

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
TEXARKANA DIVISION**

MAXELL, LTD.,

Plaintiff,

v.

APPLE INC.,

Defendant.

Case No. 5:19-cv-0036-RWS

**JURY TRIAL DEMANDED**

**COVID-19 ADDENDUM TO PROTECTIVE ORDER**

WHEREAS, Plaintiff Maxell, Ltd. and Defendant Apple Inc., hereafter referred to as “the Parties,” have worked together to reconcile the needs of this case with the exigencies of the ongoing public health emergency;

WHEREAS, the Court entered an Agreed Protective Order on July 2, 2019 (Dkt. No. 45) (“the Protective Order”);

WHEREAS, since the Parties entered into the Protective Order, the outbreak of the novel coronavirus (COVID-19) has been declared a global pandemic by the World Health Organization, and the Centers for Disease Control and Prevention has described the outbreak of COVID-19 in the United States as a “rapidly evolving situation” and has recommended social distancing to limit further community spread of COVID-19;

WHEREAS, in response to the COVID-19 pandemic, virtually every state has issued a “shelter-in-place” or “stay-at-home” order to limit the spread of the disease, including those

currently in place in Texas and California, which vary in scope and duration but generally require businesses not considered “essential” to close their physical offices and continue their operations remotely;

WHEREAS, in addition to these orders and advisories, numerous state and federal courts, including the U.S. District Court for the Eastern District of Texas, have issued Orders restricting or preventing public access to courthouses given the severity of risk to persons by the spread of COVID-19;

WHEREAS, Apple’s normal and necessary security procedures, memorialized in the existing agreed-to Protective Order, for the treatment of computer source code used as part of litigation are not possible given the public health orders and advisories;

WHEREAS, Chief District Judge Rodney Gilstrap issued a Standing Order Regarding Pretrial Procedures in Civil Cases Assigned to Chief District Judge Rodney Gilstrap During the Present Covid-19 Pandemic on April 20, 2020 that expressly recognizes that: “[t]rying to keep cases moving forward while prioritizing the health of individuals” may require “unconventional practices and accommodations that would not normally be accepted as appropriate,” such as “the production of computer source code that are not consistent with the producing party’s normal security protocols” (¶2); to encourage parties “to be willing to make special accommodations during the health emergency,” that “those special accommodations will not be used against them in the future” (¶ 3); and that with respect to source code production, the “the use of . . . temporary code-review procedures during the pandemic will not be citable as evidence of appropriate code-review procedures after the pandemic” and that “[a]fter the pandemic, parties producing source code can return to advocating all their normal security protocols” (¶20 (emphasis in original));

WHEREAS, solely in this period of national—and international—public health emergency, Apple has developed, as a special accommodation, a temporary alternative to the inspection protocols set forth in the Protective Order that uses dedicated, specially-configured source code discovery laptops (“Remote Review Laptop”) that can be shipped to reviewers who are sheltering in place and enable the recipient of each such Remote Review Laptop to review code in an environment designed to approximate the security precautions set forth in the Protective Order to allow discovery of source code in this action to continue while the public health restrictions are in place; and

WHEREAS, Plaintiff acknowledges the exceptional exigencies presented by the international health emergency and will not later argue that Apple’s accommodations during this emergency constitute a proper approach in any other circumstances;

NOW THEREFORE, it is hereby stipulated among the Parties and **ORDERED** that:

1. This COVID-19 Addendum to the Protective Order shall be effective immediately upon entry and shall continue in effect until September 1, 2020, unless extended by agreement of the Parties or further order of the Court. Except as modified herein, all other provisions of the Protective Order shall remain in full force and effect.

2. Defined terms in this Addendum have the meaning established in the Protective Order entered in this action (i.e., Dkt. No. 45). In addition, “Authorized Reviewer,” in the context of this Addendum, shall mean any person who (a) is authorized under the Protective Order (i.e., Dkt. No. 45) to access materials designated as “CONFIDENTIAL - OUTSIDE ATTORNEYS’ EYES ONLY - SOURCE CODE” and “INTEL CONFIDENTIAL - OUTSIDE ATTORNEYS’ EYES ONLY - SOURCE CODE” and (b) has agreed to be bound by the provisions of this Addendum by signing a copy of Exhibit B.

3. Notwithstanding anything to the contrary in the Protective Order:

(a) Any Remote Review Laptop made available by Defendant may be used as

follows:

(i) The Remote Review Laptop must be kept, at all times when not in use in accordance herewith, within a locked safe or a locked room (including a secure closet or cabinet) within the office or home of the Authorized Reviewers when not in use;

(ii) Any Authorized Reviewer who is to receive a Remote Review Laptop shall, prior to receipt thereof, and upon Defendant's request, provide Defendants with details regarding the location at which such computer will be used for reviewing ("Source Code Review Room") and the location at which such computer will be stored when not being used for reviewing, for the sole purposes of ensuring compliance with the requirements of this Addendum regarding the location in which such computer is to be stored;

(iii) No recordable media or recordable devices, including without limitation sound recorders, computers, cell phones, smart watches, peripheral equipment, cameras, devices containing unobstructed cameras (e.g., webcams, unless entirely shielded with an opaque material), CDs, DVDs, or drives of any kind, may be in the Source Code Review Room when the Remote Review Laptop is powered on; however, to the extent such devices are unable to be removed without substantial burden (e.g. desktop computer) such devices shall be powered off and remain off during the review of the source code;

(iv) Upon the completion of each review session, Authorized Reviewer shall provide, at Defendant's request, a declaration confirming under penalty of perjury that no unauthorized electronic records of the Source Code were created or transmitted in any way;

(v) While any Remote Review Laptop is in use, its screen shall be positioned in such a way that it is not visible from any external window of the room in which it is stored, or such window shall be covered with blinds, shades, or a similar covering;

(vi) Before the Remote Review Laptop is turned on, the Authorized Reviewer who intends to review the Source Code shall provide a least one hour's notice to Defendant via email at [vzhou@omm.com](mailto:vzhou@omm.com), [dsilverman@omm.com](mailto:dsilverman@omm.com), and [kgodfrey@omm.com](mailto:kgodfrey@omm.com) that they are beginning a review session;

(vii) Upon receiving such notification, Defendant's counsel shall provide the Authorized Reviewer with a single-use password to access the Remote Review Laptop;

(viii) During the review session and at all other times, the Authorized Reviewers shall not copy, remove, or otherwise transfer any Source Code from the Remote Review Laptop including, without limitation, copying, removing, or transferring the Source Code onto any recordable media or recordable device;

(ix) The Remote Review Laptop must be turned off when not in active use;

(x) Immediately after the Remote Review Laptop is turned off, the Plaintiff's Authorized Reviewers shall notify Defendant via email at [vzhou@omm.com](mailto:vzhou@omm.com), [dsilverman@omm.com](mailto:dsilverman@omm.com), and [kgodfrey@omm.com](mailto:kgodfrey@omm.com) that they are ending a review session;

(xi) At all times, all network and USB ports and wireless transmitters of each Remote Review Laptop shall be and remain disabled, and the Remote Review Laptop shall not be connected to a printer in any way;

(xii) Authorized Reviewers shall maintain a log of the time that they spend reviewing materials on the Remote Review Laptop during each review session in the form attached as Exhibit A, which shall be made available to Defendant upon request.

(b) Any Remote Review Laptop made available by Defendant may be transported as follows:

(i) Via hand carry, Federal Express, or other similarly reliable courier by Defendant to a location mutually agreed upon by the Parties; and

(ii) Each Remote Review Laptop may not be removed from said location, except to be returned to the location requested by the Defendant via hand carry, Federal Express, or other similarly reliable courier, after providing notice to Defendant of the intended shipment and receiving confirmation from Defendant that such shipment can be securely received.

(c) Defendant will endeavor to accommodate reasonable print requests from Plaintiff according to the following procedures:

(i) After completion of a review session (i.e., not during a review session), Plaintiff's Authorized Reviewer may inform Plaintiff's outside counsel of record via phone call of the precise file path, file name, and line number range to print;

(ii) Then, Plaintiff's outside counsel of record may provide the precise file path, file name, and line number range to print to Defendant's outside counsel of record by sending that information in formal letter correspondence, encrypted,

# 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.