UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JORGE NEWBERY and **HOLLY RINGLING,** individually and on behalf of all others similarly situated, Plaintiffs, v. **SAMSUNG ELECTRONICS AMERICA, INC.,** Defendant.	Case No. 1:22-cv-5325 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs JORGE NEWBERY and HOLLY RINGLING ("Plaintiffs"), individually and on behalf of all others similarly situated, through their attorneys, bring this action against Defendant SAMSUNG ELECTRONICS AMERICA, INC ("Defendant" or "Samsung"), and allege upon personal knowledge as to their own actions and experiences, and upon investigation, information, and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach lawsuit arises out of Defendant's failure to implement and maintain adequate security and safeguards with respect to its collection and maintenance of highly sensitive and confidential personal information of its customers, including name, contact and demographic information, date of birth, and product registration information. Defendant's insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach and its impact on Plaintiffs and Class members.

2. Samsung is a leader in the global market for high-tech computers and electronics manufacturing and digital media.

3. By Defendant's own admission, in late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems (the "Data Breach"). According to Defendant, on or around August 4, 2022, Defendant determined through its ongoing investigation that personal information of its customers was affected. Although Defendant identified the incident as early as August 4, 2022, Defendant did not warn those most at risk—Plaintiffs and Class members, until September 2, 2022.

4. The Data Breach exposed Plaintiffs' and Class members' personally identifiable information to criminals, including, but not limited to, name, contact and demographic information, date of birth, and product registration information ("PII").

5. The PII that unauthorized persons accessed on Defendant's systems can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiffs and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

6. Plaintiffs and Class members entrusted Defendant with their sensitive PII. Defendant understands the importance of protecting such information. For example, on its website, Defendant states "How We Protect Personal Information" and explains "We maintain safeguards designed to protect personal information we obtain through the Services."[1]

7. Defendant's representations concerning privacy practices and data security were false. Defendant does not state the date that it began investigating the incident, only that on or

[1] *See* https://www.samsung.com/us/account/privacy-policy/ (last visited Sept. 21, 2022).

around August 4, 2022, Defendant determined that its customers' information was acquired in the Data Breach that occurred in late July 2022. Criminals breached Defendant's inadequately defended systems, and accessed and acquired electronic files containing the PII of Plaintiffs and Class members. The criminals gained unauthorized access by thwarting, circumventing, and defeating Defendant's unreasonably deficient data security measures and protocols. Defendant did not start notifying Plaintiffs and other Class members of the Data Breach until on or around September 2, 2022.

8. Plaintiffs, individually, and on behalf of all persons similarly situated, seek to be made whole for the losses incurred by Plaintiffs and other victims of the Data Breach, and the losses that will be incurred in the future. Plaintiffs also seek injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendant's systems, and monitoring and audits of Defendant's security practices going forward because Defendant continues to collect, maintain, and store Plaintiffs' and Class members' PII.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Jorge Newbery resides in Barrington, Illinois and is a citizen of Illinois.

10. Plaintiff Holly Ringling resides in San Antonio, Texas and is a citizen of Texas.

11. Defendant is a New York corporation with its principal place of business in Ridgefield Park, New Jersey.

12. The Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiffs, are citizens of different states from Defendant.

13. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

GENERAL ALLEGATIONS

The Data Breach

14. On or about September 2, 2022, Defendants provided notice to Plaintiffs and Class members ("Data Breach Notice") via email and posted an "Important Notice Regarding Customer Information" on its website.[2] In the Data Breach Notice, Defendant states that in late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems that contain the personal information of Plaintiffs and Class members. A true and correct copy of the Data Breach Notice sent to each Plaintiff is attached as Exhibit 1.

15. The Data Breach Notice states that personal information pertaining to Plaintiffs and Class members was acquired by an unauthorized person in the Data Breach.

16. Defendant states that Plaintiffs' and Class members' information acquired in the Data Breach includes customer name, contact and demographic information, date of birth, and product registration information. *See* Exhibit 1.

17. Since discovering the Data Breach, Defendant states that "We have taken actions to secure the affected systems" and that "By working with industry - leading experts, we will further enhance the security of our systems - and your personal information." *See* Exhibit 1. These are actions that should have been employed in the first place and they would have prevented or limited the impact of the Data Breach.

[2] *See* https://www.samsung.com/us/support/securityresponsecenter/ (last visited Sept. 21, 2022).

18. Defendant does not state when the Data Breach was first detected. *See* Exhibit 1. Defendant states that on or around August 4, 2022, Defendant determined through its "ongoing investigation that personal information of certain customers was affected." *Id.* Defendant did not publicly announced the Data Breach or notify those whose PII was accessed by criminals in the Data Breach at that time.

19. On or around September 2, 2022—almost a month after learning that its customers' information was acquired by criminals in the Data Breach—Defendant sent Data Breach Notices to Plaintiffs and other persons whose PII was accessed by the criminals.

20. In the Data Breach Notice, Defendant provided information to Plaintiffs and Class members about additional steps they can take to help protect themselves. Defendant provided the contact information of the three credit bureaus that Plaintiffs and Class members could contact to obtain a credit report to help them detect possible misuse of PII. *See* Exhibit 1.

21. Additionally, Defendant provides FAQs on its website and recommends that Plaintiffs and Class members (a) remain cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information; (b) avoid clicking on links or downloading attachments from suspicious emails; and (c) review your accounts for suspicious activity. [3]

22. As a result of the Data Breach, Plaintiffs and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft or fraud, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

[3] *See* https://www.samsung.com/us/support/securityresponsecenter/ (last visited Sept. 21, 2022).

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.