UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

ANDREW BRODERICK, JACQUELINE BURKE, SUSAN CORLEY, LYNN FIELDS, KIMBERLY HERNANDEZ, KRISTINA MENTONE, MARK MILLER, MORDECHAI NEMES, RYAN OLSEN, DEBRA POTZGO, SHAWN SPEARS, JANETT STOUT, COLE STUDEBAKER, and JONATHAN WONG, each individually and on behalf of all others similarly situated,

Plaintiffs.

v.

CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (USA) N.A., AMAZON.COM, INC., and AMAZON WEB SERVICES, INC.

Defendants.

Civil Action No. ______________

CLASS ACTION COMPLAINT
<u>AND DEMAND FOR JURY TRIAL</u>

Brian J. Dunne (CA 275689)
bdunne@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
355 S. Grand Avenue, 44th Floor
Los Angeles, CA 90071
Tel: (213) 262-9333

Andrew M. Williamson (VA 83366)
awilliamson@piercebainbridgecom
Andrew J. Pecoraro (VA 92455)
apecoraro@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
601 Pennsylvania Avenue, NW
South Tower, Suite 700
Washington, D.C. 20004
Tel: (202) 318-9001

Yavar Bathaee (NY 4703443)
yavar@piercebainbridge.com
Michael M. Pomerantz (NY 2920932)
mpomerantz@piercebainbridge.com
David L. Hecht (NY 4695961)
dhecht@piercebainbridge.com
Max P. Price (NY 4684858)
mprice@piercebainbridge.com
Michael K. Eggenberger (NY 5288592)
meggenberger@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
277 Park Avenue, 45th Floor
New York, New York 10172
Tel: (212) 484-9866

Attorneys for Plaintiffs

TABLE OF CONTENTS

PAGE

TABLE OF CONTENTS

PAGE

Plaintiffs, based on personal knowledge, and upon information and belief as to all other matters, allege as follows:

INTRODUCTION[1]

1. In March 2019, Capital One was the subject of one of the largest data thefts in history. The attacker, a former employee of Amazon Web Services, was caught and indicted. As information came to light about the nature of the attack, a striking set of facts began to emerge—not about the attacker, but about Capital One and Amazon. They had together, over several years, orchestrated a massive migration of highly sensitive data to a public cloud under the cover of false statements and Potemkin security software that Capital One and Amazon jointly created and jointly marketed to customers, regulators, and to the public as a means of keeping the data safe. But it was all a lie—and unbelievably, ***the precise conditions created by Defendants that gave rise to the March data theft persist to this day***.

2. This case is about a fraud by Capital One and Amazon—not the data theft that revealed it. And at base, it is about millions of Capital One customers who entrusted their most sensitive data—data that can be used by a thief to assume those customers' economic identity—to a bank and a cloud computing company based on a lie. Capital One and Amazon thoroughly monetized (and continue to monetize) sensitive Capital One customer data, mining it for every edge and insight about the behavior of Capital One's customers. But in order to obtain that data and the lucrative interest and fees those customers generated, Capital One promised customers that their data was safe and protected. Both Capital One and Amazon assured people around the country that this was the case. Those assurances have now been shown to be indisputably, willfully false and misleading—and they continue to be false, as were the statements Defendants made together

[1] Terms not defined in this Introduction are defined in the body of the Complaint.

over the years about the safety of Amazon's AWS public cloud for storage and processing of sensitive financial data.

3. As a result of these lies, Plaintiffs have paid billions of dollars in interest and fees to Capital One that they never would have paid had they known the truth: Their sensitive personal data was being pooled in a giant "data lake" on the world's most notoriously insecure public cloud, trawled by machine learning tools while at risk of theft via a well-known, unfixed Server Side Request Forgery ("SSRF") attack vector.

4. Defendants continue to aggregate and mine that data under the same perilous conditions that existed eight months ago. Customer data—years of it—is even today being aggregated and shared across hundreds of data mining systems, a simple SSRF attack away from another massive theft. That unsafe aggregation of data is not a bug; it is a feature. It is how Capital One makes money, and it is how Amazon sells its cloud computing services. Without years' worth of aggregated customer data, both companies would lose a competitive advantage.

5. Defendants know that there is no fix. They know that there is no setting they can change, or automated software they can write, to eliminate the risks that they intentionally force on their customers.

6. This fraud must stop. Plaintiffs seek damages and an injunction ordering the removal of sensitive Capital One customer data from Amazon's public cloud servers.

* * *

7. By the end of 2014, Capital One had collected an unprecedented amount of data about its customers. That data could tell Capital One how risky its credit card users were to lend to, how often they spent, what they spent on, and even where they went and what they cared about. The problem, however, is that significant amounts of hardware and software infrastructure were

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**