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

JAWBONE INNOVATIONS, LLC,	**Case No. 6:21-CV-00984-ADA**
Plaintiff,	
v.	**PATENT CASE**
APPLE INC.,	**JURY TRIAL DEMANDED**
Defendant.	**FILED UNDER SEAL**

APPLE'S RESPONSE TO JAWBONE'S OPPOSED MOTION FOR ENTRY OF DISPUTED PROTECTIVE ORDER

I. INTRODUCTION

Defendant Apple Inc. ("Apple") respectfully requests that this Court enter Apple's Proposed Protective Order (Exhibit 1) because it balances Apple's need to safeguard its source code and highly confidential information with ensuring fair and available access to discovery to Plaintiff Jawbone Innovations, LLC ("Jawbone"). Indeed, Apple was the first to initiate negotiations for a fair protective order in February so that Apple could securely and timely produce its confidential information to Jawbone. Yet Jawbone and its counsel refused to negotiate in good faith. Jawbone declared impasse after just one meet and confer and refused all further attempts to narrow the dispute. In doing so, Plaintiff also reneged on earlier compromises in favor of a new proposal on which it is refusing to further confer. Plaintiff's counsel, Fabricant, is taking the same unreasonable positions with respect to Apple in its other active case, *RFCyber Corp. v. Apple Inc.* (Case No. 6:21-cv-00916-ADA). (Exhibit 2.)

Adopting Apple's Protective Order is not only appropriate given the sensitivity of Apple's confidential information at issue in this matter, but it would send a clear message to Jawbone—

and to future litigants—that parties should negotiate in good faith over protective order provisions tailored to the individual needs of each case. And, in doing so, deter Jawbone (for the remainder of this matter) and future litigants from refusing all attempts to engage in meaningful meet and confer efforts and simply declaring impasse at any and all deviations from the default protective order. Therefore, and for the reasons set forth below, this Court should adopt Apple's proposed protective order, attached as Exhibit 1.[1]

II. ARGUMENT

Apple's proposed protective order fairly balances Apple's need to safeguard its source code and highly confidential information with its discovery obligations. The Court's default protective order is the foundation for Apple's proposal, and the additional protections and clarifications in Apple's proposal further ensure secure and efficient access to confidential information in this matter for both Apple and Jawbone. Apple's proposal is not "replete with restrictions that would make discovery unduly burdensome, if not impossible." Dkt. 40 at 3. Apple's proposed provisions reflect the real-world restrictions and protections Apple employs for access to and review of its source code outside of litigation. *See* Declaration of Robin Goldberg (Exhibit 4, hereinafter "Goldberg Decl.") Apple's proposed additions are reasonable and indeed similar provisions have been agreed to in other cases before this Court. *See, e.g., Koss Corp. v. Apple Inc.*, Case No. 20-

[1] A redline version reflecting modifications to the Court's default order is attached as Exhibit 3. Apple has struck provision 5(d) that was in previous proposals sent to Jawbone. Provision 5(d) provided that "CONFIDENTIAL" documents, information, and material could be disclosed to: "Up to and including three (3) designated representatives of the Receiving Party, who may be, but need not be, in-house counsel for the Receiving Party, as well as their immediate paralegals and staff, to whom disclosure is reasonably necessary for this case, provided that: (a) each such person has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit 1; and (b) no unresolved objections to such disclosure exist after proper notice has been given to all Parties." Apple does not know whether Jawbone disputes the deletion.

cv-00665-ADA, Dkt. No. 70; *Fintiv, Inc. v. Apple, Inc.*, Case No. 18-cv-372-ADA. Apple's versions of the following disputed provisions are fair and warranted.

A. Section 10—Source Code Security

Apple's revolutionary products outperform competitors due in large part to its trade secret-protected source code. (Goldberg Decl. ¶¶ 3, 6.) Apple invested billions of dollars in R&D to create and maintain a business model built on its novel integration of software and hardware. (Goldberg Decl. ¶ 5.) Apple's proposed safeguards are commensurate with the level of security that Apple employs internally to protect its core assets from inadvertent disclosure. (Goldberg Decl. ¶¶ 6,7.) Jawbone's proposal unjustifiably risks disclosure of Apple's source code, a risk that is especially pronounced given the broad scope of Jawbone's infringement allegations, which accuse nearly every Apple product of infringing the nine patents in suit, and resulting broad scope of source code produced. (Exhibit 5 at 2-3 (identifying various versions of the iPhone, AirPods, HomePod, and Mac products).)

Sections 10(b), (d)-(f) safeguard Apple's source code during inspection. Despite the fact Apple's proposal accommodates Jawbone's request for peripheral devices to be provided with the source code machine, Jawbone still complains, without basis, about Apple's provisions for notification regarding the types of source code review tools that Jawbone prefers to use. The form order requires a "stand-alone" computer connected to a printer, which Apple is offering. Apple's draft proposal further accommodates Jawbone's request that the review machine "have USB ports enabled for the use of peripheral devices." (*See* Exhibit 1.) Section 10(b) clarifies the machine will be equipped with a screen, keyboard, and mouse. (*Id.*; Goldberg Decl. ¶ 13.) Section 10(d) requires Apple to install source code review tools on the machine that are presently used in the ordinary course of business. With respect to requests for ***additional*** software tools, Apple will not "reject any tool for any reason" (Dkt. 40 at 5) because "approval shall not be unreasonably withheld." (Ex. 1 at § 10(d)). Jawbone anticipates using "standard tools," so Apple's proposal should be a non-issue for Jawbone. Moreover, Jawbone did not explain why it would be burdensome to identify desired review tools 10 days in advance of its review. The notice period is necessary to allow Apple a fair opportunity to evaluate the security risk posed by the requested applications and install the applications on the source code machine. Sections 10(e)-(f) ban recordable devices in the source code review room to prevent the creation of electronic copies of source code, and the provisions mirror protections Apple has implemented internally. (Goldberg Decl. ¶ 10.) Jawbone offers no good reason why Apple should compromise its established security protocols.

Section 10(k), contrary to Jawbone's misreading, allows an expert's "direct reports and other support personnel" (Dkt. 40 at 6) to access the source code, so long as Jawbone discloses those personnel and secures prior written consent. (Section 10(k)(vi)). This approach is consistent both with Apple's internal policy of limiting access to individuals on a "need-to-know" basis (Goldberg Decl. ¶¶ 8, 9) and with the form Protective Order at footnote 2 to Section 11(e), which requires "personnel helping in the analysis of Source Code Material shall be disclosed pursuant to Paragraph 5(e)." In sum, there is no real dispute regarding this provision.

Sections 10(l), (m) reduce risk of inadvertent disclosure of source code material in Court filings and discovery correspondence. Jawbone contends that the safeguards make written discovery and court filings "practically impossible." Dkt. 40 at 4-5. But Section 10(l) merely requires a meet and confer to agree on a procedure "as to how to make such a [Court] filing while protecting the confidentiality of the Source Code" and limits the number of continuous blocks of source code to 5 pages for inclusion in filings or expert reports. Jawbone's position that Section

10(l) poses an "unnecessary burden" (Dkt. 40 at 5) ignores the consequence of source code appearing on PACER, where it is instantly available to the general public, which would be near-impossible to cure. And Jawbone's concerns about Section 10(m) hindering discovery correspondence are unfounded. Section 10(m) prohibits the inclusion of "Source Code Material" in party correspondence, including Hardware Description Language (HDL), Register Transfer Level (RTL) and Computer Aided Design (CAD) files that describe the hardware design of components in Apple's products, as Apple treats this information as akin to source code. (Goldberg Decl. ¶ 4.) **Section 8,** however, excludes functions, parameters, file names, path structures, and other "Source Code-adjacent material" from the definition of "Source Code Material." (Exhibit 1 at 9 n.6.) The parties are free to use "Source Code-adjacent material" as shorthand in discovery correspondence to communicate effectively about source code without risking exposure of the source code itself.

Sections 10(n), (o), (v) reduce the risk of inadvertent disclosure by limiting the number and nature of source code copies. Section 10(n) prohibits making electronic copies of source code without prior written consent, except as provided in Section 10(l). Section 10(l) limits the number of printouts to a "reasonable number" that presumptively does not exceed 750 pages.[2] Should the parties disagree about a "reasonable number" of pages to be printed upon request, the provision requires the "Receiving Party to demonstrate that such printed portions are no more than is reasonably necessary for a permitted purpose and not merely printed for the purposes of review and analysis elsewhere." Having the "Receiving Party" explain its need for printouts beyond the presumptive limit removes speculation over the Receiving Party's motives. Jawbone glosses over

[2] Apple has agreed to increase its previously proposed 200 page presumptive limit to 750 pages. This change is reflected in Apple's proposed protective order (Exhibit 1, § 10(o).).

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.

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

fastcase®
Smarter legal research.