UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

ADAM ZULLO, DAVID PEREZ, THOMAS BARRETTI, and THOMAS RICHARDSON, individually and on behalf of others similarly situated,

Civil Action No.

CLASS ACTION COMPLAINT

Plaintiffs,

-against-

ROBINHOOD MARKETS, INC.,

Defendant.

----------X

Plaintiffs Adam Zullo, David Perez, Thomas Barretti, and Thomas Richardson ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class members"), bring this Class Action Complaint against Defendant Robinhood Markets, Inc., based upon their individual experiences and personal information, and investigation by their counsel.

INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, bring this class action suit against Defendant because of Defendant's failure to safeguard the confidential information of millions of current and former Robinhood Markets, Inc. customers. The confidential information stolen appears to be encompass names and e-mail addresses in most cases, but also zip codes and dates of birth in others, with the full extent of the Personal Identifying Information (PII) obtained not yet being fully known.

2. Robinhood Markets, Inc. (hereinafter "Robinhood") is a financial services company offering an online stock trading platform, headquartered in Menlo Park, California and is a Financial Industry Regulatory Authority (FINRA)-regulated company and is registered with the United States Securities and Exchange Commission (SEC). With over thirty-one million users, Robinhood

collects a significant amount of data from its current and former customers, often including sensitive personal information such as Social Security numbers, addresses, telephone numbers, dates of birth, bank account numbers, credit card numbers, financial transaction records, credit ratings and driver's license numbers.

3. On or about November 8, 2021, Robinhood announced by a "Data Security Incident" on its website that on November 3, 2021:

> The unauthorized party socially engineered a customer support employee by phone and obtained access to certain customer support systems. At this time, we understand that the unauthorized party obtained a list of email addresses for approximately five million people, and full names for a different group of approximately two million people. We also believe that for a more limited number of people – approximately 310 in total – additional personal information, including name, date of birth, and zip code, was exposed, with a subset of approximately 10 customers having more extensive account details revealed. We are in the process of making appropriate disclosures to affected people.

4. The confidential information that was compromised in the Data Security Incident can be used to gain unlawful access to the users' other online accounts, carry out identity theft, or commit other fraud and can be disseminated on the internet, available to those who broker and traffic in stolen PII.

5. While the sophistication of the methods employed in effectuating the Data Security Incident is not publicly known, it is certain that the Data Security Incident could have been avoided through basic security measures, authentications, and training.

6. At all relevant times, Defendant promised and agreed in various documents to safeguard and protect Personal Identifiable Information (PII) in accordance with federal, state, and local laws, and industry standards, including the New York SHIELD Act. Defendant made these promises and agreements on its websites and other written notices and also extended this

commitment to situations in which third parties handled PII on its behalf.

7. Contrary to these promises, and despite the fact that the threat of a data breach has been a well-known risk to Defendant, which has experienced data breaches in the past, especially due to the valuable and sensitive nature of the data Defendant collects, stores and maintains, Defendant failed to take reasonable steps to adequately protect the PII of its current and former customers. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII.

8. As a result of Defendant's failure to take reasonable steps to adequately protect the PII of current and former Robinhood users, Plaintiffs' and Class members' PII is now on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

9. Defendant's failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiffs and Class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy.

10. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Data Security Incident, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and

diversity exists because Plaintiffs and Defendant are citizens of different states. Subject matter jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant as it conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Data Breach was likely stored and/or maintained in accordance with practices emanating from this District.

13. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District, and because some of the Plaintiffs reside within this District.

THE PARTIES

14. Plaintiff Adam Zullo is an individual Robinhood user residing in the County of Nassau, State of New York.

15. Plaintiff David Perez is an individual Robinhood user in the County of Queens, City and State of New York.

16. Plaintiff Thomas Barretti is an individual Robinhood user residing in the County of Nassau, State of New York.

17. Plaintiff Thomas Richardson is an individual Robinhood user residing in the County of Orange, State of New York.

18. Defendant Robinhood Markets, Inc. is a Delaware corporation authorized to conduct business in the State of New York, with its headquarters located in Menlo Park, California.

19. Defendant Robinhood conducts business within the State of New York and within

this District. It currently has thirty-one million users of its online securities trading application.

FACTUAL ALLEGATIONS

20. At all pertinent times, Plaintiffs were users of Robinhood, having entered into trading agreements to use Robinhood's application. Pursuant to said agreements, Plaintiffs were required to provide certain personal and financial information to Robinhood, including name, address, Social Security number, vehicle information, credit card numbers and driver's license numbers.

21. On or about November 8, 2021, Defendant Robinhood advised Plaintiffs via its website that a data security incident had occurred, resulting in unknown actors gaining access to and stealing PII.

22. Plaintiffs and Class members were required to agree to Robinhood's Privacy Policy, Terms of Use, Payment Authorization, and Consent to Electronic Transactions and Disclosures.

23. Robinhood promised to protect the PII of its users and emphasizes its purported commitment to protection of PII. Robinhood's website claimed, on October 18, 2021, that:

> At Robinhood, we take privacy and security seriously. This Privacy Policy outlines how Robinhood Financial LLC and its affiliates (collectively, "Robinhood," "we," "our," or "us") process the information we collect about you through our websites, mobile apps, and other online services (collectively, the "Services") and when you otherwise interact with us, such as through our customer service channels.

24. Robinhood has failed to maintain the confidentiality of PII, failed to prevent cybercriminals from access and use of PII, failed to avoid accidental loss, disclosure, or unauthorized access to PII, failed to prevent the unauthorized disclosure of PII, and failed to provide security measures consistent with industry standards for the protection of PII, of its current and former users.

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.