EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

RFCYBER CORP.,	§	Case No. 6:21-cv-00916-ADA
Plaintiff,	§	**JURY TRIAL DEMANDED**
v.	§	
APPLE, INC.,	§	
Defendant.	§	

OPPOSED MOTION FOR ENTRY OF DISPUTED PROTECTIVE ORDER

I. INTRODUCTION

Plaintiff RFCyber Corp. ("RFCyber" or "Plaintiff") respectfully requests that Court enter its Proposed Protective Order, attached hereto as Exhibit A. RFCyber's proposed order closely follows the Court's default protective order, with only three minor modifications which are highlighted in Exhibit A. Apple has refused to agree to entry of virtually *any* provision of the default protective order. Instead, Apple's proposal is based on a model protective order from the Northern District of California, with an extensive wish list of additional restrictions that would make discovery practically impossible. While Apple ultimately revised its proposal to loosely follow the format of the default protective order, the substance of its proposal remains unchanged. *See* Ex. B (highlights showing departures from the Court's default protective order). Apple's proposal more than doubles the length of the default protective order, adding at least ten entirely new sections, and at least eleven new subsections regarding source code alone. Apple fails to show any legitimate interests served by these radical departures from the default order. Instead, Apple's new provisions all serve to (1) substantively impede discovery; (2) impose an unreasonable burden on the Receiving Party; or (3) needlessly complicate the Protective Order, creating the possibility for abuse. Apple's attempt to interfere with discovery should be rejected, and the Court should enter RFCyber's proposal following its default protective order, attached as Exhibit A.

II. BACKGROUND

The parties exchanged proposed protective orders in mid-February, 2022. RFCyber proposed the Court's default order, while Apple's proposal followed an N.D. Cal. model, supplemented with a labyrinthine wish-list of restrictions. Apple maintained that proposal during and after the parties' meet and confer teleconference with lead counsel regarding the Protective Order on March 21, 2022. In view of those discussions, RFCyber agreed to a notice provision for code reviews, added a provision requiring monitors, keyboards, and mice to be provided to code

reviewers, and adopted a provision governing the procedure for adding review software in an attempt to compromise with Apple. *See* Ex. A (highlights denoting added provisions). Apple responded on April 8, 2022 by adopting Apple's proposal from an unrelated action involving an unrelated plaintiff, *Jawbone Innovations, LLC v. Apple Inc.*, 6:21-cv-00984, and improperly suggesting that Plaintiff's counsel was obligated to negotiate both protective orders jointly.

Apple's April 8 proposal, while loosely reformatted based on the Court's default order, included the same onerous restrictions as its earlier proposals, and did not include the edits from RFCyber's proposal. Realizing the parties were at an impasse, RFCyber suggested the parties file a joint motion, with each party providing a statement of its position, and provided Apple with RFCyber's position on April 22, 2022. Apple initially agreed to provide its portion of the motion by Thursday, April 28, but then reneged, stating that "Apple requires additional time to prepare its portion of the joint motion" and "will provide an update on anticipated timing next week." The parties again met and conferred on May 2, 2022, at which time Apple was still unable to provide a date certain for its position. Having exhausted all other options, and with Apple having confirmed its opposition, RFCyber was left with no choice but to file this Motion opposed.

III. ARGUMENT

The Court's default protective order already strikes the proper balance between allowing for efficient discovery and addressing the parties' legitimate security concerns. RFCyber's proposal follows the Court's default order except for minor changes which were primarily adopted in the interest of compromise. Apple's proposal is replete with restrictions that would make discovery unduly burdensome, if not impossible. Apple has failed to show any legitimate need for such restrictions.

Apple's departures from the Court's default order fall into at least one of three categories, all of which should be rejected: (1) provisions that substantively impede discovery; (2) provisions

that impose an unreasonable burden on the Receiving Party; and (3) provisions that needlessly complicate the Protective Order, adding likelihood of abuse and unnecessary disputes. For example, the following provisions fall into at least one of the first two categories:

Source Code Provisions:

- Apple's proposal at Section 10(f) would make source code discovery practically impossible by prohibiting copying of *any* "Source Code Material" into notes during review. Section 10(m) similarly prohibits use of any "Source Code Material" in discovery correspondence between the parties. In effect, Apple's proposal would prevent the parties from using even the name of any class, variable, function, namespace, or other structure inside the code. But it is impossible to take effective notes on code or to write effective discovery correspondence regarding code without referring to some portion of that code (e.g., if produced code calls a function whose code has not been produced, the Receiving Party would need to refer to the name of the function to request its code). Apple's provisions would allow the Protective Order to be used as a sword and shield to prevent Receiving Parties from specifically describing deficiencies in source code productions while simultaneously allowing the Producing Party to pretend confusion as to the code being requested. These provisions would burden the parties and impede discovery, rather than serving any legitimate security concern.
- Apple's proposal at Section 10(b) only agrees not to disable USB ports of the review computer, rather than providing for monitors, an external keyboard, and an external mouse as RFCyber proposes. It is impractical for code reviewers to travel with full-size computer monitors, and far less burdensome for the parties to provide them on-site.

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.