior specifically to circumvent instances where the user has turned on limited ad tracking. The fingerprint ID is also to link web activity to mobile app activity for the same individual, gaining a more granular picture of the person's activities and habits.

332. Branch has had its own security concerns. A year and a half ago, the company was blamed for spreading a software bug to various websites that used its service. Some experts at the time claimed the bug could have exposed data belonging to as many as 645 million people.[23]

333. AppsFlyer, a big data company focused on the mobile platform, is given a wide array of information upon app launch as well as certain user actions, such as interacting with the "Neighbors" section of the app. This information includes one's mobile carrier, when Ring was installed and first launched, a number of unique identifiers, the app from which Ring was installed, and whether AppsFlyer tracking came preinstalled on the device. This last bit of information is presumably to determine whether AppsFlyer tracking was included as bloatware on a low-end Android device. Manufacturers often offset the costs of device production by selling consumer data, a practice that disproportionately affects low-income earners. Privacy International and EFF have even petitioned Google regarding the discriminatory impacts of such practices.

---

[22] Branch's website says the company unifies "fragmented data to show you each customer's full journey."

[23] Shaun Nichols, *Now this might be going out on a limb, but here's how a branch.io bug left '685 million' netizens open to website hacks,* The Register, October 12, 2018. <https://www.theregister.com/2018/10/12/branchio_xss_flaw/>.

334. Most alarmingly, AppsFlyer also receives the sensors installed on a Ring device such as the magnetometer, gyroscope, and accelerometer and current calibration settings. This information is used to track precise movements of the device and can detect, for example, when a person is sitting, standing, walking, running, or driving.

335. Ring gives MixPanel the full names and email addresses of Ring customers as well as device information such as operating system version and model, whether bluetooth is enabled, and app settings such as the number of locations a user has Ring devices installed in. MixPanel is briefly mentioned in Ring's list of third party services, but the extent of their data collection is not.

336. Ring could remove the personal identifiers in user data before sending it to third parties, but it does not.

337. Ring thus allows third parties to track its customers on a granular level, without meaningful user notification or consent and, in most cases, with no way to mitigate the damage done. Persistent identifiers and device information are often sent upon app install, and thus before the user has even had the opportunity to view and accept the terms and conditions.

338. The danger in sending even small bits of information, such as device specifications, and an advertising ID, anonymous ID, or fingerprint ID, is that analytics and tracking companies are able to combine these bits together to form a unique picture of the user's device (mobile phone or computer), and thus create a fingerprint that follows the user as they interact with other apps and use their device, in essence providing the ability to spy on what a user is doing in their daily lives, in their home, and precisely when they are doing it. This data detailing user behavior is linked into a profile resulting in broad yet near perfect surveillance of practically all of someone's interests, identities, and daily routines. The information Ring's app and website sends to third-party servers at a minimum would allow third parties to know when Ring users are at home or away.

339. This information is used to build precise and detailed profiles on individuals, ultimately identifying characteristics such as race, age, sexual orientation, relationship status, socioeconomic status, parental status, and much more. Facebook's longstanding indirect data collection practices in particular rely on apps to autonomously collect and send information about app usage to the social network without telling users about the arrangement.

340. Mobile devices contain many different types of identifiers, such as information relating to the device, as well applications, tools or protocols that, when used, allow the identification of the individual to whom the information may relate. However, even in the absence of such identifiers, researchers have found that knowledge of any four apps installed on users' smartphones is enough to successfully fingerprint and profile 95% of users. In fact, when Apple discovered the advertising ID (IDFA) was being exploited and not used for its intended purpose, they started pulling apps from the App Store that used the advertising ID but never showed ads.

341. Facebook (and other third parties to whom user behavior and activity is sent) combine data from different apps to create a fine-grained and intimate picture of people's activities, interests, behaviors and routines, some of which can reveal special category data, including information about people's health or religion. Facebook then combines this data with data brokers to place people in categories like, "heavy alcohol spender at home."

342. Furthermore, third parties like Facebook perform cross-device tracking, the practice of linking multiple devices, such as smartphones, television sets, smart TVs, and personal computers, to a single user. The more granular a user profile, the more intimate inferences can be derived about people's likely attributes, identities, habits, and opinions.

343. Obtaining data on and from a device, including the transmission of data linked to a unique identifier from an app to third parties, constitutes the processing of personal data. Data relating to the use of specific apps, including usage logs, from

which an individual is directly or indirectly identifiable is also personal data.

344. Data harvesting is the fastest growing industry in the U.S. As software, data mining, and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

345. Consumer data is so valuable that some have proclaimed that data is the new oil.[24] Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, internet companies earned $202 per American user. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate.[25]

346. The behavioral data within apps described above is particularly valuable because behavioral advertising in its currently dominant form is driven by a range of invisible tracking technologies, like cookies, device fingerprinting and SDKs,[26] using a variety of techniques, including cross-device tracking and identity matching. Privacy International is greatly concerned about the manifold ways in which people's data is exploited in these hidden back-end systems.[27]

---

[24] *The World's Most Valuable Resource Is No Longer Oil, But Data*, The Economist (May 6, 2017), available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

[25] R Shapiro, *What Your Data Is Really Worth to Facebook*, Washington Monthly (July/Aug. 2019), available at <https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/>; *see also* R Shapiro & A Siddhartha, *Who owns American's Personal Information and What is it Worth?*, available at <https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf>.

[26] "SDK" stands for "software development kit," essentially pre-written code that is contained within mobile applications that allow for the tracking of user interaction with the application.

[27] Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook Account),* December 2018, available at <https://privacyinternational.org/sites/default/files/2018-

G. The Accountholder Plaintiffs would not have purchased Ring devices had they been fully informed about Ring's affirmative PII disclosure to third parties

347. Plaintiff Yolanda Martinez purchased a Ring indoor camera device on October 25, 2019 and installed it in her home. Ms. Martinez uses her Android device to access her Ring account and camera device.

348. Ring shared Ms. Martinez's sensitive PII with third parties without her authorization or permission.

349. Ms. Martinez was unaware that Ring would share her sensitive PII with third parties without her authorization or permission. Ms. Martinez was also unaware that Ring's security devices contained significant vulnerabilities and flaws rendering them vulnerable to hacking, intrusion, and other access by unauthorized third parties.

350. Had she known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, she would not have purchased products from Ring or would have paid substantially less, and would not have installed a Ring device, created a Ring account, and used the Ring device and app.

351. Plaintiff Jeannette Pantoja purchased a Ring doorbell camera on December 6, 2018 and installed it in her home. She also purchased a Ring indoor camera.

352. Ms. Pantoja uses her Android tablet to access her Ring account and devices.

353. Ring shared Ms. Pantoja's sensitive PII with third parties without her authorization or permission. Ms. Pantoja was unaware that Ring would share her sensitive PII with third parties without her authorization or permission. Ms. Pantoja was also unaware that Ring's security devices contained significant vulnerabilities and flaws rendering them vulnerable to hacking, intrusion, and other access by unauthorized third parties.

12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf>

354. Had she known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, she would not have purchased products from Ring or would have paid substantially less, and would not have installed Ring devices, created a Ring account, and used the Ring devices and app.

355. Plaintiff Johnny Powell purchased a Ring doorbell camera on November 29, 2019. He uses his Android mobile device to access his Ring account and camera.

356. Ring shared Mr. Powell's sensitive PII with third parties without his authorization or permission. Mr. Powell was unaware that Ring would share his sensitive PII with third parties without his authorization or permission.

357. Mr. Powell was also unaware that Ring's security devices contained significant vulnerabilities and flaws rendering them vulnerable to hacking, intrusion, and other access by unauthorized third parties.

358. Had Mr. Powell known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, he would not have purchased products from Ring or would have paid substantially less, and would not have installed a Ring doorbell camera, created a Ring account, and used the Ring device and app.

359. Plaintiff Abhi Sheth purchased a Ring doorbell camera on June 12, 2019.

360. Ring shared Mr. Sheth's sensitive PII with third parties without his authorization or permission. Mr. Sheth was unaware that Ring would share his sensitive PII with third parties without his authorization or permission.

361. Mr. Sheth was also unaware that Ring's security devices contained significant vulnerabilities and flaws rendering them vulnerable to hacking, intrusion, and other access by unauthorized third parties.

362. Had Mr. Sheth known the truth about Ring's substandard data security practices, and its practice of sharing sensitive PII with third parties, he would not have purchased products from Ring or would have paid substantially less, and would not

have installed a Ring doorbell camera, created a Ring account, and used the Ring device and app.

363. Not only did Ring knowingly use and disseminate its customers' PII without their authorization, it was also grossly negligent with some customers' account security, in some instances even reassigning account credentials of one consumer to another and thus disclosing sensitive PII without authorization in those instances as well.

364. Plaintiff Marco Mariutto, a resident of California, purchased a Ring indoor camera in 2019 and installed it in his home.

365. Mr. Mariutto uses his mobile device to access his Ring account and camera.

366. In January 2020, Ring shared access to Mr. Mariutto's Ring account, containing sensitive personal identifying information, with third parties without his authorization or permission. Without Mr. Mariutto's knowledge or authorization, a Ring employee assigned his account to a stranger by adding an unknown person's email to his account, granting that individual access to Mr. Mariutto's cameras.

367. Mr. Mariutto was unaware that Ring would assign access to his account containing sensitive PII with third parties without his authorization or permission.

368. Mr. Mariutto was also unaware that Ring's security devices contained significant vulnerabilities and flaws rendering them vulnerable to hacking, intrusion, and other access by unauthorized third parties.

369. Had he known the truth about Ring's substandard data security practices, he would not have purchased products from Ring or would have paid substantially less, and would not have installed a Ring doorbell camera, created a Ring account, and used the Ring device and app.

370. In addition to suffering harm due to the extreme violation of his privacy, Mr. Mariutto suffered damages due to this unauthorized disclosure because he had to spend time contacting Ring to fix their error and regain access to his account. He also

had to purchase a new security system from another company because he could no longer trust Ring.

371. These damages would not have been incurred but for Ring's acts and omissions.

H. Ring continues to disclose PII to third Parties without clear, informed consent

372. As of December 14, 2020, Ring continues to integrate a sweeping combination of third party "analytics tools" and trackers that require collection of PII to serve their purpose. At a minimum, Ring integrates: Optimizely, Kenshoo, Heap (automatically captures every user action in an app), Solvvy, Google Conversion Tracking, Bing Universal Event Tracking, Facebook Pixel, Facebook Conversion Tracking, Mixpanel, Google Analytics, and Google Universal Analytics.[28]

373. As illustrated with branch.io, Ring customers are put at risk when information is shared with third parties. Ring customers do not have an opportunity to meaningfully research and evaluate the safety and security of Ring's services and thus potential for their sensitive information to be compromised by third parties, because Ring's privacy policy does not identify them in their privacy policy.

374. Ring's privacy policy told customers that it shared some of their data with some third parties but did not provide a complete list of who those third parties are. Regardless, customers of Ring were and are completely unaware, and could not imagine in their wildest dreams, that their daily activity and behavior patterns would be shared with third parties.

375. And, when Ring updated its privacy policy in February 2020, it *removed* links to opt out of data-sharing with third party sites. A Ring spokesperson told CBS

[28] BuiltWith Detailed Technology Profile for Ring, December 14, 2020.

news that people could opt out of sharing agreements "where applicable," but declined to clarify what "where applicable" might mean.[29]

376. Based on information and belief, Ring further uses videos containing images of Plaintiffs, including, but not limited to, members of the Non-Purchaser Hacked Families Class, for promotional and advertisement purposes and in use and/or advancement of its other services, and Ring derives a monetary benefit, profit, and additional exposure from its use of these videos.[30]

377. Based on information and belief, Ring derives data from the videos containing images of Plaintiffs, including, but not limited to, members of the Non-Purchaser Hacked Families Class, for promotional and advertisement purposes and in use and/or advancement of its other services, and Ring derives a monetary benefit, profit, and additional exposure from its use of these videos.

I. Ring's failure to protect the Plaintiffs' privacy and security, its inadequate response to the hacking incidents, and its practice of sharing customer PII with third parties were contrary to Ring's representations about its products.

378. Ring's conduct was contrary to its representations about its products.

379. Ring markets and sells security devices intended for use inside the home. Ring also markets and sells other home security devices, including motion-sensor-activated outdoor lighting and home alarm systems. It claims that its indoor security cameras offer "smart security here, there, everywhere." Ring promises users that it takes security seriously and will safeguard consumers' private information. Its deficient acts and omissions described herein were contrary to its stated mission and goals.

---

[29] Stephen Gandel, *Ring to tighten privacy amid concerns it shares customer data with Facebook and Google*, CBS (Feb. 14, 2020), <https://www.cbsnews.com/news/ring-facebook-google-personal-information-privacy-settings-change/>.

[30] Davey Alba, *Ring is using its customers' Doorbell camera video for ads. It says it's allowed to*, Buzzfeed News (June 7, 2019), <https://www.buzzfeednews.com/article/daveyalba/amazon-ring-doorbell-company-using-security-footage-for-ads?bfsource=relatedmanual>.

380. Ring's entire brand is built on the perception that its products increase the safety and security of consumers' homes. Ring's stated mission is "to make neighborhoods safer."[31] Indeed, according to Ring, it is "driven to create products that help you protect what matters most at home . . . ."[32] At other times, Ring has claimed that its mission is to "reduce crime in neighborhoods."

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

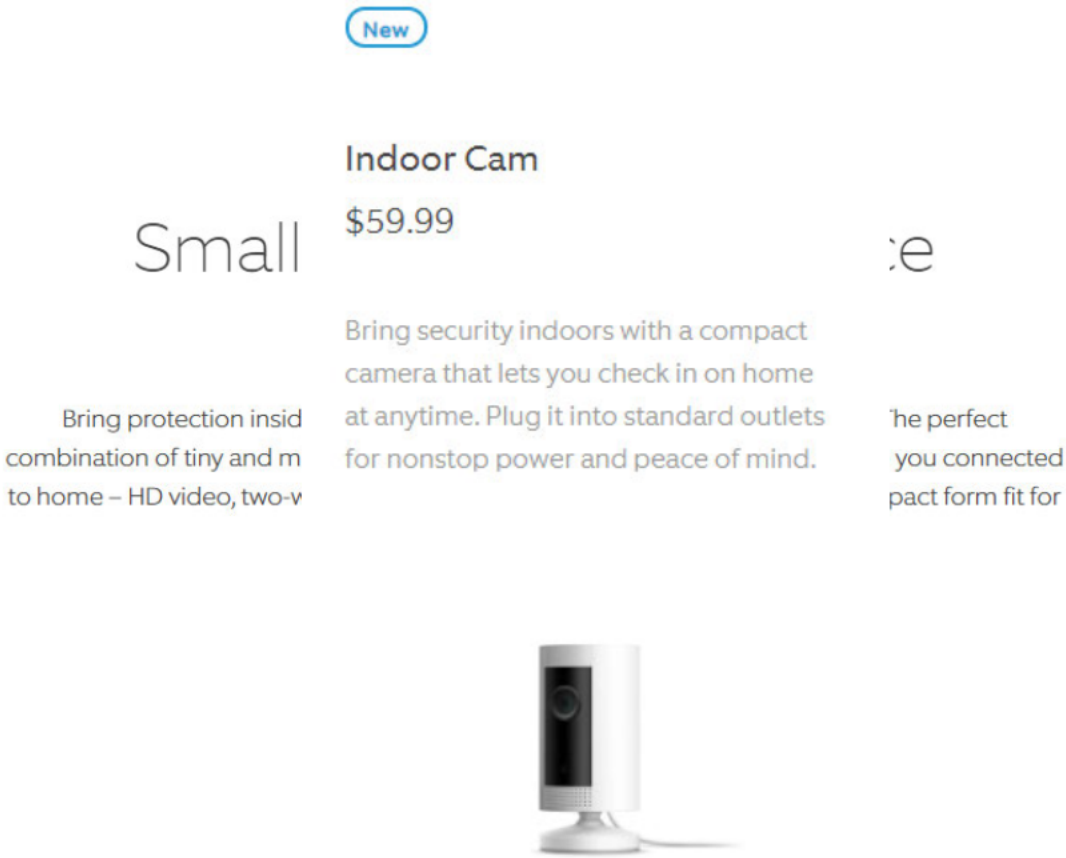
382. Ring's claims that it deters or reduces crime have helped Ring cultivate a surveillance network around the country, assisted by dozens of taxpayer-funded camera discount programs and over 600 police partnerships.[33]

383. On its website, Ring boasts that it has worked with the National Center for Missing and Exploited Children to reunite missing children with their families[34] and worked with law enforcement and communities to "achieve amazing results" like "getting stolen guns off the streets" and "helping families keep their children safe."[35]

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

[31] <https://shop.ring.com/pages/about>
[32] <https://shop.ring.com/pages/about>
[33] Caroline Haskins, How Ring Went from Shark Tank Reject to One of America's Scariest 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>.
[34] Eric Kuhn, Ring and the National Center for Missing & Exploited Children Come 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/>.
[35] Jamie Siminoff, Building Better Communities Together: How Ring Connects Communities and Law Enforcement Through the Neighbors App, Ring (Aug. 2, 2019), <https://blog.ring.com/2019/08/02/building-better-communities-together/>.

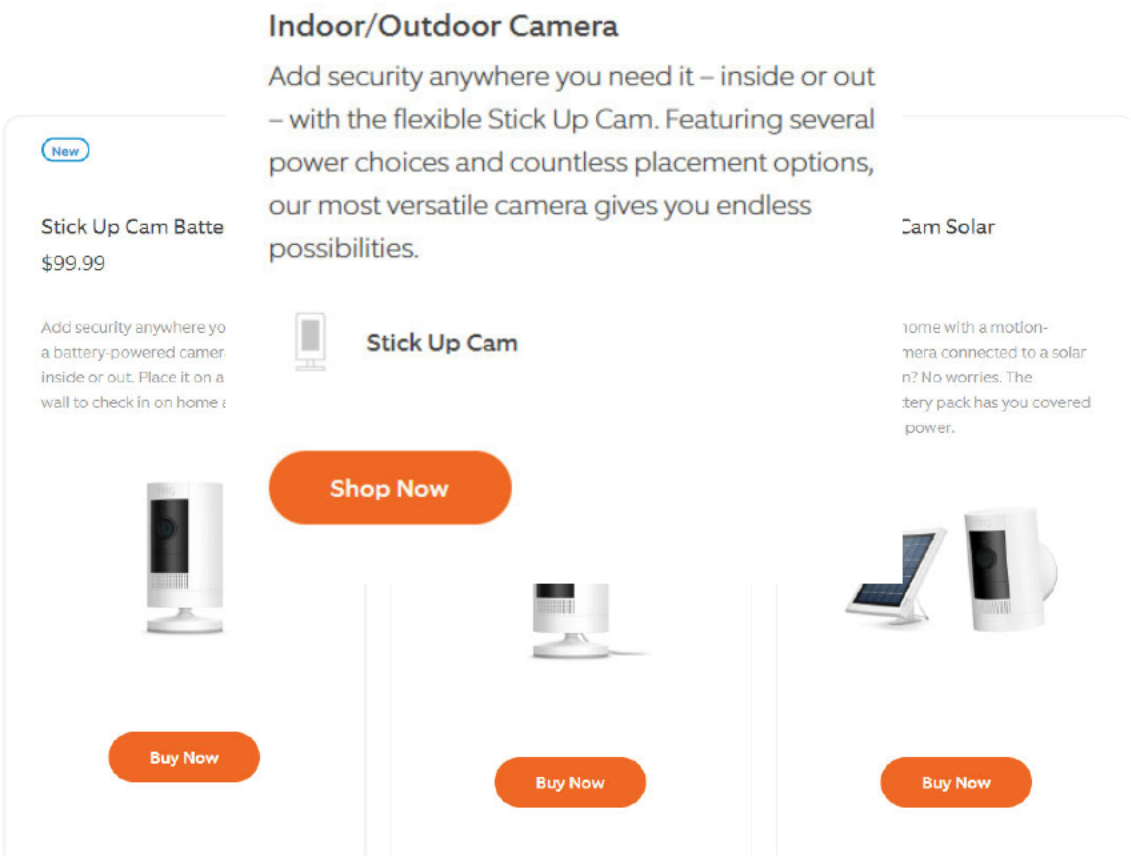
385. For example, an advertisement for Ring's "Indoor Cams" around the time of the hacking incidents invited users to "start protecting your home, and family, with a small, sleek, and discreet Indoor Cam by Ring." Ring claims that the "Indoor Cam" allows users to "bring security indoors" to achieve "peace of mind":



386. At that same time, Ring also claimed that the Indoor Cam allows users to "bring protection inside":

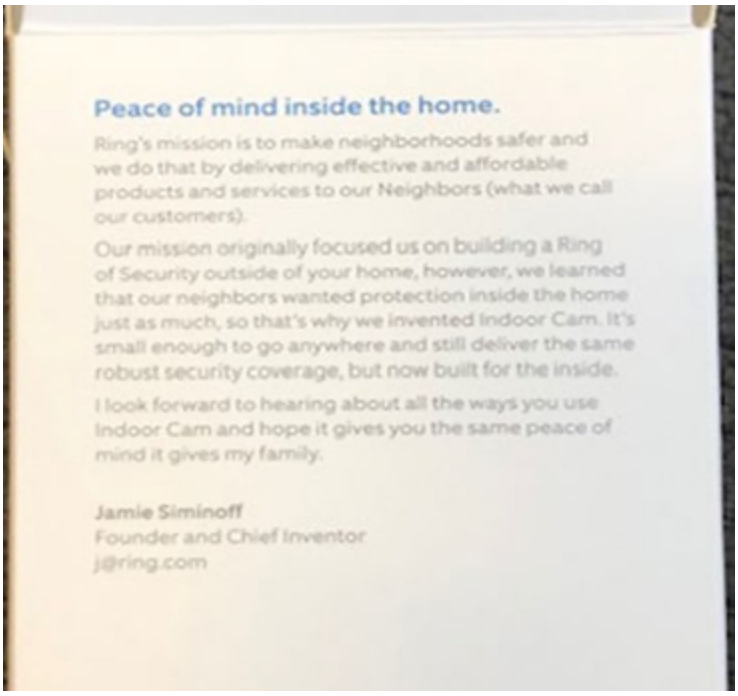
387. Similarly, Ring claimed that the Stick Up Cam lets users "add security anywhere they need it"[36]:

[36] <https://shop.ring.com/pages/security-cameras>



388. Ring invited users to "add security anywhere you need it," "protect your home," and "watch over home" with the Stick Up Cam:

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



Peace of mind inside the home.

Ring's mission is to make neighborhoods safer and we do that by delivering effective and affordable products and services to our Neighbors (what we call our customers).

Our mission originally focused us on building a Ring of Security outside of your home, however, we learned that our neighbors wanted protection inside the home just as much, so that's why we invented Indoor Cam. It's small enough to go anywhere and still deliver the same robust security coverage, but now built for the inside.

I look forward to hearing about all the ways you use Indoor Cam and hope it gives you the same peace of mind it gives my family.

Jamie Siminoff
Founder and Chief Inventor
j@ring.com

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

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

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

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

394. Unlike other companies that use online accounts, as of the dates the Plaintiffs purchased their Ring devices, Ring did not require basic, industry-standard measures to protect the security of users' accounts. And instead of following any

industry standard practices or providing customers clear channels of remediation, Ring places the blame for the data breach on their own users.

395. Ring devices have extremely sensitive data—*live footage adjacent to and often within the home*—at their disposal. This means that Ring should be *especially* careful with account information, not just employ basic account protections.

396. Password security depends significantly on how platforms store credentials or how vulnerable the platform is to breaches and leaks. Web platforms can make a hacker's job more difficult by locking accounts after a certain number of failed attempts, encrypting passwords, reducing login attempt rates, or using salt hashing.

397. Best practices in website security provide a few basic guidelines. First, numerous subsequent failed attempts on an account should result in extra scrutiny for logging in to that account. This may include limiting the number of attempts or locking the account until the owner can be contacted. Second, when a password is chosen for an account, this should go through some form of scrutiny: checking whether it is in a list of known compromised passwords and ensuring that it is sufficiently complex. Third, account holders should be able to see (and audit) the list of devices that have logged in to their account. Finally, companies should encourage users to enable two-factor authentication in their account settings.

398. Two-factor (or dual factor) authentication is a common, industry-standard security feature in which the user provides two different authentication factors to verify themselves to better protect the user's credentials. Two-factor authentication provides higher security than single-factor authentication, in which a user can provide only a password to access an account. Although Ring offers two-factor authentication, it did not require it, or even prompt users to enable it, until *after* national and international news media reported on the hacks described in this Complaint and in similar cases filed.

399. Additionally, Ring did not have security protocols in place to notify users when someone logs into their account from a new device or an unrecognized IP address.

Whereas most companies request confirmation from the accountholder before allowing a suspicious sign-in to occur, Ring let it happen with no questions asked.

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

401. In December 2019, security professionals from the website Motherboard tested Ring's security procedures.[37] The testers logged into the Ring app from the United States, United Kingdom, Spain, and Singapore, in some cases simultaneously and from various devices and browsers that had never been used to log into the platform before. At no point did Ring trigger any alert, such as an email notification or text message, to the accountholder to alert them of suspicious logins or check whether the logins were legitimate.

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

403. Ring also offered no protection against repeated, automated attempts to login to its services. It was well known across the security industry that hackers can use software to rapidly check whether email and password combinations will grant access to a Ring account. Hackers typically use lists of already compromised combinations from other services. Standard security measures would include a procedure for

[37] 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>.

preventing someone from using software to rapidly check these account combinations after too many incorrect requests to login, by, for example, temporarily blocking access; marking their IP address as suspicious; or presenting a CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) check to ensure that the user is a human rather than an automated program.

404. Ring does not offer these standard measures.

405. Ring also offered no protection against repeated attempts to try new password combinations with known email addresses, sometimes called "brute force entry." In a brute force attack, a hacker uses a rapid trial and error approach to guess the correct password, PIN, or encryption keys. It does not require a lot of intellect or complex algorithms – it's merely a guessing game. It is well known across the industry that hackers can use bots or other software to rapidly enter combinations of letters, numbers, and symbols into the password field, essentially guessing at an endless string of attempted passwords. Most online accounts will lockout a user after three to five incorrect password attempts. But Ring allows hackers (and hacker software) to try as many passwords as they want without locking them out.

406. Furthermore, most websites also add extra security steps such as password hashing and encryption to protect customer information meaning passwords are never saved in plain text. So even if they do leak, hackers will need to go through an astronomical number of attempts to guess the encryption key and get a password.[38]

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

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

[38] 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>.

409. Furthermore, Ring has demonstrated a pattern of being negligent in enforcing even basic web application security controls. In February 2019, it was discovered that Ring sent video feeds to their cloud providers completely unencrypted.[39] This is particularly problematic because video footage is extremely easily accessible for misuse. The quintessential illustration occurred within Ring itself. In January of 2020, Ring admitted that it had fired employees who improperly accessed Ring users' video data. And at least one Ring employee reassigned a user's account—Mr. Mariutto's—to a stranger.

410. Ring's failings were recognized by the broader tech community. CNET reported that the combination of Ring's own privacy and security issues led them to remove all of Ring's products from CNET's recommendations for 2019.[40]

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

412. All Plaintiffs and Purchaser/Accountholder Class members were harmed as a result of Ring's failure to safeguard privacy and their practice of sharing their PII with third parties.

---

[39] Cory Doctrow, *Bad security design made it easy to spy on video doorbells and insert fake video into their feeds*, BoingBoing (Feb. 28, 2019), <https://boingboing.net/2019/02/28/recon-mode-active-mode.html>.

[40] Megan Wollerton, Ring's new privacy and security features prove that hardware isn't the only important thing, CNET (July 29, 2020), <https://www.cnet.com/news/rings-new-privacy-and-security-features-prove-that-hardware-isnt-the-only-important-thing/>.

J. Ring owed a duty to Plaintiffs to protect their privacy and secure their sensitive account information and access.

413. Ring still has not disclosed the identity of the hacker(s) who threatened the Hacked Families Class members. Nor has Ring confirmed how the unauthorized access occurred.

414. While the precise mechanics of the hack are known only to the hacker(s) and to Ring, it is clear the hacker(s) were able to access the Hacked Families Class members' Ring accounts because Ring did not adopt industry-standard security procedures designed to prevent such access.

415. All Plaintiffs had a special relationship with Ring. Ring provided services to the Plaintiffs, including the ability to monitor their indoor security device via their Ring accounts. The transaction between Ring, on the one hand, and Plaintiffs, on the other, was intended to benefit the Plaintiffs by providing them the ability to use the devices for all of the purposes they expected and which Ring intended.

416. It was entirely foreseeable to Ring that Plaintiffs would be harmed if Ring failed to adequately safeguard access to their Ring accounts and security devices.

417. But for Ring's acts and omissions in maintaining deficient and inadequately protected systems, and allowing hackers to gain access to customer accounts, the Hacked Families' devices would not have been taken over or their homes spied on. They would not have been harassed and exposed to an imminent risk of theft or fraud.

418. Ring knew before selling its devices that they were susceptible to third party intrusion. Ring received further notice of these defects when other Ring users' accounts were hacked around the same time period as the horrific incidents suffered by the Hacked Families.

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

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

421. The injury to the Hacked Families, and to the other Plaintiffs, was reasonably foreseeable as a result of Ring's failure to exercise reasonable care in safeguarding their account information.

V. CLASS ALLEGATIONS

422. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3), all Purchaser/Accountholder Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class:

> **Accountholder Class:** All persons who purchased a Ring security device of any kind from Ring LLC and/or created a Ring account during the applicable limitations period.

423. Pursuant to Federal Rule of Civil Procedure 23(c)(4), the Hacked Families, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Classes, for a liability determination with damages to be determined on an individual basis:

> **Purchaser Hacked Families Class:** All persons who were victims of hacking of a Ring account during the applicable limitations period, and who have purchased a Ring product and/or created a Ring account.
>
> **Non-Purchaser Hacked Families Class:** All persons who were victims of hacking of a Ring account during the applicable limitations period, and who have not purchased a Ring product or created a Ring account.

424. While some of the Purchaser Hacked Families are members of the Accountholder Class and the Purchaser Hacked Families Class, the Purchaser Hacked Families request that the Court name them as Class Representatives on behalf of the Purchaser Hacked Families Class only. Similarly, the Accountholder Plaintiffs request that the Court name them as Class Representatives on behalf of the Accountholder Class only.

425. Excluded from the Classes[41] are any entities, including Ring, and Ring's officers, agents, and employees. Also excluded from the Classes are counsel for Plaintiffs, any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

426. Members of the Classes are so numerous that joinder is impracticable. While the exact number of members of each Class is unknown to Plaintiffs, it is believed that each Class is comprised of dozens, if not thousands, of members.

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

a. Whether Ring violated Plaintiffs' and Class Members' privacy rights;

b. Whether Ring failed to safeguard adequately Plaintiffs' and Class Members' property, including their private and personal information;

[41] The Purchaser/Account Holder Class, Purchaser Hacked Families Class, and Non-Purchaser Hacked Families Class are collectively referred to as the "Classes." The Purchaser/Account Holder Class and Purchaser Hacked Families Class are collectively referred to as the "Purchaser Classes" and their respective class representatives as "Purchaser Plaintiffs." The Purchaser Hacked Families Class and Non-Purchaser Hacked Families Class are collectively referred to as the "Hacked Families Classes."

c. Whether Ring's collection and storage of Plaintiffs' and Class Members' private and personal information in the manner alleged herein violated federal, state, and local laws, or industry standards;

d. Whether Ring's disclosure of Plaintiffs' and Class Members' private and personal information in the manner alleged herein violated federal, state, and local laws, or industry standards;

e. Whether Ring acted negligently;

f. Whether Plaintiffs and the Class Members were harmed;

g. Whether Ring and Plaintiffs formed implied contracts;

h. Whether Ring breached implied contracts with Plaintiffs and the Class Members;

i. Whether Ring's conduct was unfair;

j. Whether Ring's conduct was fraudulent;

k. Whether Plaintiffs and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and

l. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

428. In addition to the above, common and legal factual questions for the Hacked Families Classes include:

a. Whether Ring allowed hackers to access the Hacked Families Class members accounts;

b. Whether Ring's acts, practices, and omissions complained of herein amount to egregious breaches of social norms;

c. Whether Ring failed to protect or otherwise adequately safeguard the Hacked Families Class members' homes, including their private and sensitive information, as promised; and

d. Whether Ring intruded upon the Hacked Families Class members' seclusion.

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

430. 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.

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

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

433. Ring has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Classes as a whole.

434. Plaintiffs suffer a substantial and imminent risk of repeated injury in the future.

435. California law applies to the claims of all members of the Classes

436. The State of California has sufficient contacts to Ring's relevant conduct

for California law to be uniformly applied to the claims of the Classes. Application of California law to all relevant Class Member transactions comports with the Due Process Clause given the significant aggregation of contacts between Ring's conduct and California.

437. Ring is headquartered and does substantial business in California.

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

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

440. California has a greater interest than any other state in applying its law to the claims at issue in this case. California has a very strong interest in preventing its resident corporations from engaging in unfair and deceptive conduct and in ensuring that harm inflicted on resident consumers is redressed. California's interest in preventing unlawful corporate behavior occurring in California substantially outweighs any interest of any other state in denying recovery to its residents injured by an out-of-state defendant or in applying its laws to conduct occurring outside its borders. If other states' laws were applied to Class Members' claims, California's interest in deterring resident corporations from committing unfair and deceptive practices would be impaired.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

441. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

442. Ring owed Purchaser Plaintiffs and the members of the Purchaser Classes a duty to exercise reasonable care in safeguarding and protecting access to their Ring accounts and keeping them from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

443. This duty included, among other things, designing, maintaining, and testing security systems to ensure that users' account information is adequately secured and protected. Ring's duty to Purchaser Plaintiffs and the members of the Purchaser Classes arose from the sensitivity of the information and privacy rights that Ring's devices were designed to secure and protect. This duty further arose because Ring affirmatively designed, developed, maintained, and provided the Ring products and services to its customers, who were the foreseeable victims of negligence in the design, development, and maintenance of Ring's products and services.

444. Ring's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable data security measures to protect consumers. Various FTC publications and data security breach orders further form the basis of Ring's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) were intended to guard against.

445. Ring breached its duty to Purchaser Plaintiffs and the members of the Purchaser Classes when it allowed unauthorized users to access their accounts, when it failed to implement and maintain reasonable security protections and protocols, and when it knowingly shared and/or sold customers' PII to third parties for analytics and marketing purposes without adequate disclosure to and consent from its customers.

446. Ring, a sophisticated tech company, knows what the industry-standard security practices are, but chose not to implement them.

447. As a result of Ring's breaches, the Purchaser Hacked Families Class members suffered serious injuries when unauthorized third parties were able to access their Ring accounts. The Purchaser Hacked Families and the members of the Purchaser Hacked Families Class were deprived of their privacy rights and the related value of keeping their likenesses and personal information private and not disseminated publicly, including on platforms like Discord and the dark web. The Purchaser Hacked Families and the members of the Purchaser Hacked Families Class also experienced anxiety, emotional distress, loss of privacy, and loss of time investigating and mitigating the effects of the hack, and are at an increased risk of future harm. And all Purchaser Plaintiffs suffered injury due to Ring's breaches because they incurred expenses associated with purchasing, installing, creating accounts for, and using the insecure devices in and around their homes. It was entirely foreseeable to Ring that Purchaser Plaintiffs and the members of the Purchaser Classes would be harmed if it failed to adequately safeguard access to their Ring accounts and security devices. Failure to protect their Ring accounts and access to their security devices was likely to result in injury to Purchaser Plaintiffs and the members of the Purchaser Classes because hackers could gain unauthorized access to private information about their lives, spy on them, harass them, threaten them, endanger them, and commit financial fraud or theft using information learned through the unauthorized access.

448. There is a close connection between Ring's failure to adequately safeguard access to the Ring accounts of the members of the Purchaser Classes and the injuries suffered by them.

449. But for Ring's acts and omissions in maintaining inadequate security, and allowing hackers to gain access to customer accounts, the Purchaser Hacked Families and the Purchaser Hacked Families Class members' devices would not have been taken over, their homes spied on, and loved ones harassed. This close connection is further reinforced by the broader general evidence of hacks of others' Ring devices occurring around the same time period as the hack of Purchaser Plaintiffs' devices.

450. Further, but for Ring's disclosure and/or sale of PII to third parties for analytics and marketing purposes without disclosure and consent, the Accountholder/Purchaser Plaintiffs' and the Accountholder/Purchaser Class Members' PII and privacy rights would not have been compromised.

451. Ring's conduct also involves moral blame. Aware of the vulnerability of its customers, and the sensitive nature of the information available to anyone who watches an indoor camera security feed, Ring has not taken sufficient actions to prevent hackers from gaining unauthorized access. Ring was aware of the problems with its security systems and that they were vulnerable to intrusion by hackers because these issues were widely covered in the media. There was even a podcast dedicated to entertaining subscribers by hacking and harassing Ring customers through their devices. But even though Ring was aware of the vulnerability of its customers to being hacked through its accounts and devices, Ring failed to cure those vulnerabilities or protect its customers' accounts.

452. Purchaser Plaintiffs and the members of the Purchaser Classes enjoy a special relationship with Ring. Ring provided services to Purchaser Plaintiffs and members of the Purchaser Classes, including the ability to monitor their indoor security devices via their Ring accounts. The transactions between Ring and the members of both Classes are intended to benefit Purchaser Plaintiffs and the members of the Purchaser Classes by providing them the ability to use the indoor devices for all of the purposes they expected and Ring intended.

453. Purchaser Plaintiffs and the members of the Purchaser Classes were harmed by Ring's failure to exercise reasonable care in safeguarding their account information, and that harm was reasonably foreseeable.

COUNT II
Violation of California Unfair Competition Law ("UCL")
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

454. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

455. Purchaser Plaintiffs have standing to pursue this cause of action because Purchaser Plaintiffs suffered injury in fact and lost money as a result of Ring's misconduct described herein.

456. As described herein, Ring advertised their products and services as enhancing security and safety, but in fact provided products and services that were highly vulnerable to hacking and that worsened the safety and security of Purchaser Plaintiffs and the members of the Purchaser Classes.

457. Purchaser Plaintiffs would continue using their Ring products and services if they could be assured that Ring would take adequate security measures to protect the security of their accounts and devices going forward.

458. 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. Ring has engaged in business acts and practices that, as alleged above, constitute unfair competition in violation of Business and Professions Code section 17200.

Unlawful

459. Ring's business practices, as alleged herein, violate the "unlawful" prong because Ring violates Purchaser Plaintiffs' and the Purchaser Classes Members' rights to privacy and state laws, including Article 1, Section 1 of the California Constitution, and the California Consumers Legal Remedies Act.

Unfair

460. Ring's business practices, as alleged herein, violate the "unfair" prong of the UCL because they offend an established public policy and are immoral, unethical, and unscrupulous or substantially injurious to consumers.

461. Purchaser Plaintiffs and the members of the Purchaser Classes have a well-established right to privacy and well-established privacy interests in their homes and in their sensitive personal information. Ring's failure to implement and maintain adequate security protocols, and its disclosure and/or sale of customers PII to third

parties without their permission or consent, violated those interests and substantially injured them.

462. The reasons, justifications, or motives that Ring may offer for the acts and omissions described herein are outweighed by the gravity of harm to the victims. The injuries suffered by Purchaser Plaintiffs and the members of the Purchaser Classes are substantial and are not outweighed by any countervailing benefits to consumers or competition.

Fraudulent

463. Ring's acts, as described herein, are "fraudulent" because they are likely to deceive the general public.

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

465. As a result of Ring's unlawful, unfair, and fraudulent business practices, Purchaser Plaintiffs and the members of the Purchaser Classes suffered injury, including paying a price premium for an insecure product and service.

466. If Ring is permitted to continue to engage in the unfair and fraudulent business practices described above, its conduct will engender further injury, expanding the number of injured members of the public beyond its already large size, and will tend to render any judgment at law, by itself, ineffectual. Under such circumstances, Purchaser Plaintiffs and the members of the Purchaser Classes have no adequate remedy at law in that Ring will continue to engage in the wrongful conduct alleged herein, thus engendering a multiplicity of judicial proceedings. Purchaser Plaintiffs and

the members of the Purchaser Classes request and are entitled to injunctive relief, enjoining Ring from engaging in the unfair and fraudulent acts described herein.

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

COUNT III
Breach of Implied Contract
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

468. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

469. Ring sold devices to Plaintiffs and the members of the Purchaser Classes. In exchange, Ring received benefits in the form of monetary payments. Plaintiffs and the members of both Classes also created Ring accounts, providing Ring with their valuable personal data and, in some cases, money in exchange for upgraded subscription services.

470. Ring has acknowledged these benefits and accepted or retained them.

471. Implicit in the exchange of the devices for the monetary payments and the exchange of personal data for Ring accounts required to use those devices is an agreement that Ring would provide devices suitable for their purpose—providing home security—and not designed with flaws that render them vulnerable to hacking and therefore inadequate to provide safety and security.

472. Without such implied contracts, Purchaser Plaintiffs and the members of the Purchaser Classes would not have paid for and conferred benefits on Ring, but rather would have chosen an alternative security system that did not present such dire hidden safety risks or implement third party software enabling surveillance of activity within their own homes.

473. Purchaser Plaintiffs and the members of the Purchaser Classes fully performed their obligations under their implied contracts with Ring, but Ring did not.

474. Ring breached its implied contracts with Purchaser Plaintiffs and the Purchaser Classes Members by failing to acknowledge and repair the inherent vulnerabilities in their accounts and devices and by willfully violating customer privacy interests by disclosing personal data to third parties without full disclosure or consent. These circumstances are such that it would be inequitable for Ring to retain the benefits received.

475. As a direct and proximate result of Ring's breach of its implied contracts with Purchaser Plaintiffs and the members of the Purchaser Classes, Purchaser Plaintiffs and the members of the Purchaser Classes have suffered and will suffer injury, including paying a price premium for an insecure product and service.

COUNT IV
Unjust Enrichment
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

476. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein, and to the extent necessary, assert this count in the alternative to their breach of implied contract claim.

477. Ring has profited and benefited from the purchase of its devices by Purchaser Plaintiffs and the members of the Purchaser Classes.

478. Ring has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Purchaser Plaintiffs and the members of the Purchaser Classes did not receive products of the quality, nature, fitness, or value represented by Ring and that reasonable consumers expected.

479. Ring has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Purchaser Plaintiffs and the members of the Purchaser Classes.

480. Equity and justice militate against permitting Ring to retain these profits and benefits.

481. Purchaser Plaintiffs and the members of the Purchaser Classes suffered injury as a direct and proximate result of Ring's unjust enrichment and seek an order directing Ring to disgorge these benefits and pay restitution to Purchaser Plaintiffs and the members of the Purchaser Classes.

COUNT V
Invasion of Privacy (Intrusion Upon Seclusion) and Violation of the California Constitution, Art. 1, § 1 (On behalf of the Purchaser Hacked Families Class)

482. The Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

483. The Purchaser Hacked Families and the Purchaser Hacked Families Class members have reasonable expectations of privacy in their homes. This interest is protected by Article 1, Section 1 of the California Constitution.

484. The Purchaser Hacked Families and the Purchaser Hacked Families Class members' privacy interest as described herein is legally protected because they have an interest in precluding the dissemination or misuse of sensitive information and an interest in making intimate personal decisions and conducting personal activities without observation, intrusion, or interference.

485. Ring intruded on the Purchaser Hacked Families' and the Purchaser Hacked Families Class's solitude, seclusion, and private affairs when it allowed their Ring account information to be compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

486. Ring knew before selling its devices that they were susceptible to unauthorized third-party intrusion. Ring received further notice of these defects when other Ring users' accounts were hacked around the same time period as the horrific incidents suffered by the Hacked Families.

487. Ring declined to adopt sufficient security measures to protect the Purchaser Hacked Families and the Purchaser Hacked Families Class; indeed, Ring chose not to implement even ordinary, commonplace security measures and instead

adopted dismal security features that permitted hackers to easily access user accounts. As a result of Ring's acts, hackers have been able to gain access to Ring users' devices and spy on them inside of their homes.

488. Ring's failure to protect its customers' accounts and security is highly offensive to a reasonable person. Ring accounts grant access to exceptionally intimate and private parts of someone's life: the inside of their homes, sometimes their bedrooms. Reasonable persons would expect, and the Purchaser Hacked Families and the Purchaser Hacked Families Class did expect, that Ring would properly safeguard their accounts and information. The Purchaser Hacked Families and the Purchaser Hacked Families Class entrusted Ring with this highly sensitive access, and Ring's failure to properly safeguard it is an egregious violation of societal norms.

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

490. The Purchaser Hacked Families and the Purchaser Hacked Families Class were harmed by the intrusion into their private affairs as detailed herein. The Purchaser Hacked Families and the members of the Purchaser Hacked Families Class were deprived of their privacy rights and the related value of keeping their likenesses and personal information private and not disseminated publicly, including on platforms like Discord and the dark web. The Purchaser Hacked Families and the members of the Purchaser Hacked Families Class also experienced anxiety, emotional distress, loss of privacy, loss of time investigating and mitigating the effects of the hack, and are at an increased risk of future harm.

491. Ring's actions and omissions described herein were a substantial factor in causing the harm suffered by the Purchaser Hacked Families and the Purchaser Hacked Families Class.

492. As a result of Ring's actions, the Purchaser Hacked Families and the Purchaser Hacked Families Class seek damages, including compensatory, nominal, and punitive damages, in an amount to be determined at trial.

COUNT VI
Invasion of Privacy (Public Disclosure of Private Facts) and Violation of the California Constitution, Art. 1 § 1
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

493. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written.

494. In the alternative, the Purchaser Hacked Families and the Purchaser Hacked Families Class re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

495. Purchaser Plaintiffs and the members of the Purchaser Classes have reasonable expectations of privacy in their homes. This interest is protected by Article 1, Section 1 of the California Constitution.

496. The privacy interests as described herein are legally protected because Purchaser Plaintiffs and the members of the Purchaser Classes have an interest in precluding the dissemination or misuse of sensitive information and an interest in making intimate personal decisions and conducting personal activities without observation, intrusion, or interference.

497. Ring declined to adopt sufficient security measures to protect Purchaser Plaintiffs and the Purchaser Class Members; indeed, Ring chose not to implement even ordinary, commonplace security measures and instead adopted dismal security features that permitted hackers to easily access user accounts. As a result of Ring's acts, hackers have been able to gain access to Ring users' devices, including the devices belonging

to the Purchaser Hacked Families and the Purchaser Hacked Families Class, and spy on them inside of their homes.

498. Ring knew before selling its devices that they were susceptible to unauthorized third-party intrusion. Ring received further notice of these defects when other Ring users' accounts were hacked around the same time period as the horrific incidents suffered by the Hacked Families.

499. Ring's acts and omissions caused the exposure and publicity of intimate details of the Purchaser Hacked Families' and the Purchaser Hacked Families Class's private lives—matters that are of no concern to the public.

500. Ring's failure to protect its customers' accounts and security from exposure by and to unauthorized third parties is highly offensive to a reasonable person. Ring accounts grant access to exceptionally intimate and private parts of someone's life: the inside of their homes, sometimes their bedrooms. Reasonable persons would expect, and the Purchaser Hacked Families and the Purchaser Hacked Families Class did expect, that Ring would properly safeguard their accounts and information. The Purchaser Hacked Families and the Purchaser Hacked Families Class entrusted Ring with this highly sensitive access, and Ring's failure to properly safeguard it is an egregious violation of societal norms

501. The disclosure and exposure that Ring's acts and omissions caused are highly offensive to a reasonable person. Ring's actions alleged herein are particularly egregious because through these actions, Ring represents that it cares about and prioritizes security, is aware of the vulnerability of their customers and is aware of the sensitive nature of the information available to anyone who watches an indoor camera security feed, yet it has done nothing to prevent hackers from gaining unauthorized access and have refused to take responsibility. In fact, Ring chose to implement security measures that were deficient and made it easy for hackers to obtain access to user accounts.

502. Purchaser Plaintiffs and the members of the Purchaser Classes have reasonable expectations of privacy in their personal identifying information. Yet, Ring disclosed their personal and private information to unauthorized parties without the informed and clear consent of Purchaser Plaintiffs and the Purchaser Class members.

503. As a direct and proximate result of Ring's unlawful privacy invasions, Purchaser Plaintiffs' and the Purchaser Class members' private, personal, and confidential information was unlawfully disclosed to third parties without their permission or consent. Purchaser Plaintiffs and the Purchaser Class members suffered injury as a result of these invasion.

504. Purchaser Plaintiffs and the members of the Purchaser Classes were harmed by the public disclosure of their private affairs as detailed herein.

505. Ring's actions described herein were a substantial factor in causing the harm suffered by Purchaser Plaintiffs and the members of the Purchaser Classes.

506. As a result of Ring's actions, Purchaser Plaintiffs and the members of the Purchaser Classes seek damages, including compensatory, nominal, and punitive damages, in an amount to be determined at trial.

COUNT VII

Violation of the Consumers Legal Remedies Act
Cal. Civ. Code § 1770
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

507. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

508. Ring engages in practices that violate the Consumers Legal Remedies Act ("CLRA"), Civil Code § 1770, *et seq.*, specifically unfair, deceptive, unlawful, and unconscionable commercial practices in connection with the sale of its security devices to consumers.

509. Ring is a "person" under Cal. Civ. Code § 1761.

510. Purchaser Plaintiffs and the Purchaser Class Members are "consumers" as defined by Civil Code § 1761(d).

511. Ring's security devices are "goods" within the meaning of Civil Code § 1761(a).

512. The practices engaged in by Ring that violate the CLRA include, *inter alia*:

a. Representing that the Ring security devices are suitable for home security and protection when in fact they contain significant flaws and vulnerabilities, and inadequate security features, and do not protect users' sensitive and private information;

b. Advertising Ring security devices as suitable for home security and protection when in fact they contain significant flaws and vulnerabilities, and inadequate security features, and do not protect users' sensitive and private information;

c. Representing that Ring will safeguard users' personal and private information, when in fact it did not do so; and

d. Representing that Ring will safeguard users' personal and private information when in fact it discloses their PII to third parties without their consent.

See Civ. Code §§ 1770(a)(5), (7), (9), (14), and (16).

513. Ring's advertisement, packaging, and representations contained deceptive statements that Ring's products "bring security indoors," "bring protection inside," give families "peace of mind," provide "robust security coverage," add "security," and protect your home," among other representations relating to privacy, safety, and security.

514. Ring's advertisements and representations concealed and failed to disclose that Ring's products were insecure and vulnerable to intrusion and access by third parties.

515. Ring also concealed and failed to disclose that Ring shares its customers' PII to third parties without their consent.

516. These misrepresentations and omissions were misleading and deceptive.

517. Ring induced consumers to buy Ring products it made and disseminated, and caused to be made and disseminated, from California, misrepresentations and omissions that were untrue and misleading.

518. Ring knew or should have known that its misrepresentations and/or omissions were false and misleading, and intended for consumers to rely on such misrepresentations and omissions.

519. The misrepresentations and omissions were likely to, and did, deceive reasonable consumers, including Purchaser Plaintiffs. Reasonable consumers, including Purchaser Plaintiffs, would have found it material to their purchasing decisions that Ring's products were insecure, did not have adequate safety and security protections, did not have common-sense, industry-standard security protections, and were vulnerable to hacking and intrusion by third parties. Reasonable consumers, including Purchaser Plaintiffs, would have found it material that Ring shares consumers' PII with third parties without their consent. Knowledge of these facts would have been a substantial factor in Purchaser Plaintiffs' and the members of the Purchaser Classes' decision to purchase Ring's products.

520. Ring's conduct was likely to, and did, deceive reasonable consumers, including Purchaser Plaintiffs. Reasonable consumers, including Purchaser Plaintiffs, would find it material to their purchasing decisions that Ring's products were insecure, did not include adequate security and privacy protections, were vulnerable to hacking and intrusion, and would result in their PII being shared with third parties.

521. Ring owed Purchaser Plaintiffs and the members of both Classes a duty to disclose these facts because they were known and/or accessible exclusively to Ring (and potentially other unnamed parties other than Purchaser Plaintiffs and the Purchaser Class Members), who had exclusive and superior knowledge of Ring's security practices, protocols, and features; because Ring actively concealed them; because Ring intended for consumers to rely on its misrepresentations and omissions; and because its products pose a risk to the health and safety of consumers.

522. In purchasing Ring's product, each of Purchaser Plaintiffs relied on the misrepresentations or omissions by Ring. Reasonable consumers would have been expected to rely on those misrepresentations and omissions.

523. As a result of Ring's violations, Plaintiffs and the members of both Classes suffered ascertainable monetary losses. They would not have incurred these losses but for Rings' unlawful practices. Ring's conduct actually and proximately caused actual damages to Purchaser Plaintiffs and the Purchaser Class Members. Absent Ring's unfair and fraudulent conduct, Purchaser Plaintiffs and the Purchaser Class Members would have behaved differently and would not have purchased Ring's products or would have paid less for them. Ring's misrepresentations and omissions induced Purchaser Plaintiffs to purchase products they would not have otherwise purchased and enter into contracts they would not have otherwise entered into.

524. In accordance with Cal. Civ. Code § 1782(a), Purchaser Plaintiffs have served Ring with notices of these CLRA violations by certified mail, return receipt requested. Ring has received Purchaser Plaintiffs' notices but has failed to provide any relief within 30 days of receipt.

525. Purchaser Plaintiffs seek, on behalf of themselves and the Purchaser Classes, restitution, damages, and injunctive relief, as well as any other such relief the Court may deem just and proper.

COUNT VIII

Breach of the Implied Warranty of Merchantability
(On behalf of Purchaser Plaintiffs and the Purchaser Classes)

526. Purchaser Plaintiffs re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

527. Ring is a manufacturer and seller, as it designed, assembled, fabricated, produced, constructed, and prepared its products (combined in one as hardware and software) before they were sold. Ring is a seller because it was a manufacturer, wholesaler, and distributor engaged in the business of selling a product for use and

resale with actual knowledge that its products contain significant flaws, vulnerabilities, and inadequate security features, and that they do not protect users' sensitive and private information.

528. Ring impliedly warranted that its products (both hardware and software), which it designed, manufactured, and sold to Purchaser Plaintiffs and the members of the Purchaser Classes, were merchantable, fit, and safe for their ordinary use, not otherwise injurious to consumers, and equipped with adequate warnings.

529. Ring did not effectively disclaim this implied warranty.

530. Ring's products were defective at the time Ring sold them to Purchaser Plaintiffs and members of the Purchaser Classes. Ring breached its implied warranty of merchantability, in that, among other things, its products were not safe, merchantable, and reasonably suited for the ordinary purposes for which they were sold.

531. Ring, both directly and through authorized resellers, sold its products to Purchaser Plaintiffs and members of the Purchaser Classes.

532. Purchaser Plaintiffs were persons whom Ring reasonably would have expected to purchase its products.

533. Purchaser Plaintiffs relied upon Ring's implied warranty that the products they purchased were of merchantable quality. Yet Ring's products contain significant flaws, vulnerabilities, and inadequate security features, and they do not protect users' sensitive and private information, such that they are not merchantable and are unfit for their intended purpose of providing home security and protecting consumers' privacy in their homes.

534. Ring placed its products in the stream of commerce and expected them to reach consumers without substantial change in the condition in which they were sold. Indeed, Purchaser Plaintiffs as purchasers of Ring's products, are consumers who would reasonably be expected to use Ring's products and be affected by their

performance without substantial change in the condition in which they were sold by Ring.

535. Ring's products are defective such that, when used by Purchaser Plaintiffs and members of the Purchaser Classes as intended and in a foreseeable and reasonable manner, they fail to provide home security and protect consumers' personal information and privacy.

536. Ring's products did in fact fail to provide security and protect the privacy of Purchaser Plaintiffs and members of the Purchaser Classes as alleged above.

537. Ring knew or should have known of its products' defective design and/or manufacture and, as a result, that the products were dangerous and unfit for their intended use.

538. Ring did not warn or alert purchasers or users of the foregoing defects and dangers, despite its knowledge of them.

539. As a direct and proximate result of these failures, Purchaser Plaintiffs have sustained injuries, damages, and loss, including paying a price premium for an insecure product and service.

540. Ring is liable to Purchaser Plaintiffs and members of the Purchaser Classes for damages caused by Ring's breach of its implied warranty of merchantability in an amount to be proven at trial.

COUNT IX
Negligence

(On behalf of the Non-Purchaser Hacked Families Class)

541. The Non-Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

542. Ring owed the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class a duty to exercise reasonable care in safeguarding and protecting access to the Ring security device on which their private

information and likeness appeared and keeping such private information and likeness from being compromised, lost, stolen, misused, and/or publicly disclosed.

543. This duty included, among other things, designing, maintaining, and testing security systems to ensure that account information is adequately secured and protected. Ring's duty to the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class arose from the privacy rights that Ring's devices were designed to secure and protect. This duty further arose because Ring affirmatively designed, developed, maintained, and provided the Ring products and services to its customers.

544. This duty also arose because Ring affirmatively encouraged its customers to use its products inside their homes. For example, an advertisement for Ring's "Indoor Cams" around the time of the hacking incidents invited users to "start protecting your home, and family, with a small, sleek, and discreet Indoor Cam by Ring." Ring claimed that the "Indoor Cam" allows users to "bring security indoors" to achieve "peace of mind." Ring knew that as a result of its encouragement of the use of its products inside the home, it possessed not only the sensitive information of its customers, but also the sensitive information of its customers' families—including minor children—that would be passively exposed to the Ring devices that their guardians purchased and used. Ring's customers' family members—including minor children—were therefore the foreseeable victims of negligence in the design, development, and maintenance of Ring's products and services. Ring had a duty to take reasonable data security measures to prevent such foreseeable harm.

545. Ring breached its duty to the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class when it allowed unauthorized access to the Hacked Families' accounts and when it failed to implement and maintain reasonable security protections and protocols.

546. Ring, a sophisticated tech company, knows what the industry-standard security practices are, but chose not to implement them.

547. As a result of Ring's breaches, the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class suffered serious injuries when unauthorized third parties were able to access their families' Ring accounts. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class were deprived of their privacy rights and the related value of keeping their likenesses and personal information private and not disseminated publicly, including on platforms like Discord and the dark web.

548. It was entirely foreseeable to Ring that the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class would be harmed if it failed to adequately safeguard access to their families' Ring accounts and security devices. Failure to protect their families' Ring accounts and access to their security devices was likely to result in injury to the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class because hackers could gain unauthorized access to private information about their lives, spy on them, harass them, threaten them, endanger them, use and disseminate their private information and likeness without their authorization, and commit financial fraud or theft using information learned through the unauthorized access.

549. There is a close connection between Ring's failure to adequately safeguard access to the Ring accounts of the families of the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class and the injuries suffered by them.

550. But for Ring's acts and omissions in maintaining inadequate security, and allowing hackers to gain access to their families' accounts, the devices of the families of the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class would not have been taken over, their homes spied on, and they would not have been harassed. This close connection is further reinforced by the broader general evidence of hacks of other Ring devices occurring around the same time period as the hack of Purchaser Plaintiffs' devices.

551. Ring's conduct also involves moral blame. Aware of the vulnerability of its customers and their families (often including minor children), and the sensitive nature of the information available to anyone who watches an indoor camera's security feed, Ring failed to take sufficient actions to prevent hackers from gaining unauthorized access. Ring was aware of the problems with its security systems and that they were vulnerable to intrusion by hackers because these issues were widely covered in the media. There was even a podcast dedicated to entertaining subscribers by hacking, observing, and harassing Ring customers through their devices. But even though Ring was aware of the vulnerability of its customers and their families to being hacked through its accounts and devices, Ring failed to cure those vulnerabilities or protect its customers and their families.

552. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class enjoy a special relationship with Ring. Ring provided services to the Purchaser Plaintiffs, including the ability to monitor the Non-Purchaser Plaintiffs indoor security devices via their Ring accounts.

553. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class were harmed by Ring's failure to exercise reasonable care in safeguarding their account information, and that harm was reasonably foreseeable.

COUNT X
Violation of the UCL
(On behalf of the Non-Purchaser Hacked Families Class)

554. The Non-Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

555. The Non-Purchaser Hacked Families have standing to pursue this cause of action because the Non-Purchaser Hacked Families suffered injury in fact and lost money as a result of Ring's misconduct described herein.

556. In particular, the Non-Purchaser Hacked Families lost the value inherent in keeping their likeness (as they appear on the hacked Ring device recordings) and all other sensitive personal information about them private. The value of their likeness and their private information were disseminated and exploited, including for monetary benefit, by the hackers who accessed their families' Ring devices. Upon information and belief, the hackers captured video and still screenshots of the hacking incidents, which they then posted on the Internet (including the dark web) for nefarious and profitable purposes, depriving the Non-Purchaser Hacked Families of that value.

557. 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. Ring has engaged in business acts and practices that, as alleged above, constitute unfair competition in violation of Business and Professions Code section 17200.

Unlawful

558. Ring's business practices, as alleged herein, violate the "unlawful" prong because Ring violates the Non-Purchaser Hacked Families' and the Non-Purchaser Hacked Families Class Members' rights to privacy and state laws, including Article 1, Section 1 of the California Constitution.

Unfair

559. Ring's business practices, as alleged herein, violate the "unfair" prong of the UCL because they offend an established public policy and are immoral, unethical, and unscrupulous or substantially injurious to consumers and their families.

560. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class have a well-established right to privacy and well-established privacy interests in their homes and in their sensitive personal information. Ring's failure to implement and maintain adequate security protocols violated those interests and substantially injured them.

561. The reasons, justifications, or motives that Ring may offer for the acts and omissions described herein are outweighed by the gravity of harm to the victims. The injuries suffered by the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class are substantial and are not outweighed by any countervailing benefits to consumers or competition.

COUNT XI
Unjust Enrichment
(On behalf of the Non-Purchaser Hacked Families Class)

562. The Non-Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein, and to the extent necessary, assert this count in the alternative to their UCL claim.

563. Ring has profited and benefited from the purchase of its devices by Purchaser Plaintiffs and the members of the Purchaser Classes, which also necessarily includes the recording and use of the likenesses and other private information of the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class. Ring's entire business model depends on consumers entrusting the privacy of their homes, and the privacy of their family members who also reside in those homes, to Ring.

564. Ring has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class did not receive the protection of their privacy rights that Ring promised to their families and that reasonable consumers and their families expected.

565. Ring has been unjustly enriched by its withholding of and retention of these benefits, at the expense of the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class.

566. Based on information and belief, Ring has further been unjustly enriched by its use of videos containing members of the Non-Purchaser Hacked Families Class, including, but not limited to, for promotional and advertisement purposes and in use and/or advancement of its other services, for which Ring derives a monetary benefit, profit, and/or additional exposure.

567. Equity and justice militate against permitting Ring to retain these profits and benefits.

568. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class suffered injury as a direct and proximate result of Ring's unjust enrichment and seek an order directing Ring to disgorge these benefits and pay restitution to the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class.

COUNT XII
Invasion of Privacy (Intrusion Upon Seclusion) and Violation of the California Constitution, Art. 1, § 1
(On behalf of the Non-Purchaser Hacked Families Class)

569. The Non-Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

570. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class members have reasonable expectations of privacy in their homes. This interest is protected by Article 1, Section 1 of the California Constitution.

571. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class members' privacy interest as described herein is legally protected because they have an interest in precluding the dissemination or misuse of their likenesses and other sensitive personal information, as well as an interest in making intimate personal decisions and conducting personal activities without observation, intrusion, or interference.

572. Ring intruded on the Non-Purchaser Hacked Families' and the members of the Non-Purchaser Hacked Families Class's solitude, seclusion, and private affairs when it allowed their families' Ring account information to be compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

573. Ring knew before selling its devices that they were susceptible to unauthorized third-party intrusion. Ring received further notice of these defects when other Ring users' accounts were hacked around the same time period as the horrific incidents suffered by the Hacked Families.

574. Ring declined to adopt sufficient security measures to protect the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class; indeed, Ring chose not to implement even ordinary, commonplace security measures and instead adopted dismal security features that permitted hackers to easily access user accounts. As a result of Ring's acts, hackers have been able to gain access to Ring users' devices and spy on them inside of their homes.

575. Ring's failure to protect its customers' accounts and security is highly offensive to a reasonable person. Ring accounts grant access to exceptionally intimate and private parts of someone's life: the inside of their homes, sometimes their bedrooms and bathrooms. Reasonable persons would expect, and the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class did expect, that Ring would properly safeguard their families' Ring accounts and their own sensitive personal information. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class entrusted Ring with this highly sensitive access, and Ring's failure to properly safeguard it is an egregious violation of societal norms.

576. The intrusions that Ring caused are also highly offensive to a reasonable person. Ring's actions alleged herein are particularly egregious because it represents that it cares about and prioritizes security, is aware of the vulnerability of their customers, and is aware of the sensitive nature of the information available to anyone

who watches an indoor camera security feed, and yet it has done nothing to prevent hackers from gaining unauthorized access and has refused to take responsibility. In fact, Ring chose to implement security measures that were deficient and made it easy for hackers to obtain access to user accounts.

577. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class were harmed by the intrusion into their private affairs as detailed herein. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class were deprived of their privacy rights and the related value of keeping their likenesses and personal information private and not disseminated publicly, including on platforms like Discord and the dark web. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class also experienced anxiety, emotional distress, loss of privacy, loss of time investigating and mitigating the effects of the hack, and are at an increased risk of future harm.

578. Ring's actions and omissions described herein were a substantial factor in causing the harm suffered by the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class.

579. As a result of Ring's actions, the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class seek damages, including compensatory, nominal, and punitive damages, in an amount to be determined at trial.

COUNT XIII
Invasion of Privacy (Public Disclosure of Private Facts) and Violation of the California Constitution, Art. 1 § 1
(On behalf of the Non-Purchaser Hacked Families Class)

580. The Non-Purchaser Hacked Families re-allege and incorporate the allegations in Paragraphs 1 through 440 set forth above as if fully written herein.

581. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class have reasonable expectations of privacy in their homes. This interest is protected by Article 1, Section 1 of the California Constitution.

582. The privacy interests as described herein are legally protected because the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class have an interest in precluding the dissemination or misuse of their likenesses and other sensitive personal information, as well as an interest in making intimate personal decisions and conducting personal activities without observation, intrusion, or interference.

583. Ring knew before selling its devices that they were susceptible to third party intrusion. Ring received further notice of these defects when other Ring users' accounts were hacked around the same time period as the horrific incidents suffered by the Hacked Families.

584. Ring declined to adopt sufficient security measures to protect the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class; indeed, Ring chose not to implement even ordinary, commonplace security measures and instead adopted dismal security features that permitted hackers to easily access their families' user accounts. As a result of Ring's acts, hackers have been able to gain access to Ring users' devices, including the devices belonging to the families of the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class, and spy on them inside of their homes.

585. Ring's acts and omissions caused the exposure and publicity of intimate details of the Non-Purchaser Hacked Families' and the members of the Non-Purchaser Hacked Families Class's private lives, including unauthorized use of their private information and likenesses over the internet and the dark web—matters that are of no concern to the public.

586. Ring's failure to protect its customers' and their families' security from exposure by and to unauthorized third parties is highly offensive to a reasonable person. Ring accounts grant access to exceptionally intimate and private parts of someone's life: the inside of their homes, sometimes their bedrooms. Reasonable persons would expect, and the Non-Purchaser Hacked Families and the members of the Non-Purchaser

Hacked Families Class did expect, that Ring would properly safeguard their likenesses and sensitive information. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class, through their Purchaser Plaintiff family members, entrusted Ring with this highly sensitive access, and Ring's failure to properly safeguard it is an egregious violation of societal norms

587. The disclosure and exposure that Ring's acts and omissions caused are highly offensive to a reasonable person. Ring's actions alleged herein are particularly egregious because through these actions, Ring represents that it cares about and prioritizes security, is aware of the vulnerability of their customers and is aware of the sensitive nature of the information available to anyone who watches an indoor camera security feed, yet it has done nothing to prevent hackers from gaining unauthorized access and have refused to take responsibility. In fact, Ring chose to implement security measures that were deficient and made it easy for hackers to obtain access to user accounts.

588. As a direct and proximate result of Ring's unlawful privacy invasions, the Non-Purchaser Hacked Families' and the members of the Non-Purchaser Hacked Families Class's likenesses and private, personal, and confidential information was disseminated and disclosed to third parties without their permission or consent. Purchaser Plaintiffs and the Purchaser Class members suffered injury as a result of these invasion.

589. The Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class were harmed by the public disclosure of their private affairs as detailed herein.

590. Ring's actions described herein were a substantial factor in causing the harm suffered by the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class.

591. As a result of Ring's actions, the Non-Purchaser Hacked Families and the members of the Non-Purchaser Hacked Families Class seek damages, including compensatory, nominal, and punitive damages, in an amount to be determined at trial.

VII. PRAYER FOR RELIEF

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

(a) Certifying the Classes and appointing the Purchaser/Accountholder Plaintiffs as Class Representatives for the Purchaser/Accountholder Class, appointing the Purchaser Hacked Families as Class Representatives for the Purchaser Hacked Families Class, and appointing the Non-Purchaser Hacked Families as Class Representatives for the Non-Purchaser Hacked Families Class;

(b) Finding that Ring's conduct was unlawful as alleged herein;

(c) Awarding Plaintiffs and the Class Members nominal, actual, compensatory, consequential, and punitive damages as allowed by law;

(d) Awarding Plaintiffs and the Class Members statutory damages and penalties as allowed by law;

(e) Awarding Plaintiffs and the Class Members restitution as allowed by law;

(f) Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest as allowed by law;

(g) Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses;

(h) Awarding public injunctive relief to ensure that Ring stops making misrepresentations and omissions to the public regarding the safety of its products, its cybersecurity, and its PII sharing with third parties; and that Ring takes all necessary steps to improve its cybersecurity policies and procedures to prevent future hacks of its devices and to prevent PII

disclosure of current and future customers to third parties without informed and clear consent; and

(i) Granting such other relief as the Court deems just and proper.

Dated: August 23, 2021

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson (SBN 174806)
Theodore W. Maya (SBN 223242)
Bradley K. King (SBN 274399)
Rachel R. Johnson (SBN 331351)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585
twolfson@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com
rjohnson@ahdootwolfson.com

Daniel S. Robinson (SBN 244245)
Michael Olson (SBN 312857)
Wesley K. Polischuk (SBN 254121)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax: (949) 720-1292
drobinson@robinsonfirm.com
molson@robinsonfirm.com
wpolischuk@robinsonfirm.com

Hassan A. Zavareei (SBN 181547)
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
(202) 973-0900; Fax (202) 973-0950
hzavareei@tzlegal.com

Annick M. Persinger (SBN 272996)
TYCKO & ZAVAREEI LLP
1880 Wilshire Boulevard, Suite 1101
Los Angeles, CA 90024
(213) 425-3657; Fax: (202) 973-0950
apersinger@tzlegal.com

Interim Co-Lead Counsel for Plaintiffs

DEMAND FOR JURY TRIAL

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

Dated: August 23, 2021

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson (SBN 174806)
Theodore W. Maya (SBN 223242)
Bradley K. King (SBN 274399)
Rachel R. Johnson (SBN 331351)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585
twolfson@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com
rjohnson@ahdootwolfson.com

Daniel S. Robinson (SBN 244245)
Michael Olson (SBN 312857)
Wesley K. Polischuk (SBN 254121)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax: (949) 720-1292
drobinson@robinsonfirm.com
molson@robinsonfirm.com
wpolischuk@robinsonfirm.com

Hassan A. Zavareei (SBN 181547)
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
(202) 973-0900; Fax (202) 973-0950
hzavareei@tzlegal.com

Annick M. Persinger (SBN 272996)
TYCKO & ZAVAREEI LLP
1880 Wilshire Boulevard, Suite 1101
Los Angeles, CA 90024
(213) 425-3657; Fax: (202) 973-0950
apersinger@tzlegal.com

Interim Co-Lead Counsel for Plaintiffs