United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SOCIAL APPS, LLC,

    Plaintiff,

    vs.

ZYNGA, INC.,

    Defendant.

Case No.: 4:11-CV-04910 YGR

ORDER GRANTING MOTION OF DEFENDANT ZYNGA, INC. TO COMPEL FURTHER TRADE SECRET DISCLOSURE AND FURTHER RESPONSES TO INTERROGATORIES

Defendant Zynga, Inc. ("Zynga") filed a discovery letter brief (Dkt. No. 61) seeking to compel Plaintiff SocialApps, LLC ("SocialApps") to: (1) identify its alleged trade secrets with particularity consistent with California Code of Civil Procedure §2019.210; and (2) provide adequate responses to Zynga's First Set of Interrogatories, served March 20, 2012. SocialApps filed its responsive letter brief. (Dkt. No. 64.)

Having carefully considered the papers submitted and the pleadings in this action, and for the reasons set forth below, the Court hereby **GRANTS** Zynga's discovery requests.

BACKGROUND

SocialApps alleges that around May 2009, Zynga approached SocialApps in an attempt to acquire the intellectual property rights, confidential information and source code for a social

network game it had developed, myFarm. (Dkt. No. 11, First Amended Complaint ("FAC") at

¶10.) On May 19, 2009, Defendants and Plaintiff entered into a Letter Agreement and Term Sheet

providing key business terms and for confidentiality concerning both the transaction and any

company information—including proprietary source code and confidential information—Plaintiff

provided to Defendants in what Defendants called their "due diligence." (*Id.*) Social Apps alleges

that under the guise of "due diligence," Zynga required SocialApps to produce its confidential

source code and other information for myFarm. (FAC ¶11.) By providing this confidential source

code and other information, Plaintiff revealed to Defendants numerous aspects of myFarm's

functionality, including its processes for using myFarm Credits, myFarm's key revenue-generating

feature. (*Id.*) Zynga is alleged to have misappropriated trade secrets it learned through this due

diligence.

ANALYSIS

I.   PROPRIETY OF REQUIRING TRADE SECRET DISCLOSURE CONSISTENT
       WITH CAL. CODE CIV. PROC §2019.210

First, the Court finds that the trade secret disclosure provisions in section California Code of

Civil Procedure § 2019.210 are properly applied here. When questions of state law are raised in

federal court, the federal court generally applies the state's substantive law but federal procedural

law. *Erie R. Co. v. Tompkins*, 304 U.S. 64, 78 (1938). The determination of whether a rule is

"substantive" or "procedural" is not mechanical and depends on the legal context. *Hanna v.

Plumer,* 380 U.S. 460, 471 (1965). The determination requires the court to consider whether the

state rule conflicts with any applicable federal rule. *Id.* at 471. If there is a conflict, the federal rule

prevails. If there is not, the court then looks to the question of whether the failure to apply the state

rule would significantly affect the outcome of the litigation or forum-shopping incentives. *Id.* at

2

468; *Computer Economics, Inc. v. Gartner Group, Inc.,* 50 F.Supp.2d 980, 986 (S.D. Cal. May 25, 1999).

While the Ninth Circuit has not decided whether section 2019.210 applies to actions in federal court, district courts within the circuit have reached differing conclusions on the issue. *See, e.g., Gabriel Technologies Corp. v. Qualcomm Inc.,* 2012 WL 849167 (S.D. Cal. March 13, 2012) (applying *Erie* and *Hanna* to find that § 2019.210 should be applied because it does not conflict with any federal rule and avoids undesirable forum shopping); *Hilderman v. Enea TekSci, Inc.*, 2010 WL 143440 (S.D. Cal. Jan. 8, 2010) (holding that § 2019.210 conflicts with Rule 26); *Funcat Leisure Craft, Inc. v. Johnson Outdoors, Inc.,* 2007 WL 273949 (E.D.Cal. Jan.29, 2007) (even if federal rules do not directly address matter of discovery procedure, court is not free to adopt "bits and pieces of the discovery civil procedure codes of the various states"); *Advante International Corp. v. Mintel Learning Technology,* 2006 WL 3371576 n. 4 (N.D.Cal. Nov. 21, 2006) (declining to decide applicability of § 2019.210 in federal cases but using it as guide); *Excelligence Learning Corp. v. Oriental Trading Co., Inc.,* 2004 WL 2452834, n. 3 (N.D.Cal. June 14, 2004) (finding §2019.210 not binding, but applying it because there was no parallel trade secret discovery provision in Federal Rules of Civil Procedure).

The Court finds the reasoning of the cases applying section 2019.210 more persuasive. Section 2019.210 does not conflict with any Federal Rule of Civil Procedure but rather assists the court and parties in defining the appropriate scope of discovery. *See Computer Economics, Inc., supra*, 50 F.Supp.2d at 989; *see also Gabriel Technologies Corp. v. Qualcomm Inc.,* 2012 WL 849167 (S.D. Cal. March 13, 2012). The nature of a trade secrets claim is such that pleading is necessarily general. To require more detail would be to force a plaintiff to disclose, in a publicly filed pleading, the very secrets it seeks to protect. However, the countervailing concern is that

3

discovery must be limited to those matters that the plaintiff truly contends are secret. Otherwise the discovery mechanism, and the litigation itself, could become a tool to force a defendant to reveal its own trade secrets in defense against unfounded or specious claims. The section 2019.210 disclosure defines the trade secrets at issue in the litigation with sufficient specificity that the defendant, as well as the court, is notified of the scope of the matters relevant to the claims. *Advanced Modular Sputtering, Inc. v. Superior Court*, 132 Cal. App. 4th 826, 835 (2005) ("The trade secret designation mandated by section 2019.210 is not itself a pleading but it functions like one in a trade secret case because it limits the scope of discovery in much the same way as the allegations of a complaint limit discovery in other types of civil actions").

Requiring compliance with section 2019.210 does not conflict with any federal rule. To the contrary, application of section 2019.210 is generally consistent with Rule 26's requirements of early disclosure of evidence relevant to the claims at issue and the Court's authority to control the timing and sequence of discovery in the interests of justice. It is likewise consistent, not in conflict, with the court's authority to issue a protective order regarding discovery of trade secret and confidential information as set forth in Rule 26(c)(1)(G). *See also Agency Solutions.Com, LLC v. TriZetto Group, Inc.*, 819 F. Supp. 2d 1001, 1017 (E.D. Cal. 2011) ("district court can therefore reject a claim that information is a trade secret *sua sponte* if the information is not identified by the claimant with sufficient particularity to allow the court to determine what the information is"); *Applied Materials, Inc. v. Advanced Micro–Fabrication Equipment (Shanghai) Co.*, 2008 WL 183520, at *1 (N.D. Cal. Jan. 18, 2008) (court has inherent discretion to manage discovery by requiring trade secret disclosure).

Moreover, application of section 2019.210 to trade secret claims filed in the federal court avoids improper incentives for choosing a federal forum. As other courts examining the question

1
2
3
4
5
6

have stated, refusal to enforce the requirement in federal cases would open up discovery so broadly

that it might allow a plaintiff in a federal forum to change its claims to conform to the information

defendant revealed in discovery, which would inevitably attract plaintiffs to the federal forum.

Computer Economics, supra, 50 F.Supp.2d at 992; *Gabriel Technologies, supra,* 2012 WL 849167

at *4.

7
8

Based upon the foregoing, the Court finds that the framework provided in California Code

of Civil Procedure § 2019.210 is properly applied in this case.

9

II.   SUFFICIENCY OF SOCIALAPPS' DISCLOSURE

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The Court next turns to the question of whether SocialApps has sufficiently identified the

trade secrets at issue in its disclosures served thus far. A trade secret is "information, including a

formula, pattern, compilation, program, device, method, technique, or process, that: [¶] (1) Derives

independent economic value, actual or potential, from not being generally known to the public or to

other persons who can obtain economic value from its disclosure or use; and [¶] (2) Is the subject of

efforts that are reasonable under the circumstances to maintain its secrecy." Civ.Code, § 3426.1,

subd. (d); *see also Advanced Modular,* 132 Cal. App. 4th at 833; *IMAX Corp., supra,* 152 F.3d at

1165. The disclosure required by section 2019.210 must identify the alleged trade secrets at issue

with sufficient particularity to define the contours of discovery and to distinguish the trade secrets

from matters within general or even highly specialized knowledge within the field. *Advanced*

Modular, supra, 132 Cal. App. 4th at 835; *IMAX Corp. v. Cinema Technologies, Inc.* 152 F.3d

1161, 1165 (9th Cir. 1998). While reasonable particularity does not require a party to define its

trade secret down to the finest detail or require a mini-trial on mis-appropriation before discovery

may commence, it does require that the plaintiff make some effort to define the trade secret in a

manner that is fair and proper under all the circumstances. *Advanced Modular, supra,* 132 Cal.App.4th at 835-36.

SocialApps has identified trade secrets here only categorically. In its original disclosure, it identified three broad categories of trade secret information, with some detail provided in the nature of subcategories. Those three categories were:

1. computer source code for Revision 21 of the myFarm game;

2. Technical aspects of Revision 21 of the myFarm game including server architecture, client architecture, database architecture, statistic recording and reporting, processes for adding and updating content, processes for expanding server capacity, functionality and organization of the source code, programming languages used to create the game, proprietary and open source software used to create the game; and

3. gameplay items, icons, and interface artwork that had not yet been released in a public version, including items such as various types of farm animals and trees.

SocialApps' First Amended CCP § 2019.210 Identification of Misappropriated Trade Secrets was essentially identical except that the second category was amended to add two more items: the "main ActionScript file for the Flash client (farmgame.as and farmgame.fla) that contained the entire game logic for the Flash client"; and source code that pertained to certain functions of the game logic, "such as taking snapshots of the farm (lines 28-38), load balancing (lines 197- 251), rendering the visual elements of the farm on the screen when the user visits it (lines 482-585), saving data after a user action (lines 608- 643, 727-1025, 1040-1097) and how zooming was implemented (lines1281-1314)."

While these two later additions identifying specific lines of code or file names are sufficiently detailed to identify what it is that SocialApps claims is secret, they are the only

6

instances in SocialApps' disclosure that do so. A description of the category, or even of the

subcategories of information within a category, does not comply with the requirement to identify

the actual matter that is claimed to be a trade secret. For instance, SocialApps asserts that its trade

secrets include "gameplay items, icons and interface artwork," and describes certain items and

icons by name, but does not provide any specific identification of the items and icons, such as a

copy of the graphic itself, or a specific statement of where the icon can be found in the materials it

provided to Zynga as part of the due diligence. Similarly, identification of the trade secret as

"server architecture" clearly is far too general but the further description of "server architecture"—

as including "memory utilization, storage utilization, server synchronization, scalability of all

resources (including memory, network bandwidth, storage devices and CPU), operating system

type, scripting engine, the number of servers, server functions and the ability and server

architecture for multiple users to execute and save game functions in real time—adds little more

than an elaborate categorization scheme for a variety of related concepts. It is no substitute for

specifically identifying and describing the actual architecture that SocialApps claims was stolen, or

pointing to where it might be found in the information it turned over to Zynga in the course of "due

diligence."

The California court's decision in *Silvaco Data Systems* case explains the distinction

between describing concepts or ideas versus identifying actual trade secrets. *Silvaco Data Sys. v.*

Intel Corp., 184 Cal. App. 4th 210, 222 (2010), as modified on denial of reh'g (May 27, 2010),

review denied (Aug. 18, 2010), *disapproved on other grounds by Kwikset Corp. v. Superior Court*,

51 Cal. 4th 310 (2011). In *Silvaco Data Systems*, the court noted that, while patent law protects

ideas, concepts and design, trade secret law protects factual, empirical data. Thus, the court held

that:

7

> The design may constitute the *basis* for a trade secret, such that *information concerning it* could be actionably misappropriated; but it is the information—not the design itself—that must form the basis for the cause of action. And while the finished (compiled) product might have distinctive characteristics resulting from that design—such as improved performance—they cannot constitute trade secrets because they are not secret, but are evident to anyone running the finished program. Indeed, to the extent [enhanced characteristics] tend to disclose the underlying design, [the design] ceases to be a protectable secret for that same reason.

Id. at 221–222 (all italics in original). Thus, the court there held that a trade secret designation that attempted to characterize various aspects of the underlying design of a software program as trade secrets failed to describe the trade secret properly, and the only protectable secret identified was the source code itself. *Id.* at 222.

Here, leaving aside the two instances where SocialApps identified a specific file name or source code line numbers, SocialApps has only offered the most general concepts to describe what it believes is its trade secret information. This is not sufficient.

The Court is mindful that an identification of the trade secrets at issue might require a protective order or sealing order, to the extent the parties' existing protective order (Dkt. No. 50) does not address the potential issues sufficiently. However, the need to seek further protective or sealing orders does not excuse SocialApps' failure to identify the trade secrets.

CONCLUSION

Based on the foregoing, the Court **ORDERS** as follows:

1. The motion to compel a further trade secret disclosure is GRANTED. SocialApps shall serve an amended identification of the trade secrets it alleges were misappropriated, stating the trade secret with particularity and including diagrams, exhibits or specific locations where information can be found as necessary. The identification of trade secrets should be made without reservation of right to amend. Any further amendment to the identification may be made only upon showing of good cause by motion to the Court.

2. As to the sufficiency of SocialApps' Response to Zynga's Interrogatories, the issues raised concerning those responses mirror the trade secret disclosure issues. The request to compel a further response is GRANTED for the same reasons. SocialApps is directed to serve an amended response to the interrogatories consistent with the Court's order on the disclosure.

3. Further disclosure and responses shall be served within 28 days of this Order. Should SocialApps find that a request for protective order or sealing order is necessary, it shall file and serve such motion within 28 days of this order, and its time to serve the further disclosure and responses will be stayed until the Court rules on such motion.

4. It appears to the Court that this case may require intensive, hands-on discovery dispute resolution. For that reason, all further discovery matters are referred for review and recommendation to Magistrate Judge Donna Ryu. Parties should contact Magistrate Judge Ryu's chambers for scheduling of any protective order motion or other discovery matter.

IT IS SO ORDERED.

This order terminates Dkt Nos. 61 and 64.

Date: June 14, 2012

_____
YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE