UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FINJAN, INC.,

Plaintiff,

v.

ESET, LLC and ESET SPOL. S.R.O.,

Defendants.

Case No.: 17CV183 CAB (BGS)

**ORDER REGARDING PROTECTIVE ORDER VIOLATIONS**

[ECF 292]

This dispute concerns alleged violations of the parties' stipulated Protective Order by counsel for Finjan, Mr. Lee. (ECF 292.) In reviewing Eset's source code, Mr. Lee compiled directory information from the source code computer into a 40-page document that he then produced to a witness during a deposition without any confidentiality designation on the document. (*Id.*) As explained more fully below, the Court finds Mr. Lee did violate the Protective Order in copying and compiling the directory structure of Eset's source code from the source code computer. However, the level of sanctions Eset requests are not warranted.

## BACKGROUND

This dispute arose when Finjan's counsel, Mr. Lee presented a deposition witness with a 40-page document listing the directory structure[1] of Eset's source code ("Exhibit

[1] The Court refers to the listing Mr. Lee created as "directory structure" or "directories and subdirectories," based on the Court's own review of the document. While it may contain folder names, as Finjan *now* refers to them, in earlier filings with the Court, discussed below, Finjan also described them as directories and subdirectories.

3"). The document lacked any confidentiality designation. During a call with the Court regarding this issue, Mr. Lee indicated he had taken notes about the source code on his laptop while reviewing the source code on the source code computer and that the 40-page document presented to the witness was accessible on Finjan's counsel's computer network.

By prior order, the Court addressed the more immediate dispute as to whether Mr. Lee should be precluded from accessing Eset's source code based on these possible violations and how to proceed going forward with review of Eset's source code. (ECF 306.) The Court found he could have access to the source code computer subject to certain limitations, including that he treat the directories, subdirectories, and file paths of the source code as he would treat source code with all the limitations imposed by a "HIGHLY CONFIDENTIAL – SOURCE CODE" designation and that he not take notes "onto any recordable media or recordable device" that could constitute "copy[ing], remov[ing], or otherwise transfer[ring] any portion of the source code" or the directories, subdirectories, or file paths as set forth in §9(c) of the Protective Order. (*Id.*) The Court also imposed these same limitations on anyone else accessing the source code because of the ongoing need for other individuals to also have access to the source code. (*Id.*)

## DISCUSSION

Eset asserts numerous violations of the Protective Order under a number of different sections. The relevant sections are summarized here in the order they appear in the Protective Order. A summary of the parties' positions on their application and the Court's analysis follow.

### I. Protective Order

Section 2 of the Protective Order is the Definitions section. Section 2.9 is titled "'HIGHLY CONFIDENTIAL – SOURCE CODE' Information or Items" and defines HIGHLY CONFIDENTIAL – SOURCE CODE as:

> extremely sensitive "Confidential Information or items" representing computer code and associated comments and revision histories, formulas,

> engineering specifications, or schematics that define or otherwise describe in detail the algorithms or structure of software or hardware designs, disclosure of which to another Party or Non-Party would create a substantial risk of serious harm that could not be avoided by less restrictive means.

Section 5 addresses designation of protected material. Section 5.2(a), addresses information in a documentary form (paper or electronic). The first paragraph of the section requires a producing party to "affix the legend 'CONFIDENTIAL OR HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY' or 'HIGHLY CONFIDENTIAL – SOURCE CODE' to each page that contains protected material." The second paragraph of § 5.2(a) indicates that:

> A Party or Non-Party that makes original documents or materials available for inspection need not designate them for protection until after the inspecting Party has indicated which material it would like copied and produced. During the inspection and before the designation, all of the material made available for inspection shall be deemed "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY." After the inspecting Party has identified the documents it wants copied and produced, the Producing Party must determine which documents, or portions thereof, qualify for protection under this Order. Then, before producing the specified documents, the Producing Party must affix the appropriate legend ("CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" or "HIGHLY CONFIDENTIAL – SOURCE CODE) to each page that contains Protected Material.

Section 5.2(c) requires "for information produced in some form other than documentary and for any tangible items, that the Producing Party affix in a prominent place on the exterior of the container or containers in which the information or item is stored the legend 'CONFIDENTIAL' or 'HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY' or 'HIGHLY CONFIDENTIAL – SOURCE CODE.'"

Section 6 of the Protective Order provides a detailed process to challenge a confidentiality designation, including the timing of a challenge (§ 6.1), a meet and confer

requirement (§ 6.2), and a process for raising an unresolved challenge with the Court (§ 6.3).

Section 9, SOURCE CODE, addresses designation, treatment, and procedures for access to and documentation of those that have accessed source code. Section 9(a) provides that "[t]o the extent production of source code becomes necessary in this case, a Producing Party may designate source code as 'HIGHLY CONFIDENTIAL – SOURCE CODE' if it comprises or includes confidential, proprietary, or trade secret source code." Section 9(b) indicates that materials "designated as 'HIGHLY CONFIDENTIAL – SOURCE CODE' shall be subject to all the protections afforded to 'HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY' information" and limits disclosure to those "to whom 'HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY' information may be disclosed, as set forth in Paragraphs 7.3 and 7.4."

Section 9(c) dictates how any source code will be produced in discovery. It provides:

> The source code shall be made available for inspection on a secured computer in a secured room without Internet access or network access to other computers, and the Receiving Party shall not copy, remove, or otherwise transfer any portion of the source code onto any recordable media or recordable device.

Section 9(d) provides that a "Receiving Party may request paper copies of limited portions of source code that are reasonably necessary for the preparation of court filings, pleadings, expert reports, or other papers, or for deposition or trial, but shall not request paper copies for purposes of reviewing the source code other than electronically as set forth in paragraph (c) in the first instance." It requires the Producing party to provide the requested source code in paper form with bates numbers and the label HIGHLY CONFIDENTIAL – SOURCE CODE and allows the Producing Party to challenge the amount of source code requested in paper form under § 6. Section 9(e) requires the Receiving Party to keep a record of anyone that has inspected any portion, electronic or paper, of the source code and to keep printed portions in a secured locked area. It also

prohibits creation of "any electronic or other images of the paper copies" and "convert[ing] any of the information contained in the paper copies into any electronic format." Section 9(e) requires the Receiving Party to "maintain a record of any individual who has inspected any portion of the source code in electronic or paper form."

## II. Parties' Positions[2]

### A. Eset's Position

Eset asserts that Mr. Lee's conduct violated § 5.2(a) of the Protective Order because, instead of requesting copies of the directory structure from the source code computer from Eset, it just copied the directories and subdirectories and proceeded to compile and disclose it without any designation. Similarly, ESET asserts Mr. Lee also violated §6 by ignoring the process set out in that section to challenge a designation. In essence, Eset argues that if Finjan believed the directory structure it was compiling from the source code computer should not have the HIGHLY CONFIDENTIAL – SOURCE CODE designation, it should have challenged it through this process rather than taking the information without asking and not designating it at all. Eset also argues Finjan violated § 9 of the Protective Order because the directory structure Mr. Lee copied onto his laptop constitutes source code. By copying it from the source code computer onto his laptop he violated § 9(c)'s prohibition on "copy[ing], remov[ing] or otherwise transfer[ring] any portion of the source code onto any recordable media or recordable device." Finally, Eset argues Finjan failed to abide by the procedures set out in § 9(d) for obtaining portions of source code.

### B. Finjan's Position

Finjan does not dispute the directory structure was copied from the source code computer, compiled into a 40-page document, and presented to a witness without any confidentiality designation. Rather, Finjan argues that there was no violation of the

---

[2] The Court only summarizes pertinent portions of the parties' arguments. (*See* Joint Statement [ECF 345] for each parties' entire argument.)

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.