Deepali A. Brahmbhatt (SBN 255646)
Email: dbrahmbhatt@devlinlawfirm.com
DEVLIN LAW FIRM LLC
3120 Scott Blvd. #13,
Santa Clara, CA 95054
Telephone: (650) 254-9805

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

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

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

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

Plaintiff,

v.

Ring, LLC, a Delaware limited liability corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR DATA BREACH

DEMAND FOR JURY TRIAL

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

I. INTRODUCTION

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

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 cybersecurity seriously and will safeguard users' private information.

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

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

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

5. Furthermore, Ring actively shared users' sensitive personal identifying information ("PII") with third parties without first obtaining users' authorization or consent. This sensitive data 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.

6. 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.

7. Plaintiff brings 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. Plaintiff requests 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 Plaintiff and the Class members for the damage that Ring's acts and omissions have caused.

8. Plaintiff intends 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 "Purchaser/Accountholder Class") and is at a significant risk of harm through hacking, data breach and unauthorized sharing of PII.

II. THE PARTIES

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

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

III. JURISDICTION AND VENUE

11. 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.

12. 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.

13. Venue is proper in this District 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. BACKGROUND

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

15. 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's 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 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.

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

17. 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[1]. This unauthorized release further exposed customers to privacy violations by sharing their PII with third parties and increasing the risk of unauthorized access.

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

19. 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.

20. 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

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

DOCKET ALARM

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.