

1 Deepali A. Brahmhatt (SBN 255646)  
Email: [dbrahmhhatt@devlinlawfirm.com](mailto:dbrahmhhatt@devlinlawfirm.com)  
2 DEVLIN LAW FIRM LLC  
3120 Scott Blvd. #13,  
3 Santa Clara, CA 95054  
Telephone: (650) 254-9805

4 Timothy Devlin (*pro hac vice* pending)  
5 Email: [tdevlin@devlinlawfirm.com](mailto:tdevlin@devlinlawfirm.com)  
Robert Kiddie (*pro hac vice* pending)  
6 Email: [rkiddie@devlinlawfirm.com](mailto:rkiddie@devlinlawfirm.com)  
7 Robyn Williams (*pro hac vice* pending)  
8 Email: [rwilliams@devlinlawfirm.com](mailto:rwilliams@devlinlawfirm.com)  
Devlin Law Firm LLC  
9 1526 Gilpin Avenue  
Wilmington, DE 19806  
Telephone: (302) 449-9010

10 *Attorneys for Plaintiff,*  
11 *Catherine Foster, on behalf of herself*  
*and all others similarly situated*

12 **UNITED STATES DISTRICT COURT**  
13 **CENTRAL DISTRICT OF CALIFORNIA**  
14 **SOUTHERN DIVISION**

15 Catherine Foster, on behalf of herself and  
16 all others similarly situated,

17 Plaintiff,

18 v.

19 Ring, LLC, a Delaware limited liability  
20 corporation,

21 Defendant.

Case No.

**CLASS ACTION COMPLAINT  
FOR DATA BREACH**

**DEMAND FOR JURY TRIAL**

22  
23  
24  
25  
26  
27  
28

1 Plaintiff, Catherine Foster (“Plaintiff”), individually and on behalf of all  
2 others similarly situated, brings this class action against Defendant Ring LLC  
3 (“Ring” or “Defendant”), and alleges the following:

4 **I. INTRODUCTION**

5 1. This action addresses Ring’s egregious failure to provide the safety and  
6 security it ostensibly promises its customers and to respect the most fundamental of  
7 its customers’ autonomy and privacy rights—the right to privacy in one’s home—and  
8 the very principles upon which the company was purportedly built.

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

16 3. Despite Ring expressly promising to provide its customers with “peace  
17 of mind” and to put its customers’ “security first,” its devices actually expose the most  
18 intimate areas of customers’ homes—and consequently the most private aspects of  
19 customers’ lives—to unauthorized third parties through its deliberately inadequate  
20 security measures that allows hackers to invade and terrorize their homes. Ring has  
21 failed to protect consumers against ill-meaning hackers despite the fact that it had  
22 been on notice of the inadequacies of its cybersecurity because of previous breach  
23 incidents.

24 4. Instead of helping families protect their homes, Ring’s devices—which  
25 were plagued with cyber-security vulnerabilities—have provided hackers a wide-  
26 open back door to enter the very homes the devices were supposed to protect. These  
27 simple vulnerabilities permit vicious criminals to hack into Ring devices and  
28

1 potentially their home networks. Based on the in-built vulnerabilities in the Ring  
2 devices, Plaintiff is at a high risk of injury based on hacking or data breach.

3 5. Furthermore, Ring actively shared users' sensitive personal identifying  
4 information ("PII") with third parties without first obtaining users' authorization or  
5 consent. This sensitive data allows third parties to build comprehensive and unique  
6 digital fingerprints to track consumer behavior and engage in surveillance behind the  
7 walls of one's private home, further enriching both Ring and the third parties.

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

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

19 8. Plaintiff intends to ask the Court to certify a Class under Rule 23(b)(2)  
20 and 23(b)(3) on behalf of all persons in the United States who purchased Ring's  
21 defective devices and insecure services and/or created an account for use of such  
22 devices (the "Purchaser/Accountholder Class") and is at a significant risk of harm  
23 through hacking, data breach and unauthorized sharing of PII.

24 **II. THE PARTIES**

25 9. Plaintiff Catherine Foster is a resident and citizen of Massachusetts and  
26 is a member of the Purchaser/Accountholder Class.

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

1 **III. JURISDICTION AND VENUE**

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

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

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

14 **IV. BACKGROUND**

15 14. Several of its user accounts and devices were hacked, putting Ring on  
16 notice that its service and devices had serious security vulnerabilities. The very  
17 purpose of the device and service was to provide security. The existing security  
18 vulnerabilities make a user account or device from Ring more likely at risk to be  
19 hacked or data breached. Such security risks take away from any benefits Ring  
20 products or services provide.

21 15. To date, Ring's tardy updates are still insufficient to protect their  
22 consumers' privacy and security going forward. There is no indication that Ring has  
23 addressed gaping security holes like Ring's leaving their devices vulnerable to brute  
24 force attacks and credential stuffing, failure to limit the number of failed login  
25 attempts, or Ring's failure to conduct basic IP detection to warn a customer that  
26 someone is attempting to login to their account from multiple different geographic  
27 locations at the same time. There is also no indication that Ring plans to require  
28

1 customers to use strong passwords or will prevent them from using passwords that  
2 are known to be exposed from previous data breaches.

3 16. Not only did Ring fail to protect Plaintiff's Ring account in adopting  
4 substandard security and privacy protocols, it also violated their customers' privacy  
5 by affirmatively sharing PII with third parties without authorization or consent.

6 17. After widespread reporting on the Ring hacks, an investigation by the  
7 Electronic Frontier Foundation ("EFF"), a nonprofit organization that educates  
8 consumers on privacy matters, found that the Ring app integrated multiple third-party  
9 trackers<sup>1</sup>. This unauthorized release further exposed customers to privacy violations  
10 by sharing their PII with third parties and increasing the risk of unauthorized access.

11 18. Among the information shared with these third parties were customers'  
12 names, private IP addresses, mobile network carriers, persistent identifiers, and sensor  
13 data on the devices of Ring's customers. Ring could remove the personal identifiers  
14 in user data before sending it to third parties, but it does not.

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

20 20. The danger in sending even small bits of information, such as device  
21 specifications, and an advertising ID, anonymous ID, or fingerprint ID, is that  
22 analytics and tracking companies are able to combine these bits together to form a  
23 unique picture of the user's device (mobile phone or computer), and thus create a  
24 fingerprint that follows the user as they interact with other apps and use their device,  
25 in essence providing the ability to spy on what a user is doing in their daily lives, in

26 \_\_\_\_\_  
27 <sup>1</sup> Bill Budington, Ring Doorbell App Packed with Third-Party Trackers, Electronic  
28 Frontier Foundation (Jan. 27, 2020),  
<<https://www.eff.org/deeplinks/2020/01/ringdoorbell-app-packed-third-party-trackers>>.

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.