Navistar, Inc., et al vs. New Baltimore Garage, Incorporated Doc. 34

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

NAVISTAR, INC., ET AL.	)	
	)	
Plaintiffs,	)	
	)	Case No. 11-cv-6269
v.	)	
	)	Judge Robert M. Dow, Jr.
NEW BALTIMORE GARAGE, INCORPORATED,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Plaintiffs Navistar, Inc. ("Navistar") and International Truck Intellectual Property Company, LLC ("International") (collectively "Plaintiffs") allege that Defendant New Baltimore Garage's unauthorized use and distribution of codes needed to access Plaintiffs' computer system enabled unauthorized third parties to access Plaintiffs' proprietary and confidential materials and intellectual property, in direct violation of the parties' agreements and to the detriment of Plaintiffs and their authorized dealers. Plaintiffs' original complaint asserts claims for (1) breach of contract; (2) violation of the Digital Millennium Copyright Act ("DMCA"); (3) violation of the Computer Fraud and Abuse Act ("CFAA"); and (4) misappropriation of trade secrets. Defendant has moved to dismiss all claims. In response, Plaintiffs have filed a motion for leave to amend their complaint, which Defendant opposes. Plaintiffs' amended complaint contains additional factual allegations as well as two new claims for unjust enrichment (Count II) and contributory copyright infringement (Count VI). For the reasons set forth below, the Court grants in part and denies in part Defendant's motion to dismiss [17] and grants Plaintiffs' motion for leave to amend [24], subject to the limitations set forth in this opinion.

Dockets.Justia.com

I. Background[1]

Navistar manufacturers, sells, and services trucks, buses, engines, and parts. Navistar operates in segments, and, as relevant here, the International Truck Intellectual Property Company segment holds and administers the intellectual property of Navistar. Navistar creates, develops, oversees, controls, and utilizes proprietary and confidential information essential to Navistar's success. Compl. at ¶ 11–12. A significant aspect of Navistar's business is the merchandising and licensing of distinctive elements associated with its products and services, including material protected under U.S. copyright law. Navistar enters into license agreements before authorizing others to access or use this information, as well as Navistar's other intellectual property. *Id.* at ¶¶ 20, 22–24. Navistar has implemented a variety of measures to protect this information, including technological barriers to prevent unauthorized access, such as its "Dealer Communication Network" ("DCN"). *Id.* at ¶¶ 18–24. Navistar's DCN is a password-protected computer system that enables only authorized users access to some of Navistar's confidential information and intellectual property subject to the "DCN System and Services Agreement," which prohibits use of DCN, or the underlying materials and information, by unauthorized parties. *Id.* Notably, this agreement specifically prohibits sharing with or otherwise distributing passwords to third parties and using a third party's password to gain access to DCN. *Id.* at ¶ 24.

Plaintiffs allege that on August 11, 2008, Navistar sent Defendant a cease and desist letter when it was alerted that Defendant may have provided a third party, Liberty Equipment Repair, with unauthorized access to DCN. *Id.* at ¶ 25. When third party Liberty Equipment's license with Navistar terminated in 2005, it was no longer authorized to access DCN and the information

[1] For purposes of ruling on Defendant's motion to dismiss and Plaintiff's motion to amend, the Court assumes as true all well-pleaded allegations set forth in Plaintiffs' complaint and Plaintiffs' proposed amended complaint. See, *e.g.*, *Killingsworth v. HSBC Bank Nevada, N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

and materials contained on the network. *Id.* at ¶ 27–29. New Baltimore responded to the correspondence, denying that it authorized a third party to access DCN.

Relying on Defendant New Baltimore's representation, in July 2009, Navistar hired investigative firm Pinkerton to ascertain whether any unauthorized access had occurred, how, and the extent of the damage resulting from any breach. From July through November 2009, Pinkerton investigated Plaintiffs' concerns, including an investigation of Liberty. Plaintiffs allege that Pinkerton's investigation of Liberty revealed evidence of Liberty employees (1) logging into Navistar's website on August 10, 2009, and printing off a spindle specification, (2) logging into Navistar's website on August 31, 2009, using a DYY access code, and (3) logging into Navistar's website on September 18, 2009, using a DYY access code and printing steering gear specifications. Navistar's authorized dealer, International Trust Sales of Richmond ("ITSR"), eventually filed a complaint against Liberty in Virginia state court. Plaintiffs allege that during discovery in the Virginia case, Liberty Equipment admitted that it and its employees continued to surreptitiously access and utilize DCN with the permission of New Baltimore, which at all times relevant had a DCN password. *Id.* at ¶¶ 30–32. According to Plaintiffs, this access was in direct contravention of the terms of Navistar's agreement with New Baltimore. *Id.* at ¶ 24.

II. Legal Standards

A motion to dismiss pursuant to Rule 12(b)(6) tests the sufficiency of the complaint, not the merits of the case. See *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). To survive a Rule 12(b)(6) motion to dismiss, the complaint first must comply with Rule 8(a) by providing "a short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), such that the defendant is given "fair notice of what the * * * claim is and

the grounds upon which it rests." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). Second, the factual allegations in the complaint must be sufficient to raise the possibility of relief above the "speculative level," assuming that all of the allegations in the complaint are true. *E.E.O.C. v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007) (quoting *Twombly*, 550 U.S. at 555). "[O]nce a claim has been stated adequately, it may be supported by showing any set of facts consistent with the allegations in the complaint." *Twombly*, 550 U.S. at 563. The Court accepts as true all of the well-pleaded facts alleged by the plaintiff and all reasonable inferences that can be drawn therefrom. See *Barnes v. Briley*, 420 F.3d 673, 677 (7th Cir. 2005).

Leave to amend a complaint should be freely given "when justice so requires." Fed. R. Civ. P. 15(a). However, it is well settled that a district court may deny a motion for leave to amend when the amended pleading would be futile. *Bethany Phamacal Co. v. QVC, Inc.*, 241 F.3d 854, 861 (7th Cir. 2001). An amended complaint is futile if it could not withstand a motion to dismiss. See *Smart v. Local 702 Int'l Bhd. of Elec. Workers*, 562 F.3d 798, 811 (7th Cir. 2009).

III. Analysis

Plaintiffs seek leave to amend their complaint to add a few new factual allegations and two new counts. Defendants seek dismissal of all counts in the original complaint and maintain that the proposed amended complaint would be futile. In ruling on the parties' motions, the Court will consider together the various arguments presented by the parties in briefing both motions.

A. Violation of DMCA (Count III of Proposed Amended Complaint)

Plaintiffs allege that Defendant violated the Digital Millennium Copyright Act ("DMCA"). Specifically, Plaintiffs allege that Defendant "circumvented the digital security of

Navistar's [DCN] and related computers which protected Navistar's materials and Defendant trafficked in the means to do so." Congress enacted the DMCA in 1998 "to strengthen copyright protection in the digital age." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001); see also *Egilman v. Keller & Heckman, LLP.*, 401 F. Supp. 2d 105, 112 (D.D.C. 2005). Section 1201 of the DMCA addresses liability for circumventing systems that protect copyrights. See 17 U.S.C. § 1201. Based on their response brief, Plaintiffs appear to bring their claim pursuant to §§ 1201(a)(1), (a)(2), and (b)(1) of the DMCA.

Section 1201(a)(1)(A) provides: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A). Section 1201(a)(2)(A) provides that no person "shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that * * * is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under" the copyright laws. 17 U.S.C. § 1201(a)(2)(A). To "circumvent a technological measure" means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Further, "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." § 1201(a)(3)(B).

Section 1201(b)(1) provides that no person "shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that * * * is primarily designed or produced for the purpose of circumventing

protection afforded by a technological measure that effectively controls access to a work protected under" the copyright laws. 17 U.S.C. § 1201(b)(1). To "circumvent protection by a technological measure" means "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." § 1201(b)(2)(A). Further, "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." § 1201(b)(2)(B).

Regardless of which section of the statute applies, Plaintiffs' allegations are the same. Plaintiffs have alleged that they restricted access to their copyright-protected work by using a network that required a username/password combination to access. The precise issue raised by these allegations is whether providing a third party with access to Plaintiffs' computer system through the unauthorized use of a valid password constitutes circumvention of a technological measure or trafficking in technology designed to circumvent access or copy controls. Defendant asserts that Plaintiffs' DMCA claim fails because improper use of a password issued by the copyright holder—specifically, providing a third party with that password—does not amount to "circumvention" under the DMCA. Defendant's position finds support in district court decisions around the country. See, *e.g.*, *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004); *R.C. Olmstead, Inc. v. CU Interface LLC*, 2009 WL 3049867 (N.D. Ohio 2009); *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 113–14 (D.D.C. 2005). Plaintiffs counter that Defendants' cases are distinguishable because they address claims under section § 1201(a)(1) whereas their claim is asserted under § 1201(a)(2) or (b)(1). A number of California district court cases support Plaintiffs' interpretation of the statute. See, *e.g.*, *Actuate Corp. v. International Business*

Machines Corp., 2010 WL 1340519, at *5 (N.D. Cal. 2010); *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004); *Microsoft Corp. v. EEE Business Inc.*, 555 F. Supp. 2d 1051 (N.D. Cal. 2008). The Seventh Circuit has yet to weigh in on the precise issues identified in this case.

In determining whether unauthorized password use constitutes a violation of § 1201 of the DMCA, the court in *I.M.S.* held that the plaintiff's password system was within the definition of "technological measure" as the term is defined in the DMCA. 307 F. Supp. 2d at 531-32. Nonetheless, the court concluded that the plaintiff's allegations did not constitute circumvention under the DMCA because, although the defendant's actions bypassed permission to access the plaintiff's copyrighted works, they were not a *circumvention* of the technological means to protect the copyrighted material. *Id.* at 532. The *I.M.S.* court stated:

> Circumvention requires * * * descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure qua technological measure. In the instant matter, defendant is not said to have avoided or bypassed the deployed technological measure in the measure's gatekeeping capacity. The Amended Complaint never accuses defendant of accessing the [website] without first entering a plaintiff-generated password.

Id. Because the defendant "did not surmount or puncture or evade any technological measure" but instead "used a password intentionally issued by plaintiff to another entity," the court found that there was no circumvention under § 1201(a)(1). The court noted that "what defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure's author. Unlike the CFAA, a cause of action under the DMCA does not accrue upon unauthorized and injurious access *alone;* rather, the DMCA targets the *circumvention* of digital walls guarding copyrighted material." *Id.* The Court further concluded that it was irrelevant who provided the username/password combination to the defendant, or, given that the combination itself was legitimate, how it was obtained.

Plaintiffs' allegations demonstrate that "an otherwise legitimate, owner-issued password" (*I.M.S.*, 307 F. Supp. 2d at 531) was used to access their website; these allegations fall squarely within the *I.M.S.* court's conclusion that, "[w]hatever the impropriety of defendant's conduct, the DMCA and the anti-circumvention provision at issue do not target" the unauthorized use of a "password intentionally issued by plaintiff to another entity." *Id.* at 533; see also *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d at 114. Plaintiffs contend that the cases supporting Defendant's argument focus on a narrow construction of the term "circumvention" because the focus is on the password, rather than the technology at issue (i.e. the password-protected network). Whether the focus is on the password or the network, Plaintiffs must adequately allege circumvention or trafficking. Acts of circumvention expressly limited by the statute are descrambling a work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing a "technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). There is no question here that Plaintiffs have alleged that they were attempting to "effectively control[] access to a work." § 1201(a)(3)(B). However, viewing the allegations in light of persuasive authority, using a password to access a copyrighted work, even without authorization, does not constitute "circumvention" under the DMCA because it does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a "technological measure." Instead, it amounts to unauthorized access to Plaintiffs' system, which itself does not appear to be a violation of this particular statute. See also *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 692 (D. Md. 2011).

Furthermore, with respect to the anti-trafficking portion of the statute, Plaintiffs have not sufficiently alleged that Defendant trafficked in "any technology, product, service, device,

component, or part thereof, that * * * is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively controls access to a work protected under" the copyright laws. 17 U.S.C. § 1201(b)(1). The allegations are that Defendant provided an authorized password to a third-party who was not an authorized user of the password. The allegations do not support a theory that Defendant developed a means (for instance, by creating software, purposely disabling a security measure, or supplying an access key) to distribute Plaintiffs' materials to the public for profit. Compare *Actuate Corp.*, 2010 WL 1340519, at *5 (posting plaintiff's software and related materials for sale to consumers for profit); *321 Studios*, 307 F. Supp. 2d 1085 (creating and distributing software to the public for profit); *Microsoft Corp. v. EEE Business Inc.*, 555 F. Supp. 2d 1051 (distributing Microsoft software and licensing key outside a licensing restriction to consumers for profit). Instead, Plaintiffs' allegations amount to a theory that Defendant shared its password with a third-party; such an action simply does not appear to be covered by the DMCA. As evident from the additional causes of action asserted in their proposed amended complaint, Plaintiffs have several avenues by which they can pursue damages for the conduct at issue; however, the Court does not believe that Congress intended the DMCA to cover the conduct complained of in this instance.

B. Violation of the CFAA (Count IV of Proposed Amended Complaint)

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, provides for the entry of civil injunctive relief as well as the recovery of money damages for a violation of its provisions. See 18 U.S.C. § 1030(g) (providing that "[a]ny 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"). In Count IV of the proposed amended complaint (Count III of the original complaint), Plaintiffs allege that

Defendant "intentionally accessed Navistar's computer system without authorization and/or exceeded the access authorized by Navistar" and, as a result, "accessed and obtained confidential and proprietary business information from a protected computer in interstate commerce." Plaintiffs also maintain that Defendant's conduct caused them to suffer "a loss of at least $5,000." Defendant contends that this claim is time-barred and, in any event, that Plaintiffs have failed to state a cause of action.

The CFAA provides for civil liability if one "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage * * *." 18 U.S.C. § 1030(a)(5)(A)(iii). A plaintiff must demonstrate damage in order to recover under this provision of the CFAA. See *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 766 (N.D. Ill. Feb. 11, 2009); *Garelli Wong & Associates, Inc. v. Nichols*, 551 F. Supp. 2d 704, 708-09 (N.D. Ill. 2008). The CFAA defines "damage" as "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

The CFAA provisions at issue in this case prohibit "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, * * * thereby obtain[ing] information from any protected computer," (see 18 U.S.C. § 1030(a)(2)(C)), and "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1–year period" (see 18 U.S.C. § 1030(a)(4)).[2]

[2] Congress amended several sections of the CFAA in September 2008. See Identity Theft Enforcement and Restitution Act, Pub.L. No. 110–326, §§ 203–208, 122 Stat. 3560, 3561–63 (2008). Because the parties have identified no substantive change in language relevant to the Court's current analysis, and because the conduct at issue in this case allegedly occurred both before and after the date of amendment,

Although the CFAA generally is criminal in nature, it also provides a private right of action for a person "who suffers damage or loss by reason of a [CFAA] violation." 18 U.S.C. § 1030(g). "Thus, to recoup compensatory damages, a plaintiff must show *either* damage or loss." *US Gypsum Co. v. Lafarge N. Am. Inc.*, 670 F. Supp. 2d 737, 743 (N.D. Ill. Oct. 27, 2009) (emphasis in original); see also *Motorola, Inc. v. Lemko Corp.*, 609 F.Supp.2d 760, 767 (N.D. Ill. Feb. 11, 2009). Defendant argues that Plaintiffs' CFAA claim must be dismissed for failure to state a claim, because Plaintiffs have failed to adequately allege either "damage" or "loss" as defined by the CFAA.

The CFAA defines the term "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Courts have interpreted the CFAA's definition of damage to include the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any "diminution in the completeness or usability of the data on a computer system." *Cassetica Software, Inc. v. Computer Sciences Corp.*, 2009 WL 1703015, at *3 (N.D. Ill. June 18, 2009); see also *Mintel Int'l Group, Ltd. v. Neergheen*, 2010 WL 145786, at *9 (N.D. Ill. Jan. 12, 2010); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 810 (N.D. Ill. Mar. 19, 2009); *Motorola*, 609 F.Supp.2d at 769 ("The plain language of the statutory definition refers to situations in which data is lost or impaired because it was erased or because (for example) a defendant smashed a hard drive with a hammer."). On the other hand, the mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement. See *Mintel*, 2010 WL 145786, at *9 ("copying, e-mailing or printing electronic files from a computer database is not enough to satisfy the damage requirement of the CFAA"); *Del Monte*,

---

all citations in this opinion are to the CFAA in its amended form. See *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 719 n.12 (N.D. Ill. Apr. 24, 2009).

616 F.Supp.2d at 811 ("copying electronic files from a computer database—even when the ex-employee e-mails those files to a competitor—is not enough to satisfy the damage requirement of the CFAA"). Courts also have found that the disclosure of trade secrets misappropriated through unauthorized computer access does not qualify as damage under the CFAA's definition of the term. See *U.S. Gypsum Co.*, 670 F. Supp. 2d at 744 ("the CFAA is not intended to expansively apply to all cases where a trade secret has been misappropriated by use of a computer"); *Motorola,* 609 F. Supp. 2d at 769 ("The only harm [plaintiff] has alleged is the disclosure to a competitor of its trade secrets and other confidential information. The CFAA's definition of damage does not cover such harm * * *."); *Nichols,* 551 F. Supp. 2d at 710 ("Though [plaintiff] would like us to believe that recent amendments to the CFAA are intended to expand the use of the CFAA to cases where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show 'impairment to the integrity or availability of data, a program, a system, or information.'") (quoting 18 U.S.C. § 1030(e)(8)).

At most, Plaintiffs have alleged that they were concerned that Defendant may have impaired the integrity of its data, thus causing Plaintiffs to investigate the extent of Defendants' (or third parties) unauthorized access to, and acquisition of, Plaintiffs' confidential information. Plaintiffs have not pleaded that Defendant actually impaired their databases or data as those terms have been interpreted and therefore have not satisfied the "damage" requirement of the CFAA.

In addition to a "damage" component, the CFAA also has a "loss" component. The CFAA defines the term "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). District courts within this circuit have interpreted this language in different ways. Compare *Cassetica Software, Inc. v. Computer Sciences Corp.*, 2009 WL 1703015, at *4 (N.D. Ill. June 18, 2009) (finding that the CFAA's definition of "loss" applies only to "costs of 'conducting a damage assessment * * * incurred *because of the interruption of service*'") (emphasis in original), with *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. Apr. 24, 2009) ("As defined in section 1030(e)(11), 'loss' means two things: first, 'any reasonable cost to the victim,' such as responding to the offense or otherwise restoring lost material; second, lost revenue or other damages incurred as a result of an interruption of service."). The Seventh Circuit has not yet ruled on this point of law.

Plaintiffs have alleged that they incurred costs associated with investigating the extent of unauthorized access to their network. They also claim that Defendant's activities "impair interfere with, and hinder Navistar's business, burden and impair Navistar's computer systems and personnel resources; impair efficiency, fairness and simplicity of Navistar systems and services; and harm, interfere with, and impair Navistar's relationship, reputation and goodwill with legitimate Navistar users." Defendant argues that Plaintiffs cannot plausibly allege that they suffered any loss as defined by the CFAA, because Plaintiffs did not sustain any damage to its computers, data, or databases, nor have Plaintiffs alleged any interruption of service. In response, Plaintiffs argue that "any reasonable cost to any victim" can be considered a loss under the CFAA, including "the cost of responding to an offense."

Based on the plain language of the CFAA, the Court concludes that a plaintiff can satisfy the CFAA's definition of loss by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as

defined by the CFAA. See *Farmers Ins. Exchange v. Auto Club Group*, 823 F. Supp. 2d 847, 851-56 (N.D. Ill. 2011); *1st Rate Mortg. Corp. v. Vision Mortg. Servs. Corp.*, 2011 WL 666088, at *2 (E.D. Wis. Feb. 15, 2011) (agreeing with plaintiffs that "the CFAA allows recovery for losses sustained even if data or computers were not damaged"); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 811 (N.D. Ill. Mar. 19, 2009) ("The CFAA states that a company that pays for damage assessment may satisfy the loss requirement."); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 768 (N.D. Ill. Feb. 11, 2009) (allegations of loss "related to damage and security assessments * * * are sufficient to allege loss for purposes of the CFAA").[3] Thus, at a minimum, Plaintiffs have stated a CFAA claim by alleging that they incurred costs in investigating an alleged CFAA offense.

Defendant's other argument—that Plaintiffs' CFAA claim is time-barred—fares no better at this stage. It is undisputed that the CFAA is governed by a two-year statute of limitations that "begins to run when the plaintiff knew or reasonably should have known that he or she was wrongfully injured." *Horbach v. Kaczmarek*, 288 F.3d 969, 973 (7th Cir. 2002). At this stage, the parties dispute (i) when Plaintiffs learned that they had been injured, and (ii) whether Defendant actively concealed any wrongdoing and involvement. Because of these disputes, the Court cannot determine whether Plaintiffs' CFAA claim falls outside the two-year statute of limitations; therefore, dismissal of the CFAA claim on a limitation ground at this early stage is not warranted.

[3] The Court acknowledges the presence of conflicting case law within this circuit. See *Von Holdt v. A–1 Tool Corp.*, 714 F.Supp.2d 863, 875–76 (N.D.Ill. May 17, 2010) (requiring "damage to the computer or computer system" before a plaintiff can prove "loss" under the CFAA); *Cassetica Software, Inc. v. Computer Sciences Corp.*, 2009 WL 1703015, at *4 (N.D. Ill. June 18, 2009) ("The CFAA only permits the recovery of costs incurred for damage assessment or recovery when the costs are related to an interruption of service.").

C. Misappropriation of Trade Secrets (Count V of Proposed Amended Complaint)

Defendant's argument for dismissal of Plaintiffs' misappropriation of trade secret claim is not well taken. Defendant maintains that Plaintiffs have brought a common law claim that is preempted by the ITSA. As Plaintiffs state in the first paragraph of both the original complaint and the proposed first amended complaint, "[t]his action has been filed by the Plaintiff to combat Defendant's wrongful conduct and includes claims for * * * violation of the Illinois Trade Secrets Act (765 Ill. Comp. Stat. 1065/1-9)." Even if Plaintiffs had not made it expressly clear in the first paragraph that their claim was brought under the Illinois Trade Secret Act, pleading each element of the claim (which Plaintiffs have done) would suffice for notice pleading requirements. See, *e.g. Rohler v. TRW, Inc*., 576 F.2d 1260, 1264 (7th Cir. 1978) (statute need not be cited if facts alleged support claim). Defendant's motion to dismiss Plaintiffs' misappropriation of trade secret claim is denied.

D. Unjust Enrichment (Count II of Proposed Amended Complaint)

Plaintiffs have pled unjust enrichment as an alternative to their breach of contract claim. To state a claim based on a theory of unjust enrichment under Illinois law, "a plaintiff must allege that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience." *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 545 N.E.2d 672, 679 (Ill. 1989). Under Illinois law, "[w]hen two parties' relationship is governed by contract, they may not bring a claim of unjust enrichment unless the claim falls outside the contract." *Utility Audit, Inc. v. Horace Mann Serv. Corp.*, 383 F.3d 683, 688–89 (7th Cir.2004). "In determining whether a claim falls outside a contract, the subject matter of the contract governs, not whether the contract contains terms or provisions related to the claim." *Id.* As previously indicated,

Plaintiffs have pled this claim in the alternative, which they are entitled to do. Discovery will shed light on whether a contract governs the dealings between the parties and also on whether Plaintiffs' unjust enrichment claim is preempted by the ITSA; until then, Plaintiffs may proceed with their claim of unjust enrichment. See *FAIP North America, Inc. v. Sistema s.r.l.*, 2005 WL 3436398, at *6 (N.D. Ill. Dec. 14, 2005).

E. Contributory Copyright Infringement (Count VI of Proposed Amended Complaint)

Plaintiffs' proposed amended complaint brings a cause of action for contributory copyright infringement. Plaintiffs allege that (1) Navistar owns valid copyright registrations; (2) third party, Liberty Equipment, infringed Navistar's copyrighted works; (3) Defendant induced/caused/encouraged that third party to infringe Navistar's copyright or contributed in a significant way to the infringing party's infringement of Plaintiff's copyright; and (4) Defendant knew of the third party's infringing activity. At this stage, no more is required. See, *e.g. Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2011 U.S. Dist. LEXIS 82955 at *20-*21 (N.D. Ill. July 27, 2011). Plaintiffs have satisfied the notice pleading requirement and sufficiently state a claim for contributory copyright infringement in the proposed amended complaint.

F. Breach of Contract (Count I of Proposed Amended Complaint)

Plaintiffs have brought a breach of contract claim, alleging that Defendant breached Navistar's Dealer Communication Network System and Services Agreement through improper use of the DCN, improper use of the Dealer's ID and password, improper access to the DCN, violation of good faith and fair dealing obligations, improper disclosure, improper reporting, improper communication, violation of confidentiality agreement, copyright violations, improper distribution, and improper grant of permission. Defendant objects to Plaintiffs' breach of contract claim, arguing that "[b]ecause the conduct underlying the contributory copyright

infringement and breach of contract claims is the same, the breach of contract claim – like the contributory copyright infringement claim – would not survive a motion to dismiss." As the Court indicated in addressing the copyright claim, at this stage, Plaintiffs have provided more than enough information to put Defendant on notice of the contributory copyright infringement claim against it and the grounds upon which that claim rests. Likewise, Plaintiffs have sufficiently apprised Defendant of their breach of contract claim and the grounds upon which this claim rests. The Court denies Defendant's motion to dismiss Plaintiffs' breach of contract claim.

IV. Conclusion

For these reasons, the Court grants in part and denies in part Defendant's motion to dismiss [17]. The Court grants Defendant's motion to dismiss Plaintiffs' DMCA claim and denies the motion in all other respects. The Court grants Plaintiffs' motion to amend [24], subject to the limitations set forth in this opinion. At this time, Plaintiffs' DMCA claim is dismissed without prejudice; however, the Court cautions Plaintiffs that the claim as set forth in the proposed amended complaint would not survive a motion to dismiss for the reasons stated in this opinion. If Plaintiffs believe that they can allege additional facts that will cure the deficiencies noted, they may seek leave of court within fourteen days to include a DMCA claim in their amended complaint. Otherwise, Plaintiffs are directed to file their amended complaint (without the DMCA claim) within twenty-one days of the date of this order.

Dated: September 20, 2012

Robert M. Dow, Jr.
United States District Judge