UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
BOWING GREEN DIVISION
CASE NO. 1:09-CV-00090-M

EVERCOM SYSTEM, INC. — **PLAINTIFF / COUNTER-DEFENDANT**

v.

COMBINED PUBLIC COMMUNICATIONS, INC. — **DEFENDANT / COUNTER-PLAINTIFF / THIRD-PARTY PLAINTIFF**

v.

SECURUS TECHNOLOGIES, INC. — **THIRD-PARTY DEFENDANT**

MEMORANDUM OPINION AND ORDER

This matter is before the Court upon the motion of the Defendant, Combined Public Communications (hereinafter "CPC"), to compel production and for attorneys fees, to which the Plaintiff, Evercom System, and the Third-Party Defendant, Securus Technologies, have responded in opposition, and CPC has replied (Docket Entry No. (DN) 84, 92, and 97). The Court has referred this action to the undersigned Magistrate Judge for determination of nondispositive matters pursuant to 28 U.S.C. § 636(b)(1)(A).

On August 13, 2012, a telephonic status conference was held in which the parties outlined their positions with respect to the pending motions.

For the reasons below, the Magistrate Judge shall DENY Evecom / Securus' motion for a hearing on CPC's motion to compel (DN 107); GRANT in part and DENY in part CPC's motion to compel (DN 84); and DENY CPC's request for attorneys fees (DN 84). All pending, unopposed motions for extension of time to file pleadings and to file pleadings under seal (DN 85, 89, 98, and 101) shall be GRANTED.

CLAIMS AND COUNTER-CLAIMS

Evercom asserts claims of tortious interference with contract against CPC, a competitor in the telecommunications business. Evercom provides telecommunications services to correctional facilities in Indiana and Kentucky. Evercom had contracts with jails in Spencer County and Crawford County, Indiana and with the Monroe County, Kentucky jail facility. The Indiana contracts contained a provision providing that the contracts would be automatically renewed beginning on May 21, 2007. The Kentucky contract was for a term of five years ending on April 3, 2012.

New sheriffs were elected in all three counties, and each newly-elected sheriff terminated the Evercom contract.

Evercom alleges that CPC tortiously interfered with its contracts by making false statements to the new sheriffs that induced them into illegally terminating and breaching their contracts with Evercom (DN 1, p. 8). CPC allegedly contacted the Indiana sheriffs and told them that the Indiana contracts were void upon election of a new sheriff and informed the Kentucky sheriff that the contract was invalid under Kentucky law for lack of a provision stating that a newly-elected sheriff may terminate within 30 days.

The Court previously granted Evercom's Motion for Judgment on the Pleading as to Count II and determined, as a matter of law, that the information allegedly given by CPC to the sheriffs was inaccurate (DN 33). The Court found that the Indiana contracts "result from the exercise of proprietary [as opposed to governmental] power, [therefore] they are binding upon the newly elected sheriffs and were not properly terminated" (p. 6). The Kentucky contract "is not a personal service contract and, thus, was not required to contain a provision allowing it to be terminated on 30 days notice" (p. 7).

CPC filed counter-claims against Evercom and third-party claims against Securus, Evercom's close business associate, alleging tortious interference with a contractual relationship in the Kentucky counties of Simpson, McCreary, Christian, Hickman, and Whitley, *iter alia*, due to unlawful refusal to remove equipment (DN 53, p. 11). CPC also asserted claims for tortious interference with another's performance of its own contract and for defamation (pp. 15 and 17).

THE INFORMATION SOUGHT BY CPC

CPC claims it became aware of the existence of an affidavit produced in connection with unrelated litigation either in Texas or Florida state court in which Securus Technologies sought to prohibit a former employee from working for a competitor. Securus gave the former employee access to information contained in its customer relationship management (CRM) system.

According to the affidavit of Securus employee Joshua Conklin, submitted in connection with the Texas / Florida case, the CRM contains "highly confidential and proprietary" data "relating to each account's service history, correspondence, customer preferences, and customer requests" (DN 84-2, pp. 2 and 3). "In particular, every Securus client or potential client has its own file within the CRM that contains their account plan, details and information gathered from site visits and client meetings, and its bidding plan, which is comprised of all pricing and cost information, customer preferences and requests, site requirements, and other various pieces of information crucial to arranging a bid" (Conklin affidavit, p. 3).

Evercom / Securus claims that the CRM data are highly restricted even for individuals working within the system, the data can be accessed only through the Securus virtual private network (VPN), the system has cost Securus millions of dollars to develop and maintain, and it provides Securus with a "competitive advantage in the inmate communications industry" (affidavit, p. 2).

CPC has moved to compel production of the Evercom / Securus CRM system data, allegedly to show the "true reason(s) certain facilities asserted [that] their contracts with the Securus Entities were no longer valid" (DN 97, p. 2). CPC seeks an order from this Court to the effect that (Proposed Order, DN 84-15):

> Evercom Systems, Inc. and Securus Technologies, Inc. (collectively, the "Securus Entities") must produce all materials responsive to Request for Production No. 6 contained in CPC's Third Set of Interrogatories and Requests for Production to Third-Party Defendant Securus Technologies, Inc. in the manner provided for in those discovery requests within five business days of the date of this Order;

CPC propounded its third set of interrogatories and requests for production on or about September 30, 2011. While both parties reference Interrogatory No. 1, Request for Production No. 4, and Request for Production No. 6, it appears that CPC's motion to compel is only seeking relief with regard to Request for Production No. 6.

Request for Production No. 6 states that (DN 84-4, p. 10):

> REQUEST FOR PRODUCTION NO 6. Please provide copies of any materials and Documents contained within any file housed, contained, kept within, part of, or along with Your "Customer Relationship Management" system, including, but not limited to, any account plans, bidding plans, pricing and cost information, customer preferences, profiles, requests, and site requirements for correctional facilities in the following locations:
>
> (a) Crawford County, Indiana;
> (b) Spencer County, Indiana;
> (c) Monroe County, Kentucky;
> (d) Simpson County, Kentucky;
> (e) McCreary County, Kentucky;
> (f) Christian County, Kentucky;
> (g) Hickman County, Kentucky;
> (h) Whitley County, Kentucky;
> (i) Washington County, Indiana; and
> (j) Boone County, Kentucky.

According to Evercom, these ten facilities "are now under contract with [CPC]," and CPC

can obtain the information concerning the "true" reasons why the facilities terminated the Evercom contracts through alternative means (DN 92, p. 10).

THE CRM SYSTEM DATA ARE CONFIDENTIAL

This case turns upon whether the proper characterization of the CRM data is, as Evercom insists, "highly sensitive and confidential information, trade secrets and customer information" (DN 92, p. 2) or, as CPC argues, merely "internal records kept in the ordinary course of business regarding their sales, management, and service team's interactions with representatives from the jails and detention centers" (DN 84, p. 17).

This difference of characterization is important because, if CPC's characterization is correct, it is entitled to discovery of any "nonprivileged matter that is relevant to any party's claim or defense." Fed.R.Civ.P. 26(b)(1). "Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." *Id.* On the other hand, if Evercom's characterization of the CRM data is correct, it is entitled to protection against discovery of any "trade secret or other confidential research, development, or commercial information." Fed.R.Civ.P. 26(c)(1)(G).

Federal courts within the Sixth Circuit have held that CRM data are "confidential and proprietary," rising to the level of a trade secret. In *Xerox Corp. v. O'Dowd*, 2006 WL 3053408, the Middle District of Tennessee noted that Xerox maintained a MarketSmart database, which was, in effect, a CRM system. The Court held that a reasonable factfinder could find the type of data in Xerox' MarketSmart database to be a trade secret. *Id.* at *8-9.

A former Xerox employee, Mr. O'Dowd, started his own company, DDS. DDS and Xerox worked in cooperation for some time, and Xerox provided DDS with access to its MarketSmart

database. DDS eventually terminated its relationship with Xerox. However, prior to termination, Mr. O'Dowd decided to "dump" MarketSmart in favor of a "new customer management tool [the CRM system]." *Xerox* at *3. DDS "downloaded the information from MarketSmart to Excel format, and then uploaded the information into Microsoft CRM to create a new marketing database for DDS" in violation of a Xerox-DDS confidentiality agreement. *Id.* The MarketSmart / CRM data were utilized by Xerox' business competitor, and Xerox sued Mr. O'Dowd and DDS for, *inter alia*, misappropriation of trade secrets. *Xerox* held that "[w]hether a customer list is a trade secret is generally a question of fact" and that a reasonable factfinder could find the type of data in the MarketSmart / CRM system to be a trade secret. *Id.* at *8-9.

The same factors applied in *Xerox* to find that the CRM data constitute trade secrets apply in this case. The information was not generally known outside of Xerox, and such information is divulged to Xerox employees and agents under strict conditions. Xerox takes numerous security measures to guard the secrecy of the information because the information is very valuable to Xerox and its competitors. Xerox has spent millions of dollars developing and maintaining the database about its own customers.

Similarly, in *Allen v. Howmedica Leibinger, GmhH*, 190 F.R.D. 518, 526 (1999), the Western District of Tennessee, held that "Allen seeks marketing information, sales data, sales projections, and product details. All of these are the type of information which give one an advantage over competition and have traditionally been protected." Compare *VAS Aero Services, LLC v. Arroyo*, 2012 WL 1825275 at *9 (S.D.Fla.) ("Documents containing strategic marketing plans and pricing information have been held to constitute trade secrets").

The CRM system data sought by CPC constitute a "trade secret or other confidential research,

development, or commercial information" as contemplated by Fed.R.Civ.P. 26(c)(1)(G) and are entitled to protection.

STANDARD FOR DISCOVERY OF CONFIDENTIAL INFORMATION

Having concluded that the CRM system data are confidential and entitled to protection does not end our inquiry. "It is well settled that a concern for protecting confidentiality does not equate to privilege, and that information and documents are not shielded from discovery on the sole basis that the they are confidential." *Mafcote, Inc. v. Federal Ins. Co.*, 2010 WL 1929900 (W.D.Ky.).

CPC argues that Evercom's ability to designate information from the CRM as "Confidential – Attorney Eyes Only" – pursuant to the terms of the Supplemental Agreed Protective order (DN 67, p. 2) – will "alleviates [all] concerns regarding confidentiality" (DN 84-1, p. 14). On the contrary, if it is established that the information being sought is confidential, the party seeking discovery must establish, not only that the information is relevant to a claim or defense, but also that it necessary to its case. *R.C. Olmstead, Inc. v. CU Interface, LLC.*, 606 F.3d 262, 269 (6th Cir.2010).

The evaluation of necessity should include consideration of all pertinent circumstances, including dangers of abuse and harm to the party resisting discovery, good faith, and availability of other means of proof, and whether the issues can be fairly adjudicated without the information. Miller and Wright, Federal Practice and Procedure § 2043 ("protection for confidential information").

Courts within the Sixth Circuit have held that, once it is established that the information sought is confidential and potentially-harmful if discovered, the burden shifts to the party seeking discovery to establish that the disclosure is relevant and necessary to the action. *Dow Corning Corp. v. Jie Xiao*, 2012 WL 1957293 (E.D.Mich.) at *7. If proof of relevancy or need is not established

or if discovery would nevertheless be unreasonable, oppressive, annoying, or embarrassing, or otherwise unduly injurious, discovery should be denied. *Id.*

DISCUSSION

Under the foregoing standards, we conclude that CPC has adequately demonstrated its need for discovery of any communication recorded in the CRM system from the sheriff or other county official in the ten counties listed in CPC's Request for Production No. 6. This is particularly so with respect to any communication in which the sheriff or other county official gave reasons for cancelling the contract or indicated that termination of services was brought on by something other than outside interference by CPC. Furthermore, in light of its defamation counter-claim, CPC has shown its need for discovery of any communication memorialized in the CRM from Securus's CEO to any nonparty regarding CPC.

With the foregoing exceptions, CPC's request for "any file housed, contained, kept within, part of, or along with Your 'Customer Relationship Management' system, including, but not limited to, any account plans, bidding plans, pricing and cost information, customer preferences, profiles, requests, and site requirements" (DN 84-4, p. 10) is overbroad. CPC has failed to demonstrate a need to know this highly confidential and proprietary information, which, if discovered, would expose Evercom and Securus to undue risk of commercial harm.

MOTION FOR ATTORNEYS FEES

CPC's motion for attorneys fees will be denied because the position of Evercom and Securus in this matter was "substantially justified." Fed.R.Civ.P. 37(a)(5)(A)(ii).

ORDER

For the foregoing reasons, it is hereby ORDERED that

1. CPC's motion to compel (DN 84) is GRANTED to the extent that Evercom and Securus are required to produce documents from the CRM system that record or reference any and all written or oral communications with any representative from the ten counties listed in CPC's Request for Production No. 6 within 30 days of entry of this Order.

2. CPC's motion for attorneys fees (DN 84) is DENIED.

3. Evecom / Securus' motion for a hearing on CPC's motion to compel (DN 107) is DENIED. The remaining, unopposed motions (DN 85, 89, 98, and 101) are GRANTED.

NOTICE

Within 28 days after entry of this Order, the parties may file a motion to alter or amend to correct manifest error of fact or law pursuant to Fed.R.Civ.P. 59(e). Alternatively, within 14 days after being served with a copy of this Order, the parties may file objections with the District Judge alleging that it is "clearly erroneous or is contrary to law." Fed.R.Civ.P. 72(a).

Lanny King, Magistrate Judge
United States District Court

August 16, 2012

c: Counsel

0|56