UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 14-21029-CIV-ALTONAGA/O'Sullivan

XTEC, INC.,

Plaintiff,

vs.

HEMBREE CONSULTING SERVICES, INC., et al.,

Defendants.
_____/

ORDER

THIS CAUSE came before the Court upon Defendants, Hembree Consulting Services, Inc. ("HCSI") and Larry Hembree's ("Hembree") (collectively, "Defendants[']") Motion for Partial Summary Judgment . . . ("Motion") [ECF No. 152], filed May 1, 2015. In support, Defendants filed a Statement of Material Facts . . . ("Defendants' SMF") [ECF No. 153]. Plaintiff, XTec, Incorporated ("XTec") filed a Response in Opposition to Defendants' Motion . . . ("Response") [ECF No. 176], and Statement of Material Facts in Opposition . . . ("Plaintiff's Response to Defendants' SMF") [ECF No. 177]. Defendants filed a Reply . . . ("Reply") [ECF No. 186], as well as a Reply in Support of Statement of Material Facts ("Defendants' Reply SMF") [ECF No. 187]. The Court has carefully considered the parties' written submissions, the record, and applicable law.

I. BACKGROUND

XTec's Complaint alleges HCSI and its president and sole shareholder, Hembree, misused XTec proprietary software and engaged in unfair business practices. (See generally Compl. [ECF No. 1-1]). In particular, at issue is whether HCSI and Hembree wrongfully copied

"XTec's proprietary technology" (id. ¶ 22) from XTec software already in use by the United States Navy (the "Navy") to create and sell an updated version of the XTec software to the Navy. (See generally id.). Defendants move for summary judgment on Count I, violation of the Florida Uniform Trade Secrets Act ("FUTSA"), Florida Statute sections 688.001 et seq.; and Count II, violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Florida Statute sections 501.201 et seq..

Hembree worked for the Navy for a number of years on electronic security and enterprise access control systems, including smart card technology. (See Am. Countercl. ¶¶ 5–6). During his tenure, Hembree "built a professional relationship" with Jeff Huskey ("Huskey"). (Id. ¶ 7). Hembree later left the Navy and formed Hembree & Associates, Inc. ("H&A") to develop a smart card business. (See id. ¶ 8). H&A created an identity management system, along with interfaces for other access control systems. (See id.). While at H&A, Hembree met David Fisher ("Fisher"), who later created CardSmart Technologies, Inc. ("CardSmart"). (See id.).

In 2000, Hembree sold H&A to XTec. (See id.). XTec specializes in the security access and authentication industry and markets its own proprietary software, hardware, and firmware to its clients. (See Compl. ¶ 6). XTec named Hembree Director of Government Initiatives; Hembree owns 40,000 shares of XTec stock. (See Am. Countercl. ¶ 8). In early 2001, XTec entered into a joint venture with CardSmart. (See Compl. ¶ 9). This relationship spanned from 2002 through 2009. (See id. ¶ 10). In 2003, Hembree resigned from XTec, and in 2004, formed HCSI. (See Am. Countercl. ¶¶ 9, 1).

Factual Dispute Regarding XTec's Development of AuthentX

In the late 1990s, XTec developed an identity management system ("IDMS") called AuthentX. (See Defs.' SMF ¶ 1; Pl.'s Resp. Defs.' SMF ¶ 1). Although AuthentX is used in

numerous government systems (see Defs.' SMF ¶ 1), XTec maintains AuthentX was developed at private expense and has always been sold and/or offered for sale to nongovernmental entities. (See Pl.'s Resp. Defs.' SMF ¶ 1). Defendants disagree, asserting XTec has not been able to produce any commercial agreements predating XTec's initial 2004 contract with the Navy. (See Defs.' Reply SMF ¶ 1). According to Defendants, the only support for XTec's claim that AuthentX was developed at private expense and offered for sale to nongovernmental entities is "unsubstantiated deposition testimony" of XTec's President, Alberto Fernandez ("Fernandez"), and Comptroller, Antonio Arner ("Arner"), as well as "three pages of CardSmart invoices from 2003" relating to research efforts to develop strategies to attract customers. (Id.).

Factual Dispute Regarding XTec's Preservation of Proprietary Data Rights

In 2004, Defendants began working with the Navy to develop a Navy-specific IDMS — the Enterprise, Network, Application, Data Base and Logistical Enabler ("Enabler") — using XTec as a subcontractor. (See Defs.' SMF ¶ 2). XTec alleges its task was to minimize costs by adapting AuthentX to interface with multiple "'legacy' applications" already in use by the Navy, in order to strengthen the Navy's security without requiring a complete redesign of its existing infrastructure. (Compl. ¶ 13). Enabler is, according to XTec, "essentially, AuthentX software and hardware customized for the U.S. Navy and designed to work across numerous Navy platforms and networks utilizing existing technology, for purposes ranging from access control, food services, weapons issuance, card authentication and numerous other functions." (Id. ¶ 14).

XTec's Comptroller, Arner, negotiated the May 20, 2004 Enabler Contract ("May 2004 Enabler Contract") (Defs.' Mot. Ex. 5 [ECF No. 158-3]) between XTec and the Navy's Space and Naval Warfare Systems Command ("SPAWAR"). (See Defs.' SMF ¶ 3). Hembree helped negotiate the May 2004 Enabler Contract on the Navy's behalf. (See Pl.'s Resp. Defs.' SMF ¶ 3;

Defs.' Reply SMF ¶ 3). Arner had no prior government contract experience before he began working for XTec in 2002 and no experience with Federal Acquisition Regulations ("FAR") or the Defense Federal Acquisition Regulations Supplement ("DFARS") that control government contracts and transfer of data rights. (See Defs.' SMF ¶ 3).

The parties dispute whether the May 2004 Enabler Contract preserved XTec's proprietary data rights. (See Defs.' SMF ¶ 4; Pl.'s Resp. Defs.' SMF ¶ 4). Defendants argue it does not because the contract contains no language preserving any proprietary rights or restricting use of XTec's data (see Defs.' Reply SMF ¶ 4); the contract requires XTec to "provide all technology including software and hardware to implement its solution," and a host of deliverables, including all design documents, operational requirements documents, user manuals, and installation CDs for the Enabler applications, which included source code; and states XTec "will install and turn over to CNI any custom built software and supporting documentation," and "[a]ll documentation regarding the ENABLER . . . including design notes, final user documentation, and COTS documentation will be provided to the Government." (Defs.' SMF ¶ 4 (alterations added)).

XTec does not contest this contractual language and the required deliveries. (See Pl.'s Resp. Defs.' SMF ¶¶ 4, 5; Defs.' SMF ¶ 5). Instead, XTec argues no language preserving data rights to XTec or advising the Navy of its proprietary rights was necessary because the contracts contemplated the provision of "commercial items." (Pl.'s Resp. Defs.' SMF ¶ 5). XTec notes the first page of the May 2004 Enabler Contract states, "This delivery order/call is issued on another Govt. agency or in accordance with and subject to the terms and conditions of above numbered contract," and refers to Contract number GS-07F-0823N. (Id. ¶ 4). Contract number GS-07F-0823N is XTec's September 15, 2003 General Services Administration Schedule Agreement ("2003 GSA Schedule") (Pl.'s Resp. Ex. D [ECF No. 178-5, 6]). (See Pl.'s Resp.

Defs.' SMF ¶ 4). According to XTec, the 2003 GSA Schedule demonstrates the commercial nature of all products delivered by XTec because the title of the GSA Schedule is "Solicitation/Contract/Order for Commercial Items" and contains other similar references to "Commercial Items," such as "Contract Terms and Conditions Applicable to GSA Acquisition of Commercial Items." (Id.).

XTec claims Defendants were aware of the 2003 GSA Schedule and the commercial nature of all products sold by XTec under it because prior to leaving XTec, Hembree was an "authorized negotiator" in connection with all products to be sold by XTec under the 2003 GSA Schedule. (Id.). Further, XTec notes the May 2004 Enabler Contract does not contain any reference to, or inclusion of, provisions of the FAR or DFARS that would obligate XTec to include proprietary markings on computer software or hardware in order to preclude transfer of ownership to the government. (See id.).

In response to XTec's claim regarding the commercial nature of its product and the 2003 GSA Schedule, Defendants point to Table 515-1 of the 2003 GSA Schedule (see Table 515-1 excerpt [ECF No. 187-1]), where XTec is directed to list standard discount and pricing policies for various types of customers purchasing the same or similar product as that being offered to the government, and XTec represented it "does not sell to this class of customer" for each type of customer listed. (Id.; see also Defs.' Reply SMF ¶ 4).

Up through 2008, XTec entered into several contracts with the Navy and its prime contractors regarding the Enabler system (see Defs.' SMF ¶ 6), none of which, Defendants contend, reserve any data rights or other rights in Enabler deliverables to XTec, or contain proprietary markings or reservations on ownership or use. (See id. ¶¶ 7–12). As to one contract in particular — a November 14, 2008 Subcontractor Task Order/Modification with Harris IT

Services for the Enabler project, signed by Arner — XTec checked a box representing "None of the data proposed for fulfilling such requirements qualifies as limited rights data or restricted computer software." (Id. ¶ 12). Arner testified this was "an Enabler statement of work." (Defs.' Reply SMF ¶ 12).

XTec contends several of the contracts identified by Defendants are also governed by the 2003 GSA Schedule and do not contain any reference to, or inclusion of, provisions of the FAR or DFARS that would obligate XTec to include proprietary markings on computer software or hardware in order to preclude transfer of ownership to the government. (See Pl.'s Resp. Defs.' SMF ¶¶ 7–9). XTec also challenges the relevance of several contracts relied on by Defendants because they are unexecuted and there is no record evidence establishing what was actually delivered by XTec to the contracting party. (See id. ¶¶ 10–11). Finally, as to the Harris IT Services contract, XTec insists Defendants fail to present evidence establishing what "data" the contract is referring to, and challenges whether the referenced data corresponds to the trade secrets at issue because, as of November 2008, XTec had developed and delivered Enabler 1.0 as a completed, functioning system two years earlier, and thus the data delivered under this contract did not necessarily include any components of its AuthentX system. (See id. ¶ 12).

Factual Dispute Regarding XTec's Preservation of Proprietary Data Rights in AuthentX Based on Contracts with Other Government Entities

Defendants assert XTec, in a 2006 contract with the Department of Labor for an AuthentX-based system, transferred unlimited rights in the AuthentX data to the government. (See Defs.' SMF ¶ 16). But Defendants later abandon this position in their Reply Statement of Material Facts (see Defs.' Reply SMF ¶ 16), after XTec demonstrated this contract was controlled by XTec's 2006 GSA Schedule (Pl.'s Resp. Ex. G [ECF No. 178-9]), which omits and overrides any contractual provisions contemplating a transfer of proprietary rights as to any of

the products listed thereunder. (See Pl.'s Resp. Defs.' SMF ¶ 16). Defendants nonetheless argue such protective language was absent in XTec's Navy contracts and construe this as further proof XTec failed to protect its trade secret and ceded rights to the Navy when it delivered the Enabler source code with no restrictions. (See Defs.' Reply SMF ¶ 16).

In addition, Defendants rely on an apparently incomplete set of pre-Enabler contracts produced by XTec that do not contain restrictive language or proprietary markings. (See Defs.' SMF ¶ 17). XTec again argues none of these various purchase orders contain any reference to provisions of the FAR or DFARS that would obligate XTec to include proprietary markings on computer software or hardware in order to preclude transfer of ownership to the government. (See Pl.'s Resp. Defs.' SMF ¶ 17).

Factual Dispute Regarding AuthentX License

Another point of dispute between the parties concerns whether AuthentX was licensed to the Navy. XTec did not produce any licensing agreements, and the Navy testified there was no license or license fee associated with Enabler or AuthentX. (See Defs.' SMF ¶ 13; Defs.' Reply SMF ¶ 13). Defendants concede there is at least one XTec contract with the Department of State that refers to an AuthentX license fee, but note the contract is from 2008, years after the first Navy agreement. (See Defs.' SMF ¶ 15). Although XTec's witnesses admit the Navy did not sign a license and did not pay a recurring license fee (see id. ¶ 13), XTec contends the license fee charged to the Navy for AuthentX was included in the price of the AuthentX servers (see Antonio Arner Dep. Tr. [ECF Nos. 151-1, 2, 3] 179:1–3); Hembree negotiated the licenses on the Navy's behalf (see Pl.'s Resp. Defs.' SMF ¶¶ 13–15); and the existence of the license is demonstrated by several electronic communications involving Hembree that refer to an

AuthentX license for Enabler, as well as an AuthentX license included in the price of the server (see Pl.'s Resp. Ex. F [ECF No. 178-8]).

Factual Dispute Regarding Pensacola Server's Security Provisions and CardSmart and Defendants' Access

Pursuant to the Enabler contracts, XTec delivered Enabler 1.0 source code to the Navy on Enabler servers. (See Defs.' SMF ¶ 18). In 2004 or 2005, one of the servers was sent to the Navy in Pensacola (the "Pensacola Server") and included a full copy of the Enabler 1.0 source code and AuthentX source code. (See id. ¶¶ 19–20). The Enabler 1.0 code on the Pensacola Server was not encrypted, but portions of it were "compiled" and therefore not human-readable. (Id. ¶ 21; see also Pl.'s Resp. Defs.' SMF ¶ 21). The Pensacola Server did not have a "puTTy key," "a particularly secure password used on other servers" (Defs.' SMF ¶ 21; see also Pl.'s Resp. Defs.' SMF ¶ 21), although XTec contends the Navy could determine whether or not to require a puTTy key; such a password is not needed as it was kept in a secure Navy server facility. In order for Hembree to access the Pensacola Server on behalf of CardSmart, he needed a username and root password. (See Pl.'s Resp. Defs.' SMF ¶ 21). The Enabler 1.0 source code contains no proprietary or confidential markings (see Defs.' SMF ¶ 38), and XTec could not verify whether it ever told the Navy in writing it claimed any ownership rights to the source code (see id. ¶ 40). XTec disputes the relevancy of both of these facts in light of XTec's 2003 GSA Schedule and the lack of any express provisions in XTec's SPAWAR contracts contemplating a transfer of proprietary rights to the Navy. (See Pl.'s Resp. Defs.' SMF ¶¶ 38, 40).

XTec admits the Navy, as owner of the Pensacola Server, could designate anyone to be a "superuser" with access to the Enabler 1.0 source code and with the capacity to create, delete, and rename files and directories, execute searches, run scripts, and install applications. (Defs.' SMF ¶ 22; Pl.'s Resp. Defs.' SMF ¶ 22). "Once access is granted at a root or superuser level to a

user of a Linux system, there is no way to protect anything on that system from that user." (Defs.' SMF ¶ 23). XTec contends, however, there is no evidence the Navy actually ever assigned anyone such superuser privileges and XTec's systems analyst testified various personnel working with the Navy did not have unrestricted root access to the servers. (See Pl.'s Resp. Defs.' SMF ¶ 22). XTec's servers are programmed with an Intrusion Detection System ("IDS") that notifies XTec of modifications being made to the code on the server. (See id. ¶ 21).

Factual Dispute Regarding CardSmart and Defendants' Access to the Pensacola Server

In 2008, while CardSmart was still involved in a joint venture relationship with XTec, HCSI hired CardSmart as its subcontractor to develop a new IDMS system for the Navy, Enabler 3.0. (See Defs.' SMF ¶ 24; Pl.'s Resp. Defs.' SMF ¶ 24). In 2009, XTec, through its employee Bill Mitchell ("Mitchell"), gave CardSmart root access to the Pensacola Server. (See Defs.' SMF ¶ 25; Pl.'s Resp. Defs.' SMF ¶ 25). At the time, the Pensacola server was not in active use, or "production," and was only being used for testing or training. (Defs.' SMF ¶ 26; Pl.'s Resp. Defs.' SMF ¶ 26). According to XTec, the root access provided to Defendants on CardSmart's behalf was obtained under "the falsest of pretenses." (Pl.'s Resp. Defs.' SMF ¶ 25). XTec cites evidence CardSmart had signed a Mutual Non-Disclosure Agreement with XTec; testimony XTec was told CardSmart was to be given access to the Pensacola Server to do testing and other things that did not involve CardSmart looking at XTec's source code; as well as an email sent by Hembree to Mitchell wherein Hembree requests a username and password for Fisher to have inbound access to the Pensacola Server in order for Fisher to help Hembree figure out what he owned. (See id.). XTec contends Defendants devised Enabler 3.0 as a modified version of Enabler 1.0 and intended to promote it as an "upgrade." (Id. ¶ 24).

Defendants assert they developed Enabler 3.0 at the Navy's direction and access to the Pensacola Server was obtained pursuant to the Navy's direction and authorization. (See Defs.' Reply SMF ¶¶ 24, 25). Defendants cite Huskey's testimony he allowed CardSmart access to the Pensacola Server knowing the source code was going to be used to develop Enabler 3.0, and because the Enabler system was owned by the government, the government could do with it what it wanted. (See id. ¶ 25).

After CardSmart was given access, its employee, James Wiley ("Wiley"), accessed the Pensacola Server to develop the new Enabler 3.0. (See Defs.' SMF ¶ 28). The parties dispute the amount of source code Wiley utilized. Defendants contend the amount copied made up possibly as little as one percent of the Enabler 3.0 code. (See id.). XTec argues the Enabler 3.0 code has changed over time to appear less similar to the Enabler 1.0 code upon which it was originally based. (See Pl.'s Resp. Defs.' SMF ¶ 28).

The parties also dispute the extent to which Defendants were aware CardSmart was accessing and using Enabler 1.0, or AuthentX code, in connection with the development of Enabler 3.0. Defendants rely on testimony from Wiley stating he believed "it was a Navy server that had the Navy code on it, and it was code from the Navy regarding Enabler;" he would never have copied any code he thought belonged to someone other than the Navy; and he never told Hembree or anyone at HCSI he used any of the Enabler 1.0 code in what he prepared for the Navy. (Defs.' SMF ¶ 29). XTec challenges any suggestion Defendants were unaware of the extent to which CardSmart was accessing and using Enabler 1.0 or AuthentX code on the Pensacola Server, citing a CardSmart invoice to HCSI evidencing CardSmart reviewed AuthentX files on the Pensacola server, as well as 2008 emails sent by Hembree acknowledging all

components of Enabler are government-owned with the exception of XTec's proprietary interest in AuthentX. (See Pl.'s Resp. Defs.' SMF ¶ 29).

The CardSmart Litigation and Factual Dispute Regarding Preservation of Source Code

The alleged misappropriation began in 2009. (See Compl. ¶¶ 17, 18). In July 2011, XTec filed a lawsuit against CardSmart and Fisher. (See Defs.' Notice of Removal [ECF No. 1] in XTec, Inc. v. CardSmart, Case No. 11-cv-22866-FAM (S.D. Fla.) (the "CardSmart Litigation")). "The allegations in the CardSmart Litigation are substantially similar to XTec's allegations in this case: namely, that CardSmart, Fisher, Hembree, and HCSI misappropriated proprietary XTec source code in developing the Enabler 3.0 system." (Am. Countercl. ¶ 30).[1] In June 2011, shortly before the start of the CardSmart Litigation, the Navy moved the Pensacola Server. (See Pl.'s Resp. Defs.' SMF ¶ 49; Defs.' Reply SMF ¶ 49). The parties dispute the conditions under which the server was moved and whether Defendants had any involvement. (See Pl.'s Resp. Defs.' SMF ¶ 49; Defs.' Reply SMF ¶ 49).

XTec's President, Fernandez, admitted XTec filed the lawsuit when it still had a chance to do a forensic image of the entire server, but it did not. (See Defs.' SMF ¶¶ 48–50). Because it did not have a forensic image of the entire Pensacola Server, XTec rebuilt one based on what its system indicated should have been on the server as of September 2009. (See Fernandez Dep. Tr., Defs.' Mot. Ex. 1 [ECF No. 158-2] 20:20–21:5). XTec's source code expert, Jan P. Eiras ("Eiras"), agrees the following statements from Defendants' source code experts' report (the "IIT" report) are "factually correct": "None of the evidence presented by XTec and made available to IIT for examination was obtained, handled, or delivered in a manner consistent with any forensic standards. No 'forensic' image of the Pensacola server exists, and all of the

[1] On December 29, 2014, the parties to the CardSmart Litigation entered into a Stipulated Final Judgment Granting Permanent Injunctive Relief. (See Stipulated Final J. CardSmart Litigation [ECF No. 480]).

information from that server has been reconstructed." (March 15, 2015 Jan P. Eiras Report ("Eiras Report"), Defs.' Mot. Ex. 20 [ECF No. 151-19] at 5; see also Defs.' SMF ¶ 46). Nevertheless, XTec's expert disagrees "the evidence submitted is suspect," or "that any of the data is anything other than what it has been described as." (Eiras Report 5). The experts for XTec and Defendants agree "without a forensic image of the Pensacola server, file dates cannot be verified and hashes of the files are meaningless beyond showing that they have not been modified since the hash was taken." (Defs.' SMF ¶ 47; Pl.'s Resp. Defs.' SMF ¶ 47).

Notwithstanding the foregoing, XTec downloaded forensic images of the files on the Pensacola Server believed to have been copied by CardSmart. (See Pl.'s Resp. Defs.' SMF ¶ 48). According to XTec, it produced code that is "an exact duplicate of the code that was originally resident on the Pensacola Server as of September 2009" — not simply an approximation — as a result of an alert by its IDS indicating changes were being made to the code at or around such time. (Id. ¶¶ 51–52; see also Fernandez Dep. Tr. 37:24–38:12, 40:25–41:15, 49:2–10).

The parties also dispute whether the source code produced by XTec in the CardSmart litigation is materially different from the source code produced in this case. Defendants' source code expert, Steven Clemmons, opines the Enabler 1.0 code presented in the CardSmart litigation is "far more complete than the versions presented by XTec in the Hembree case," and there are different directory structures in the codes, as well as indications the files in question were different versions developed at different points in time. (See Decl. Steven Clemmons, Defs.' Mot. Ex. 31 [ECF No. 151-31] 2). In response, XTec relies on arguments raised in its Motion to Strike . . . [ECF No. 157] Clemmons's report and testimony, to argue the Court should

"entirely disregard" Clemmons's opinions because he is not qualified and admitted he cannot read source code. (Pl.'s Resp. to Defs.' SMF ¶¶ 53–55).

II. LEGAL STANDARD

Summary judgment is to be rendered if the pleadings, the discovery and disclosure materials on file, and any affidavits show there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law. See FED. R. CIV. P. 56(a), (c). "[T]he court must view all evidence and make all reasonable inferences in favor of the party opposing summary judgment." Chapman v. AI Transport, 229 F.3d 1012, 1023 (11th Cir. 2000) (quoting Haves v. City of Miami, 52 F.3d 918, 921 (11th Cir. 1995) (alteration added; internal quotation marks omitted)). "An issue of fact is material if it is a legal element of the claim under the applicable substantive law which might affect the outcome of the case." Burgos v. Chertoff, 274 F. App'x 839, 841 (11th Cir. 2008) (quoting Allen v. Tyson Foods Inc., 121 F.3d 642, 646 (11th Cir. 1997) (internal quotation marks omitted)). "A factual dispute is genuine 'if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.'" Channa Imps., Inc. v. Hybur, Ltd., No. 07-21516-CIV, 2008 WL 2914977, at *2 (S.D. Fla. Jul. 25, 2008) (quoting Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986)).

III. ANALYSIS

Notwithstanding the number of factual disputes raised by the parties and summarized in this Order, Defendants insist summary judgment is warranted on Counts I and II of the Complaint because (1) XTec failed to protect its trade secret in the AuthentX or Enabler 1.0 source code (see Mot. 3–14); (2) XTec failed to preserve the Pensacola Enabler 1.0 Source Code and therefore cannot produce sufficient evidence to sustain its trade secret claim (see id. 15–16);

and (3) without a trade secret, XTec has no alternative ground on which to base its FDUTPA claim (see id. 16–18).

A. Count I: Florida Uniform Trade Secrets Act

To prevail on a claim for misappropriation of trade secrets under the FUTSA, XTec must demonstrate (1) it "possessed secret information and took reasonable steps to protect its secrecy and (2) the secret it possessed was misappropriated, either by one who knew or had reason to know that the secret was improperly obtained or by one who used improper means to obtain it." Del Monte Fresh Produce Co. v. Dole Food Co., Inc., 136 F. Supp. 2d 1271, 1291 (S.D. Fla. 2001) (citing FLA. STAT. § 688.002). "Trade secret" means "information, including a formula, pattern, compilation, program, device, method, technique, or process" that (1) derives economic value from not being generally known to, or readily ascertainable by, others, and (2) is the subject of reasonable efforts to maintain its secrecy. FLA. STAT. § 688.002(4).

1. Argued Loss of XTec's Trade Secret

Defendants argue DFARS provides a mechanism for government contractors to specify data rights or other deliverables the contractors desire to maintain as proprietary (see Mot. 3–4 (citing 48 C.F.R. § 252.227-7013(e)(2) Rights in technical data – Noncommercial items)), and a contractor waives its data rights and trade secret protection when it fails to utilize the DFARS mechanism and instead delivers sensitive data to the government without restrictions. (See id.). According to Defendants, XTec waived its trade secret in the AuthentX, or Enabler 1.0, source code by: (1) failing to preserve data rights in its contracts with the government for delivery of the source code; (2) neglecting to include proprietary markings or confidential designations on any source code, instructional manuals, or design documents; and (3) giving the Navy and CardSmart unrestricted access to the Pensacola Server Enabler 1.0 source code without advising either

entity, orally or in writing or via markings on the files themselves, of any XTec data rights or allegedly proprietary material in the contents of the server. (See id. 3).

Defendants' waiver argument is premised on the assumption the "more relaxed DFARS standard for data rights" in commercial software, as opposed to non-commercial software, does not apply because XTec has not produced any commercial agreements for AuthentX, or Enabler 1.0, predating the May 2004 Enabler Contract.[2] (Id. 4 n.1). "In the absence of any proof by XTec to the contrary," Defendants conclude, "the software is noncommercial, and the DFARS rule for such software applies. 48 C.F.R. 252.227-7014." Id.

According to XTec, AuthentX is commercial software, the DFARS standard for noncommercial software does not apply, and thus no proprietary language or markings were necessary. XTec challenges Defendants' claim AuthentX is noncommercial on the basis it was developed at private expense in the late 1990s and has always been sold and/or offered for sale to nongovernmental entities. (See Resp. 5–6). Although XTec has not produced any commercial agreements in support, as even Defendants concede, XTec has other evidence in the form of testimony from XTec's President and its Comptroller, as well as several pages of CardSmart invoices from 2003. (See Pl.'s Resp. Defs.' SMF ¶ 1; Defs.' Reply SMF ¶ 1). As additional evidence AuthentX is a commercial product, XTec relies on the fact it was delivered to the Navy pursuant to XTec's 2003 GSA Schedule:

> The inclusion of the subject AuthentX™ products which XTec used to develop Enabler 1.0 on XTec's GSA Schedule establishes . . . that AuthentX™ is a

[2] Pursuant to 48 C.F.R. § 252.227-7014, "Rights in noncommercial computer software and noncommercial computer software documentation," "commercial computer software" is designed as "software developed or regularly used for nongovernmental purposes which — (i) Has been sold, leased, or licensed to the public; (ii) Has been offered for sale, lease, or license to the public; (iii) Has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this contract; or (iv) Satisfies a criterion expressed in paragraph (a)(1) (i), (ii), or (iii) of this clause and would require only minor modification to meet the requirements of this contract." Id. § 252.227-7014(a)(1).

> commercial product because the Federal Supply Schedule program (pursuant to which all GSA Schedule contracts are issued) pertains only to commercial products. See FAR subpart 8.4, § 8.402(a) ("The Federal Supply Schedule program is directed and managed by GSA and provides Federal agencies . . . with a simplified process for obtaining commercial supplies and services at prices associated with volume buying").

(Id. 6 (alteration added; emphasis omitted)).

XTec also argues the DFARS provision for noncommercial software relied on by Defendants — section 252.227-7014 which codifies particular contract clauses to be included by a government contracting officer — is "not self-executing;" rather, by its own terms, this section is triggered by DFARS section 227.7203-6 and therefore "must instead be expressly included or incorporated by reference within the subject government contract in order for such provisions to apply." (Id. 7). Because the contracts do not include the relevant FAR and DFARS provisions, XTec concludes, no preservation language or restrictive markings are necessary in order to preclude a transfer of proprietary rights to the government. (See id. 8).

In the CardSmart Litigation, CardSmart moved for summary judgment and raised the same facts and legal arguments as Defendants, including that Enabler 1.0 was developed at government expense and was not commercial software (see CardSmart Motion for Summary Judgment . . . ("CardSmart Motion") [ECF No. 195] 13–14); the United States pays no license fees for the Enabler 1.0 software (see id. 14); and XTec failed to take reasonable steps to protect its trade secret by selling servers to the Navy without using restrictive markings, failing to include restrictive language or identifying any trade secrets in its government contracts, and providing CardSmart access to the Pensacola Server (see id. 12–17). Like Defendants, CardSmart also argued pursuant to DFARS section 252.227-7014, XTec "lost any 'secrecy' when it delivered the source code on the servers that it sold to the Navy in fulfillment of the SPAWAR contracts." (Id. 15). In its response to the CardSmart Motion, XTec argued, as it does

here, "no proprietary markings or limited rights notices were required under the relevant provisions of the FAR and DFARS because AuthentX® is a commercial product." (XTec Response in Opposition to CardSmart's Motion . . . ("XTec Response to CardSmart Motion") [ECF No. 206] 16). On May 15, 2014, the court denied CardSmart's Motion. (See May 15, 2014 CardSmart Litigation Order Denying Summary Judgment ("CardSmart Summary Judgment Order") [ECF No. 329]).

The court found the "record presents sufficient evidence for a reasonable jury to conclude XTec took appropriate measures to protect its alleged trade secret" (CardSmart Summ. J. Order 17), based on the following evidence, also presented here: XTec required the execution of confidentiality and non-disclosure agreements by third parties, including CardSmart; the servers containing the source code were stored at secure Navy facilities and data centers; in order to access the Pensacola Server a user had to obtain a username and password from XTec; and XTec employed an IDS which notified XTec when something was wrong with the server. (See id. 17–18).

The court also rejected CardSmart's argument the software was owned by the Navy pursuant to DFARS section 252.227-7014 (see id. 18), holding:

> First, the cases relied upon by Cardsmart are either not binding on this Court or do not involve government contracts. Additionally, the SPAWAR contracts entered into by Xtec did not expressly incorporate DFARS 252.227-2013 by reference. Further, FAR subpart 27.405-3(a) provides in pertinent part that "[i]f the computer software is to be acquired with unlimited rights, the contract shall so state." [FN 10: 48 C.F.R. Section 27.405-3(a) applies to the provision of commercial computer software to the government. It states in relevant part, . . .] Because the relevant contracts omitted provisions transferring Xtec's proprietary rights to the government, the Court cannot conclude that the Navy owned Enabler 1.0, as suggested by Cardsmart. In this regard, a genuine issue of material fact remains as to whether the Navy had unlimited rights to the source code, and, if so, where those rights began and ended.
>
> . . . .

> [I]t appears that Xtec has a proprietary interest in the AuthenX source code. This interest is different, however, from the interest that it has, if any, in the customization that it did for the Navy — Enabler 1.0. A jury could find that Xtec did not lose its proprietary rights to AuthentX when it sold Enabler 1.0 to the Navy. Nor does the fact that the AuthentX core was on the Pensacola server sold to the Navy necessarily divest Xtec of its proprietary interest or trade secret. Instead, Xtec has submitted evidence showing that AuthentX was sold as an appliance to the Navy, and a licensing fee for AuthentX was included in the cost of the appliance. Moreover, the appliance was maintained under a high level of security by the Navy. For instance, to access the code, a root password was necessary, and Xtec supplied this information to Fisher under strict circumstances only. The record also contains evidence that Xtec required Cardsmart to enter into a non-disclosure agreement before it disclosed any confidential information, including any part of the source code. For all of these reasons, a jury could find that Xtec took reasonable steps to protect the secrecy of its trade secret.

Id. (alterations added). Notably, despite XTec observing in its Response "Defendants have adopted the same arguments that were rejected by the Court" in the CardSmart litigation (Resp. 1), Defendants do not address, or attempt to distinguish, the CardSmart Summary Judgment Order.

Given the nearly identical factual and legal issues raised in the CardSmart Litigation, and the disputed issue of material fact regarding whether AuthentX is commercial or noncommercial software, the Court sees no reason to depart from the reasoning and holding of the CardSmart Summary Judgment Order. Indeed, the Court is dismayed Defendants created needless work rehashing arguments previously rejected. Defendants' request for summary judgment on this basis is denied.

2. Preservation of Pensacola Server and Trade Secret Defined

Defendants argue they are entitled to summary judgment on Counts I and II because (1) XTec "could have made a reliable forensic image of the files on the Pensacola Server" but "did not take a forensic image when it had the opportunity" and "has only been able to provide in this case a reconstructed version of what XTec believes was on the server at the time that CardSmart

was working on it" and the alleged misappropriation occurred (Mot. 15 (emphasis omitted)); and (2) XTec's definition of its trade secret is a moving target (see id. 16). Neither of these arguments is adequately developed by Defendants; certainly they do not persuade the Court to enter summary judgment.

With respect to the first argument, Defendants rely on a single copyright infringement case where summary judgment was granted because no substantial similarity test could be performed given the original code no longer existed and plaintiff "was left only with a version adulterated by years of government contracts and customizations and with no clear roadmap to decipher what alterations were made and what parties paid for which portions." Indyne, Inc. v. Abacus Tech. Corp., 876 F. Supp. 2d 1278, 1287 (M.D. Fla. 2012). This case is not clearly applicable here where, due to an IDS alert, XTec downloaded forensic images of the files copied by CardSmart and produced exact duplicates of the codes originally resident on the Pensacola Server as of the time of the alleged misappropriation. As to the reconstructed versions of the overall Pensacola Server produced by XTec, Defendants do not argue the reconstructions are unreliable and do not challenge XTec's expert's conclusion that "nothing has been presented that would indicate that any of the data is anything other than what it has been described as." (Pl.'s Resp. Defs.' SMF ¶ 46; see also Defs.' Reply SMF ¶ 46 ("Regardless, XTec admits it did not take a forensic image of the server . . . .")).

Defendants' second argument that XTec's alleged trade secret is a "moving target" (Mot. 16) was similarly raised unsuccessfully by CardSmart in its motion for summary judgment. (See CardSmart Mot. 9). As noted in the CardSmart Litigation, "[c]omputer programs may be protected and maintained as trade secrets. . . . Further, a software compilation and the overall design of a software program may be protectable as a trade secret." (CardSmart

Summ. J. Order 15 (alterations added; citing cases)). "Although Xtec must describe the trade secret for which it seeks protection with sufficient particularity to permit Defendants the ability to ascertain the boundaries of the secret, it need not specify the lines of source code that make up the trade secret." (Id. (citing Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 358–59 (D. Mass. 1993) (witness testimony and other evidence regarding design, function, and use of source code was sufficient to establish a trade secret)).

Ultimately, the court in the CardSmart Litigation found "Xtec provided notice to Cardsmart that it claimed trade-secret protection of its AuthentX IDMS/CMS based on its 'unique combination of hardware and software.' Xtec also identified lines of code in Eiras's report and states that it produced its source code to Defendants for inspection. Under these circumstances, Xtec has sufficiently described the trade secret for which it seeks protection." (Id. 16). Defendants wholly fail to persuade the Court to hold otherwise in this instance.

B. Count II: Florida Deceptive and Unfair Trade Practices Act

The FDUTPA provides a civil cause of action for "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ." FLA. STAT. § 501.204(1) (alterations added). A claim for damages under the FDUTPA has three elements: (1) a deceptive act or unfair practice; (2) causation; and (3) actual damages. See Rollins, Inc. v. Butland, 951 So. 2d 860, 869 (Fla. 2d DCA 2006) (citations omitted).

Defendants argue "[w]ithout a trade secret argument the FDUTPA claim cannot stand. What is left is simply not actionable . . . . The 'sensitive and proprietary commercial information' mentioned in [paragraphs] 49–51 of the [C]omplaint has not been established, if it is not the trade secret itself." (Reply 10 (alterations added)). Because a genuine issue of

material fact exists regarding whether a misappropriation of trade secrets occurred, and because FDUTPA claims can be based on claims of misappropriation, see CareerFairs.com v. United Business Media LLC, 838 F. Supp. 2d 1316, 1324 (S.D. Fla. 2011), Defendants' supplementary arguments for summary judgment on Count II are summarily dismissed.

One argument, clarified by Defendants in their Reply, is addressed separately. Defendants contend XTec cannot base its FDUTPA claim on alleged violations of FAR regulations[3] because such regulations do not constitute a "law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices," pursuant to Florida Statute section 501.203(3)(c).[4] (Reply 11).

[3] According to XTec, FAR subpart 9.505-1 prohibited Defendants' involvement in the development of Enabler 3.0 by virtue of Hembree's position as program manager. (See Resp. 17). FAR subpart 9.505-1: "Providing systems engineering and technical direction" provides:

> (a) A contractor that provides systems engineering and technical direction for a system but does not have overall contractual responsibility for its development, its integration, assembly, and checkout, or its production shall not-
>
> (1) Be awarded a contract to supply the system or any of its major components; or
>
> (2) Be a subcontractor or consultant to a supplier of the system or any of its major components.
>
> (b) Systems engineering includes a combination of substantially all of the following activities: determining specifications, identifying and resolving interface problems, developing test requirements, evaluating test data, and supervising design. Technical direction includes a combination of substantially all of the following activities: developing work statements, determining parameters, directing other contractors' operations, and resolving technical controversies. In performing these activities, a contractor occupies a highly influential and responsible position in determining a system's basic concepts and supervising their execution by other contractors. Therefore this contractor should not be in a position to make decisions favoring its own products or capabilities.

Id.

[4] Florida Statute section 501.203(3) provides: "Violation of this part" means any violation of this act or the rules adopted under this act and may be based upon any of the following as of July 1, 2006:

> (a) Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41 et seq.;
>
> (b) The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts;

Rather, Defendants argue, FAR 9.505-1 "provides rules of thumb for contracting officers." (Id. (citing FAR 9.500: "This subpart (a) prescribes responsibilities, general rules, and procedures for identifying, evaluating, and resolving organizational conflicts of interest; (b) provides examples to assist contracting officers in applying these rules and procedures to individual contracting situations; . . . .")).

Although there may be merit to Defendants' argument, as far as the Court is able to discern from the Complaint and XTec's Response, XTec is not raising a separate FDUTPA claim premised on Hembree violating the FAR. Rather, this alleged violation is a component of XTec's larger misappropriation claim.[5] As explained by XTec, the factual basis of the FDUTPA claim pertains to Defendants "intentionally soliciting CardSmart to develop a solution to compete with and replace Enabler 1.0 with full knowledge of CardSmart's former joint venture relationship with XTec during which CardSmart had extensive exposure to AuthentX" (Resp. 16); and Defendants' reliance upon "XTec personnel — [using] false pretenses — to provide assistance and access to Enabler 1.0/AuthentX" (id. (alteration added)); all of which "is exacerbated by Hembree's role, . . . , as the Enabler Program Manager on behalf of the CNIC"

> (c) Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices.

Id.

[5] This is distinct from the cases cited by Defendants. See In re Mona Lisa at Celebration, LLC, 472 B.R. 582, 639 (Bankr. M.D. Fla. 2012) (holding alleged violations of the 1933 Securities Act and the Florida Condominium Act could not "serve as predicate violations for a claim under FDUTPA" because the statutes "do not proscribe unfair methods of competition and are not encompassed within the penumbra of consumer protection statutes covered by FDUTPA. They instead govern the use of plaintiffs' deposits held in escrow and other technical requirements unrelated to any unfair or deceptive trade practice." (footnote call number omitted)); In re Edgewater By The Bay, LLLP, 419 B.R. 511, 516 (Bankr. S.D. Fla. 2009) (finding particular Florida statutes and county code provisions regulating the construction industry were not within the purview of Florida Statute section 501.203(3)(c); holding "[v]iolations of laws or statutes that give rise to a FDUTPA claim must be of the kind that proscribe unfair trade practices or unfair methods of competition; not, . . . , a violation of any law or statute that may have some benefit to consumers" (alterations added)).

(id. 17 (alteration added)). (See also Parties' Jointly Proposed Preliminary and Final Jury Instructions [ECF No. 203] (including no separate FDUTPA claim based on the alleged violation of FAR 9.505-1)).

IV. CONCLUSION

For the foregoing reasons, it is

ORDERED AND ADJUDGED that Defendants' Motion **[ECF No. 152]** is **DENIED**.

DONE AND ORDERED in Chambers at Miami, Florida, this 18th day of June, 2015.

Cecilia M. Altonaga

CECILIA M. ALTONAGA
UNITED STATES DISTRICT JUDGE