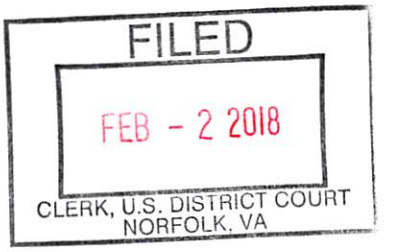
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division



SPACE SYSTEMS/LORAL, LLC

Plaintiff,

v. CIVIL ACTION NO. 4:17-cv-00025-RAJ-LRL

ORBITAL ATK, INC.,
Defendant.

MEMORANDUM OPINION AND ORDER

This matter is before the Court on Defendant's Motion to Dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). Both parties have filed memoranda supporting their respective positions. Having reviewed the parties' filings, this matter is ripe for judicial determination. For the reasons set forth below, Defendant's Motion is **GRANTED IN PART AND DENIED IN PART.**

I. BACKGROUND

Space Systems/Loral LLC, ("SSL" or "Plaintiff"), is a limited liability company that specializes in the design and manufacturing of geostationary satellites, space systems, and robotics technology. ECF No.1. Orbital ATK, Inc., ("Orbital" or "Defendant") is a Virginia based company that performs similar work. *Id.* at 6. In 2015, the National Aeronautics and Space Administration ("NASA") solicited project proposals through an RFP entitled "Utilizing Public Private Partnerships to Advance Tipping Point Strategies." *Id.* at 2. This project, commonly referred to as "Tipping Point," was aimed at expanding opportunities and capabilities in the commercial space industry through public-private partnerships. *Id*; ECF No. 8 at 8. NASA awarded SSL a contract for its "Dragonfly" project and Orbital for its "CIRAS" project respectively. ECF No. 1 at 3; No. 8 at 8. To

facilitate the sharing of information with the various contractors, NASA established the "NX" server. ECF No. 8 at 8.

On December 6, 2016, NASA informed SSL that a data breach occurred that included proprietary data from SSL located on a NASA NX server at NASA's Langley Research Center. ECF No.1 at 3. NASA provided further updates and informed SSL that an Orbital employee committed the breach. *Id.* at 4. SSL also learned that at least four files containing its proprietary data had been opened/and or viewed by as many as six Orbital employees. *Id.* Following up on this information, SSL contacted Orbital regarding the details and scope of the breach, and Orbital provided a response. ECF No. 1 at 4-6; No. 8-2 at 1. SSL filed this action seeking judicial intervention to protect its confidential and proprietary information and damages as a result of Orbital's alleged unauthorized access. ECF No. 1 at 5-6.

II. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) provides for the dismissal of actions that fail to state a claim upon which relief can be granted. For purposes of a Rule 12(b)(6) motion, courts may only rely upon the complaint's allegations and those documents attached as exhibits or incorporated by reference. *See Simons v. Montgomery Cty. Police Officers*, 762 F.2d 30, 31 (4th Cir. 1985). Courts will favorably construe the allegations of the complainant and assume that the facts alleged in the complaint are true. *See Erickson v. Pardus*, 551 U.S. 89, 93-94 (2007); *Mylan Laboratories, Inc. v. Matkari*, 7 F.3d 1130, 1134 (4th Cir. 1993). A court will only grant a motion to dismiss if "it appears to a certainty that the plaintiff would be entitled to no relief under any state of facts which could be proved in support of his claim." *Johnson v. Mueller*, 415 F.2d 354 (4th Cir. 1969).

Although a complaint need not contain detailed factual allegations, "[f]actual allegations must be enough to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). If the factual allegations alleged by the plaintiff do not nudge the plaintiff's claims "across the line from

conceivable to plausible, their complaint must be dismissed." *Id.* at 570. A plaintiff however is generally permitted to plead facts based on "information and belief" if such plaintiff is in a position of uncertainty because the necessary evidence is controlled by the defendant. *See Raub v. Bowen*, 960 F. Supp.2d 602, 615 (E.D. Va. 2013).

III. DISCUSSION

Count I: Violation of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.* (2008), is primarily a criminal statute, *see A.V. ex rel Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009), but a person who suffers damages or loss may bring a civil action for compensatory damages, injunctive or other equitable relief if the conducts involves one of the factors set forth in (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i),[1] *see* 18 U.S.C. § 1030(g) (2008). Though SSL did not specify the CFAA provisions Orbital violated, SSL states in its Response to the Motion to Dismiss that Orbital violated §§§1030(a)(2)(B), (a)(2)(C), and (a)(5)(C).[2] *See* ECF No. 12 at 20.

A cause of action under §1030(a)(2)(B) requires SSL to show that Orbital: (1) intentionally; (2) accessed a computer; (3) without authorization or exceeded its authorized access; and (4) obtained information from a department or agency of the United States; (5) which resulted in a loss to one or more persons during any one-year period aggregating at least $5,000 in value or damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

Likewise, to state a cause of action under § 1030(a)(2)(C), the defendant must have: (1) intentionally; (2) accessed a computer; (3) without authorization or exceeded its authorized access;

---

[1] Plaintiff must allege one of the following factors: (I) "loss to 1 or more persons during any 1–year period ... aggregating at least $5,000 in value"; (II) "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals"; (III) "physical injury to any person"; (IV) "a threat to public health or safety"; or (V) "damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(c)(4)(A)(i) (2008).

[2] SSL states that Orbital's conduct involves sub clause I and sub clause V. *See* ECF No. 12 at 21.

and (4) obtained information from any protected computer; (5) resulting in a loss to one or more persons during any one-year period aggregating at least $5,000 in value or damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

Lastly, to state a violation of § 1030(a)(5)(C), SSL must assert that Orbital: (1) intentionally (2) accessed a "protected computer" (3) without authorization, and, as a result of such conduct, (4) caused damage and loss (5) to one or more persons during any one-year period aggregating at least $5,000 in value.

In its Complaint, SSL alleges that Orbital, through at least one employee, intentionally accessed a computer at NASA Langley, an agency of the United States, without authorization. ECF No. 1 at 16-17. Further, SSL alleges it sustained losses that exceeded $5,000 in value during a one-year period, and that a computer used by the United States in furtherance of national defense or security was damaged. *Id.* at 17-18. In opposition, Orbital argues it did not access the information "without authorization" and that SSL fails to sufficiently plead damages or loss. *See generally* ECF No. 8 at 11. Orbital does not appear to dispute the sufficiency of the other elements however. Accordingly, the Court having reviewed the allegations taken as true and in the light most favorable to the plaintiff, finds that SSL pled sufficient facts to satisfy these elements and will limit its analysis to the elements that Orbital disputes.

i. "Without Authorization" and "Exceeds Authorized Access"

The CFAA does not define "without authorization" but defines "exceeds authorized access." "Exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030 (e)(6) (2008). The United States Court of Appeals for the Fourth Circuit ("Fourth Circuit") has held that these terms should be construed narrowly. *See WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (holding that because the statute's provisions apply

to civil and criminal actions, the terms are to be construed narrowly). In *WEC Carolina Energy Sols. LLC*, the Fourth Circuit held that a person accesses a computer "without authorization" when he or she "accesses a computer without permission." 687 F.3d at 206. Moreover, a person "exceeds authorized access" within the meaning of the statute when he or she "has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." *Id.* at 204; *see also id.* at 206 (holding that a person exceeds authorized access when he or she "obtains or alters information on a computer beyond that which he [or she] is authorized to access.").

Here, SSL alleges that Orbital accessed its proprietary and confidential information via the NASA NX server, and that the breach occurred because "an employee of another contractor, Orbital ATK, accessed files on NASA's NX Server beyond the files the employee was authorized to view." ECF No. 1 at 3-4. Orbital does not deny the breach occurred, but argues that because the former employee was authorized to access certain files on NASA's NX Server as a part of its work on the CIRAS Tipping Point Project, SSL's propriety and confidential information was not accessed within the statute's meaning. *See* ECF No. 8 at 11-15; No. 15 at 11-12. In support of its position, Orbital cites *State Analysis, Inc. v. American Fin. Servs. Assocs.*, 621 F. Supp. 2d 309 (E.D. Va. 2009), and *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005). The Court finds these cases distinguishable however.

In *State Analysis,* the court held that the defendant did not "exceed authorization" within the meaning of the CFAA because the complaint did not allege that the defendant had obtained or altered information it was not entitled to: rather the allegation was that the defendant had used the information in an inappropriate way. 621 F. Supp.2d at 317. In contrast, SSL alleges that an Orbital employee accessed files "beyond the files the employee was authorized to view." *See* ECF No. 1 at 3-4. Unlike the plaintiff in *State Analysis, Inc.*, SSL alleges that Orbital never received authorization

to view its files. For similar reasons, Orbital's reliance on *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005) also fails.

In *SecureInfo*, a licensee of the plaintiff's software was alleged to have shared the software with a competitor of the plaintiff and the plaintiff sued the competitor for violations of the CFAA. The court held that because the licensee had given the competitor permission to access the software using its license, the competitor could not have intentionally acted without authorization or in excess of its authority within the meaning of the statute. *SecureInfo*, 387 F. Supp. 2d at 609-10. This case is distinguishable however. Unlike the defendant in *SecureInfo*, that accessed the software through a valid license which permitted authorization, SSL's pleading, that an "employee accessed files on NASA's NX Server beyond the files the employee was authorized to view," essentially alleges that SSL never granted Orbital access to view its files. *See* ECF No. 1 at 3-4. Indeed, such an inference is supported by Orbital's own brief which explains that the NX server was set up "[i]n order for NASA to share information with the various contractors working with NASA *on their respective Tipping Point projects* – including Orbital ATK and SSL." ECF No. 8 at 8 (emphasis added).

Moreover, Orbital's argument fails because it is contrary to the Fourth Circuit's holding in *WEC Carolina Energy Sols. LLC.* Indeed, that case was decided after the cases Orbital cites and clarifies the scope of the terms "without authorization" and "exceeds authorized access." The Fourth Circuit held that the terms "without authorization" and "exceeds authorized access" applies when an individual "accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access." *WEC Carolina Energy Sols. LLC*, 687 F.3d at 206. Here, SSL's allegation that another contractor "accessed files on NASA's NX server beyond the files the employee was authorized to view," meets the statute's definition of "exceeds authorized access."

ii. "Damage or Loss"

SSL also alleges that Orbital's conduct caused losses in the aggregate amount of over $5,000 and resulted in "damage affecting a computer used by or for an entity of the United States

Government in furtherance of the administration of justice, national defense or national security." *See* ECF No. 12 at 17-18. In opposition, Orbital argues that SSL fails to adequately plead damages or loss. ECF No. 15 at 6-8. To Orbital, SSL's alleged losses are not actionable because losses under the CFAA are costs incurred by the party responsible for the system that was breached — not a third party. *Id.* at 8. Moreover, Orbital contends that SSL has not sufficiently pled damages because the complaint is unsupported by any evidence that the integrity or availability of its documents were impaired or that such information was used, altered or removed from the server. *See* ECF No. 8 at 15-16.

The CFAA defines loss as any "reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030 (e)(11) (2008). Although Orbital argues that the CFAA only contemplates costs incurred by the party responsible for the system but not third parties, ECF No. 15 at 8, this conclusion is contrary to the statute's plain language which states that loss means any "reasonable cost to ***any victim***," *see* § 1030 (e)(11) (emphasis added). Indeed, neither the plain language of the statute nor the case law excludes third parties.

Moreover, the Fourth Circuit has held that loss under the CFAA is a "broadly worded provision," and considers "costs incurred as a part of the response to a CFAA violation, including the investigation of an offense." *See A.V. ex rel Vanderhye*, 562 F.3d at 646. Here, SSL presents the costs it incurred as a result of the alleged CFAA violation that included conducting a damage assessment and convening and communicating with NASA and Orbital regarding the alleged breach. *See* ECF No. 1 at 17. In addition, SSL alleges that the amount of the loss exceeded well over $5,000 in value during a one-year period and the Court assumes that the facts alleged are true. *Id*; *see also Erickson*, 551 U.S. at 93-94.

Lastly, Orbital contends that SSL cannot state a cause of action for damages. ECF No. 8 at 15. The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030 (e) (8) (2008). Orbital cites a number of cases from other districts and argues that SSL's claims relate solely to the loss of trade secrets and that documents had been accessed and copied — items not recoverable under the statute. *See* ECF No. 8 at 15-16. The Court is unaware of any relevant case law from this circuit addressing this issue, but the Court need not tackle this issue as SSL sufficiently pleads "loss."

Under §§1030(a)(2)(B) and 1030(a)(2)(C), a plaintiff need only show damage or loss, and that the conduct involves one of the four factors under § 1030(c)(4)(A)(i). *See* § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."). Therefore, Plaintiff has pled a cause of action under 18 U.S.C. §§1030(a)(2)(B) and 1030(a)(2)(C).

Accordingly, the Motion to Dismiss Count I is DENIED.

Count II: Defend Trade Secrets Act

In Count II, Plaintiff alleges violations of the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1832 *et seq.* (2016). Under the DTSA, "An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." §1836 (b)(1). The DTSA defines trade secrets as "all forms and types of financial, business, scientific, technical, economic, or engineering information . . ." that "the owner thereof has taken reasonable measures to keep . . . secret." § 1839(3). This information must also "derive independent economic value . . . from not being generally known . . . ." *Id.*

Thus, SSL must allege: (1) it owns a trade secret; (2) the trade secret was misappropriated; and (3) the trade secret implicates interstate or foreign commerce. *Id.* at § 1836 (b)(1) Orbital argues

however that SSL's trade secret claims are inadequately pled. ECF No. 8 at 17. Upon review of the alleged facts, the Court finds that Plaintiff pleads a cause of action for misappropriation of trade secrets.

First, the complaint satisfies the first element. SSL's complaint provides factual descriptions of the breached documents including their relation to its technological development for robotic satellite assembly, system engineering, and research and development. *See* ECF No. 1 at 14-15, 18. These descriptions meet the DTSA's broad definition of trade secrets. Moreover, SSL sufficiently pleads that it took reasonable efforts to keep this information secret by including proprietary markings and labels describing the highly sensitive nature of the materials. *Id.* at 15. Finally, SSL sufficiently pleads that it derived independent economic value from the documents being kept secret because they contained financial data, business plans, and procurement strategies, and were created after considerable economic investment — the disclosure of which could create an unfair competitive advantage. *See id.* at 9, 15, 20-22; *see also Hawkins v. Fishbeck*, No. 3:17-CV-00032, 2017 WL 4613664, at*5 (E.D. Va. Oct. 15, 2017) (holding that trade secrets derived independent economic value where they included pricing, service delivery planning and decisions, and collaboration with outside software development firm).

Second, Plaintiff sufficiently pleads Orbital "misappropriated" a trade secret. Misappropriation is defined as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or [ ] disclosure or use of a trade secret of another without express or implied consent . . . ." § 1839(5). Moreover, the "disclosure or use" category requires that the discloser or user (i) "used improper means to acquire knowledge of the trade secret," (ii) "knew or had reason to know that the knowledge of the trade secret was . . . derived from or through a person who had used improper means to acquire the trade secret," and was "acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit

the use of the trade secret . . . ," or (iii) "knew or had reason to know that the trade secret was a trade secret," and was "acquired by accident or mistake." *Id.*

Here, Plaintiff alleges that a "data breach had occurred involving proprietary data from SSL residing on a NASA NX server . . . because an employee of another contractor accessed files on NASA's NX server beyond the files the employee was authorized to view," and through updates, learned the contractor was Orbital ATK. ECF No. 1 at 3-4. In addition, SSL pleads that:

> Orbital ATK, acting through at least one of its employees, with intent to convert SSL's trade secrets, and in knowing and willful violation of NASA policies and, upon information and belief, in violation of Orbital ATK's contractual and fiduciary duties to NASA not to access information and data belonging to competitors, improperly and without authorization from NASA, accessed SSL's highly sensitive, confidential, and proprietary information, files, documents, and data.

Id. at 19.

These facts taken as true satisfy the pleading requirement for misappropriation because it plausibly alleges "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means." The facts also support an inference of the "disclosure . . . of a trade secret . . . without express or implied consent," through "improper means" and that Orbital at the very least "knew or had reason to know that the trade secret was a trade secret," and that it was "acquired by accident or mistake." *See* § 1839(5).

Finally, Plaintiff must demonstrate that the trade secret implicates interstate or foreign commerce. Defendant does not dispute this element and the Court finds the pleading sufficient. Here, the purported information relates to services used and intended for use in interstate and foreign commerce because it contains business plans, procurement strategies and subcontractor and vendor relationships. *See* ECF No. 1 at 18; *see also Hawkins*, 2017 WL 4613664, at*6 (holding that Plaintiff satisfied interstate commerce element where trade secret contained information related to commerce with other developers, marketing plans, and feedback with potential customers).

Accordingly, the Motion to Dismiss Count II is DENIED.

Count III: Misappropriation of Trade Secrets

SSL's third cause of action alleges that Orbital misappropriated its trade secrets in violation of the Virginia Uniform Trade Secrets Act ("VUTSA"), Va. Code Ann. § 59.1-336 *et seq.* (West 2017). The VUSTA's elements are similar to the DTSA and require a plaintiff to prove: (1) the existence of a "trade secret"; and (2) the "misappropriation" of that trade secret by the defendant. *Trident Prods.& Servs., LLC v. Canadian Soiless Wholesale, Ltd*, 859 F. Supp. 2d 771, 778 (E.D. Va. 2012) *aff'd per curiam*, 505 F. App'x 242 (4th Cir. 2013) (citing *MicroStrategy, Inc. v. Li*, 268 Va. 249, 263 (Va. 2004)). Moreover, an alleged trade secret must "meet all the criteria listed in the statute: (1) independent economic value; (2) not known or readily ascertainable by proper means; and (3) subject to reasonable efforts to maintain secrecy." *Id.*; *see also* Va. Code Ann. § 59.1-336 (West 2017).

Second, to prove misappropriation, the plaintiff must establish two elements: (1) that the defendant acquired, disclosed, or used a trade secret developed by the plaintiff through improper means (namely, without express or implied consent); and (2) that the defendant knew or had reason to know that its knowledge of the trade secret was either acquired under circumstances giving rise to a duty to maintain its secrecy or derived through a person owing such a duty to the plaintiff. *Trident Prods.& Servs., LLC*, 859 F. Supp. 2d at 780.

Given the similarity of elements with the DTSA, and upon review of SSL's pleadings, the Court finds that Plaintiff also states a cause of action for trade secret misappropriation under the VUTSA.

Accordingly, the Motion to Dismiss Count III is DENIED.

Count IV: Virginia Computer Crimes Act

In Count IV, SSL alleges that Orbital violated the Virginia Computer Crimes Act ("VCCA"), Va. Code Ann. § 18.2-152.3 (West 2017). To show a violation of the VCCA, a plaintiff must demonstrate that the defendant: (1) used a computer or computer network without authority; (2) with

the intent to obtain property or services by false pretenses, embezzle or commit larceny, or convert the property of another. *Ford v. Torres*, No. 1:08cv1153 (JCC), 2009 WL 537563, at *7 (E.D.Va. Mar. 3, 2009) (citation omitted); *see also*, Va. Code Ann. § 18.2-152.3 (West 2017). Under the VCCA, a person acts without authority when "he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission." § 18.2-152.2.

Taking all facts in the complaint as true and construing them in favor of Plaintiff, Plaintiff has pled a violation of the VCCA. Plaintiff alleges that Orbital intentionally used NASA's NX server without authorization or exceeding authorized access to obtain its proprietary information and trade secrets for unauthorized purposes. *See* ECF No.1 at 22-23. These allegations are sufficient to state the elements of the claim: Defendant used a computer network "without authority," and used it to wrongfully appropriate Plaintiff's property. Although Defendant argues that Plaintiff cannot make a viable claim because it had authority to access the server, ECF No. 8 at 22, the Court is not persuaded. On the contrary, it is clear that the VCCA's definition of use of a computer network without authority applies when a person acts in a manner knowingly exceeding such right, agreement, or permission. *See* § 18.2-152.2. In this case, Plaintiff pleads sufficient facts that demonstrate such action.

Accordingly, the Motion to Dismiss Count IV is DENIED.

Count V & VI: Conversion & Unjust Enrichment

Plaintiff's remaining claims are for common law conversion and unjust enrichment. In opposition, Defendant argues these claims should be dismissed because they are preempted. ECF No 8. at 23. Plaintiff contends however they are not because the parties disagree on the trade secret status of SSL's information. ECF No.12 at 30. The Court finds that the VUTSA preempts Plaintiff's common law claims.

The VUTSA contains a preemption provision which provides:

> A. Except as provided in subsection B of this section, this chapter displaces conflicting tort, restitutionary, and other law of this Commonwealth providing civil remedies for misappropriation of a trade secret.
>
> B. This chapter does not affect:
> 1. Contractual remedies whether or not based upon misappropriation of a trade secret; or
> 2. Other civil remedies that are not based upon misappropriation of a trade secret; or
> 3. Criminal remedies, whether or not based upon misappropriation of a trade secret.

Va. Code Ann. § 59.1-341 (West 2017).

Indeed, "the plain language of the preemption provision indicates that the [VUTSA] was intended to prevent inconsistent theories of relief for the same underlying harm by eliminating alternative theories of common law recovery which are premised on the misappropriation of a trade secret." *Smithfield Ham and Prods. Co., Inc. v. Portion Pac, Inc.*, 905 F. Supp. 346, 348 (E.D. Va. 1995). Stated differently, "the preemption provision is intended to preclude only those common law claims . . . premised *entirely* on a claim for misappropriation of a trade secret." *Id.* (citation omitted). Therefore, for the VUTSA to preempt the remaining conversion and unjust enrichment claims, these claims must be predicated "entirely" on Orbital's alleged misappropriation of trade secrets. Civil remedies not exclusively based on the misappropriation of a trade secret are not preempted. *See id.*; § 59.1-341.

Here, it is clear from Plaintiff's pleadings that its conversion and unjust enrichment claims are premised entirely on an alleged misappropriation of trade secrets. In the pleadings for conversion and unjust enrichment, SSL incorporates all of its previous claims and their factual allegations. *See* ECF No.1 at 23-24. Notably, SSL incorporates claims that require a showing of the existence of a trade secret. *See supra* Section III. Counts II-Count IV. Moreover, SSL also alleges that "Orbital ATK wrongfully appropriated and exercised authority over SSL's Confidential Information," and that Orbital ATK "has been unjustly enriched by the receipt and appreciation of benefits resulting from the unauthorized access and conversion of SSL's Confidential Information," *Id.* Here, SSL's

pleadings show that the common law claims are entirely premised on the misappropriation of trade secrets. Indeed, SSL does not offer any alternative theories. As such, the VUTSA preempts these remaining claims.

Accordingly, the Motion to Dismiss Count V & VI is GRANTED.

IV. CONCLUSION

For the reasons outlined above:

Defendant's Motion to Dismiss Count I is DENIED.

Defendant's Motion to Dismiss Count II is DENIED.

Defendant's Motion to Dismiss Count III is DENIED.

Defendant's Motion to Dismiss Count IV is DENIED.

Defendant's Motion to Dismiss Count V is GRANTED.

Defendant's Motion to Dismiss Count VI is GRANTED.

The Clerk is **DIRECTED** to electronically provide a copy of this Order to all parties.

IT IS SO ORDERED.

Norfolk, Virginia
February 2, 2018

Raymond A. Jackson
United States District Judge