TPM

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

NEJLA K. LANE and LANE LEGAL SERVICES, P.C., an Illinois Professional Corporation,	)	
Plaintiffs,	)	**No. 15 C 6177**
v.	)	**Chief Judge Rubén Castillo**
STEPHEN KENJI LE BROCQ,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

This case stems from a failed business relationship between two attorneys. Nejla K. Lane ("Lane") and her law firm Lane Legal Services, P.C., ("LLS" or "the firm") (collectively "Plaintiffs") claim that when leaving his employment at LLS, Stephen Kenji Le Brocq ("Defendant") stole information off of the firm's computers in violation of the Stored Wire and Electronic Communications and Transactional Records Access Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, and the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.* (R. 36, Am. Compl.) They also assert numerous state law claims, including breach of contract, fraud, and a violation of the Illinois Trade Secrets Act ("ITSA"), 765 ILL. COMP. STAT. 1065/1 *et seq.* (*Id.*) Defendant moves to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). (R. 39, Def.'s Mot. to Dismiss.) For the reasons stated below, the motion is granted in part and denied in part.

RELEVANT FACTS

Lane is an Illinois resident who is licensed to practice law in Illinois and Michigan. (R. 36, Am. Compl. ¶ 3.) She is also a licensed private detective who has been operating under the

name Key Private Investigation Bureau, LLC, ("KPI") since 2012. (*Id.* ¶ 7.) LLS is an Illinois law firm incorporated by Lane in 2007 with its principal place of business in Chicago, Illinois. (*Id.* ¶¶ 4, 20.) The firm's practice areas include family law, immigration law, criminal law, and personal injury cases. (*Id.* ¶ 19.) Defendant is an attorney residing in Illinois who is licensed to practice in Illinois and Texas. (*Id.* ¶ 5.)

In May 2013, when Defendant was a 22-year-old law student, he began working as a "volunteer law clerk" at LLS while pursuing his law degree. (*Id.* ¶ 21.) Defendant was later offered an externship with the law firm Motherway & Napleton, LLP, and from August 2013 through December 2013, Defendant worked at both LLS and Motherway & Napleton. (*Id.* ¶¶ 22-23, 27.) Shortly after beginning with Motherway & Napleton, Defendant told Lane that he had received an offer of employment from the firm, with an annual salary of $180,000.00 and a signing bonus of $35,000.00. (*Id.* ¶ 24.) Lane later learned that this was untrue, but at the time she was concerned about losing Defendant as an employee, so she offered him a position with LLS. (*Id.* ¶¶ 24-25.)

On May 22, 2013, the two signed an agreement specifying the terms of Defendant's employment at LLS, including the scope of his duties and salary. (*Id.* ¶¶ 25-26; R. 36-1, Agreement.) Lane claims that she entered this agreement only because the parties orally agreed that Defendant would remain at LLS for at least five years after obtaining his Illinois law license. (R. 36, Am. Compl. ¶ 28.) Lane also provided Defendant with a business debit card in his own name, as well as a gym membership and other benefits. (*Id.* ¶ 28.) The debit card was intended to be used solely for business expenses. (*Id.* ¶ 31.)

In May 2014, Defendant became licensed to practice in Illinois and continued working as a staff attorney for LLS under the previously agreed-upon terms. (*Id.* ¶ 29.) Soon thereafter, Lane

added Defendant as an authorized user on all of LLS's business accounts. (*Id.* ¶ 31.) In July 2014, Lane leased a larger office space so that Defendant could have his own private office. (*Id.* ¶ 32.) Lane and Defendant negotiated the lease for this office space together. (*Id.* ¶ 33.)

On September 29, 2014, Defendant drafted a supplement to the parties' employment agreement that added additional provisions about bonuses and holidays. (*Id.* ¶ 36; R. 36-1 Suppl. Agreement at 9.) Lane signed the supplemental agreement and specified that it was to be "effective on 1/1/2015." (R. 36, Am. Compl. ¶¶ 38-39.) Sometime prior to January 1, 2015, Lane reviewed the supplemental agreement and discovered certain "errors" within it. (*Id.* ¶ 39.) She drafted a new contract with certain changes to ensure consistency with LLS's past practices and fee-sharing agreements with outside counsel. (*Id.*) This second supplemental agreement was signed by the parties on February 18, 2015. (*Id.* ¶ 39; R. 36-1, Second Suppl. Agreement at 11.) Although Defendant was not yet a named partner of LLS, the agreement granted him certain benefits similar to those of a partner, including advances on top of his salary and a right to be consulted by Lane in decisions "that affect LLS overall." (R. 36, Am. Compl. ¶¶ 41-42.)

Around this same time, Lane "became weary of [Defendant's] constant complaints" about his high interest student loans, and advanced him $55,000 to help him reduce his loans. (*Id.* ¶¶ 45-46.) Lane claims that the parties understood that, because of this advance, "going forward, Lane would not pay [Defendant] a salary when LLS' payroll account was low on funds." (*Id.* ¶¶ 48-49.)

On April 14, 2015, Lane formed a limited partnership with Defendant under the name "Lane Le Brocq & Lange, LLP," with Lane as a managing partner and Defendant as a junior partner. (*Id.* ¶¶ 8, 51.) Lane claims that she did so only because Defendant promised her that he would stay with the firm through at least December 2019. (*Id.* ¶ 51.) On April 29, 2015,

Defendant passed the Texas bar exam. (*Id.* ¶ 53.) On Saturday May 9, 2015, Defendant notified Plaintiffs by email that he was terminating his employment. (*Id.* ¶¶ 53-54.) Lane telephoned Defendant several times that day, but he did not answer any of her calls and instead responded via text message. (*Id.* ¶ 55.) Lane asked Defendant if they could meet in person to discuss his departure, but he refused. (*Id.*)

The following day Lane went to LLS's office and discovered that Defendant's desk was empty. (*Id.* ¶ 56.) The office computer and monitor that he had been using were allegedly missing, as was other LLS property. (*Id.*) Among other things, Defendant allegedly stole several books, a credit card payment processing device, and the office petty cash. (*Id.* ¶ 80.) Lane contacted Defendant and requested that he return the property he had removed; she also told him that she wanted to discuss "a proper exit method" from the firm. (*Id.* ¶ 57.) Defendant responded via text messages "demanding, among other things, a waiver for past advances and a release of all claims with regards to the newly entered five (5) year lease agreement and/or his liability under their mutual agreement." (*Id.*) On May 11, 2015, Lane Le Brocq & Lange, LLP, was dissolved. (*Id.* ¶¶ 9, 51.)

A subsequent investigation by Plaintiffs revealed that Defendant had been using his business debit card for personal expenses and that he had improperly withdrawn cash using this debit card. (*Id.* ¶¶ 60, 70, 72.) Plaintiffs also discovered that, sometime on or before January 13, 2014, Defendant had copied and stolen "vast stores of LLS's electronic data and trade secrets." (*Id.* ¶ 61.) Plaintiffs also learned that Defendant had been planning to leave LLS and start his own firm for quite some time before his departure. (*Id.* ¶¶ 63-64.) On September 28, 2014, just one day before Defendant and Lane had signed their second supplemental employment agreement, Defendant had incorporated his own law firm in Texas under the name "Le Brocq

Law Group, P.C." (*Id.* ¶ 62; R. 36-1, Incorporation Documents at 13-14.) The following month, he had registered the domain name "lebrocqlawgroup.com." (R. 36, Am. Compl. ¶ 63.) After his departure, Defendant opened his own law office in Chicago under the name Le Brocq Law Group. (*Id.* ¶ 64.) Plaintiffs allege that Defendant never intended to remain with LLS for a five-year period as he had promised Lane, and that instead "[h]is sole agenda had been to start working at LLS in order to gain Lane's trust, exploit Lane's firm by stealing Plaintiffs' trade secrets, skills, clients and funds and then to secretly abandon his workplace." (*Id.* ¶ 65.)

Plaintiffs claim that when he left the firm Defendant stole an "enormous quantity of LLS's valuable electronic data, trade secrets, clients' list, and related properties that were compiled by Lane over a ten (10) year period." (*Id.* ¶ 64.) They claim that these electronic files were "the products of many years of . . . formulating strategies, skills, forms, clients list, and templates for vari[ous] areas of law." (*Id.* ¶ 98.) These files included:

> (a) Client contact information and lists that contain confidential client information, representing Plaintiffs' considerable efforts to develop and maintain client relationships and loyalty over the course of many years;
>
> (b) Videos of past/present clients for mock depositions and trial preparation;
>
> (c) Personal data of past/present clients (social security numbers, passport numbers, naturalization certificates, marriage certificates, divorce documents, and other private matters);
>
> (d) E-Mails and other communications concerning the firm's legal services in general and specific legal matters (confidential settlement communications with government agencies, criminal and civil communications, transcripts from proceedings, etc.);
>
> (e) Court filings and other litigation documents pertaining to specific clients and specific lawsuits/claims (civil, criminal, immigration files that pertain to clients' entire lives going back decades, etc.);
>
> (f) Transactional documents, such as wills, pertaining to specific clients and specific matters (including asset information, personal data, etc.);

> (g) Memorandum detailing attorney mental impressions regarding legal strategies and issues-drafts of opening statements/closing statements (investigation reports of witnesses with their home addresses and/or other personal data, etc.);
>
> (h) The firm's purchased Family Law disks that include forms, pleadings, etc., Criminal Law disks, Immigration Law disks with numerous templates for drafting litigation documents, such as motions and briefs, and for drafting transactional documents, such as wills; [and]
>
> (i) Photographs and videos of past/present clients as well as Lane's personal matters such as . . . funerals and weddings, or private pictures of many persons and events, including but not limited to Lane.

(*Id.*)

Lane claims that her office computer was password-protected and that she generally did not allow others to use it. (*Id.* ¶ 101.) But because she trusted Defendant and "had little knowledge of computers," she put Defendant "in charge of managing the information technology ('IT') aspects of LLS." (*Id.* ¶ 102.) Defendant was given Lane's computer password "to use for limited purposes, but Lane expressly forbade him from accessing old LLS files, or any of her KPI files or personal files." (*Id.*) Plaintiffs claim that sometime around August 2013, Defendant convinced Lane to change LLS's website hosting provider to a provider called "SiteGround." (*Id.* ¶ 104.) Lane permitted Defendant to make himself the administrator of the SiteGround account. (*Id.* ¶ 107.) The SiteGround account was accessible remotely through the internet by anyone with the username and password. (*Id.* ¶ 106.) Defendant also convinced Lane to switch to a "cloud-based" electronic storage system called "DropBox." (*Id.* ¶ 109.) This system was also accessible remotely through the internet. (*Id.* ¶¶ 109-110.) Plaintiffs allege that Defendant was only authorized to use LLS's computer network, the SiteGround account, and the DropBox account "in furtherance of his work duties as an attorney of LLS, and not for his own business activities." (*Id.* ¶ 114.)

An investigation conducted by LLS after Defendant left revealed that sometime prior to his departure, Defendant had accessed these accounts and copied "all or most of the files" located in them. (*Id.* ¶ 115.) During the investigation, Plaintiffs' new IT personnel also discovered large volumes of what appeared to be deleted files once belonging to Defendant's prior employers, including Motherway & Napleton. (*Id.* ¶¶ 119-21.) After learning of the data breach, Lane transferred the entire contents of her server to an external hard drive, which was later damaged. (*Id.* ¶ 118.) LLS also notified certain clients about the data breach, which caused a "panic" among them about the confidentiality of their information. (*Id.* ¶ 144.) Plaintiffs claim that Defendant's conduct "damaged Plaintiffs' reputation and relationship with their clients." (*Id.*)

Plaintiffs also learned that sometime prior to his departure, Defendant had logged into LLS's "E-File account" with the Circuit Court of Cook County using the firm's password, and substituted his personal email address for his LLS email address on the firm's notification list. (*Id.* ¶¶ 124-28.) As a result, the E-File system sent copies of electronic notices in LLS's cases to Defendant's personal email account. (*Id.* ¶ 128.) In August 2015, Plaintiffs removed Defendant from this account. (*Id.* ¶ 131.)

Plaintiffs claim that Defendant also made "illicit electronic transfers from LLS's Chase Bank business and payroll accounts to himself via an internal wire transfer called 'QuickPay.'" (*Id.* ¶¶ 67, 75-78.) Plaintiffs claim that these improper transfers continued for several days after Defendant left. (*Id.* ¶ 67.) Plaintiffs further allege that as a result of Defendant leaving the firm, Lane tried to terminate LLS's lease on the larger office space but was been unable to do so, making LLS liable for approximately $117,685.44 over the period of the lease. (*Id.* ¶ 66.)

PROCEDURAL HISTORY

In July 2015, Plaintiffs filed this action against Defendant alleging claims under the SCA, ECPA, CFAA, and various provisions of state law. (R. 1, Compl.) Defendant moved to dismiss for failure to state a claim (R. 9) and for sanctions under Federal Rule of Civil Procedure 11 (R. 23). Plaintiffs then sought leave to amend their complaint, which the Court granted. (R. 35, Minute Entry.) The Court denied Defendant's motions without prejudice. (*Id.*)

Plaintiffs then filed a 55-page amended complaint against Defendant[1] asserting eleven separate claims. (R. 36, Am. Compl.) In Count I, they allege that Defendant violated the SCA when he accessed files in LLS's electronic storage system without proper authorization for the purpose of furthering his own business interests. (*Id.* ¶¶ 132-49.) In Count II, they allege that Defendant violated the ECPA when he added his personal email to LLS's account and intercepted electronic communications sent by the Cook County E-Filing system to LLS. (*Id.* ¶¶ 150-63.) In Count III, Plaintiffs allege that Defendant violated the CFAA when he accessed Lane's computer and copied its contents without her authorization to further his own business interests. (*Id.* ¶¶ 164-85.) In Count IV, Plaintiffs allege that Defendant violated the ITSA by misappropriating Plaintiffs' trade secrets when he left the firm, including its client lists and trial-strategy materials. (*Id.* ¶¶ 186-206.) In Counts V through XI, Plaintiffs allege state common law claims of civil conversion, fraud in the inducement, breach of fiduciary duty, breach of contract, unjust enrichment, promissory estoppel, and tortious interference with contract. (*Id.* ¶¶ 207-55.)

Defendant moves to dismiss the amended complaint in its entirety under Rules 12(b)(1) and 12(b)(6). (R. 39, Def.'s Mot. to Dismiss.) Defendant argues that all three of Plaintiffs' federal claims fail to state a claim for relief and must be dismissed under Rule 12(b)(6). (*Id.* at

[1] Plaintiffs also asserted a claim against Bridget Metoyer, a former client of LLS's, but they have since settled with Metoyer and dismissed her as a defendant. (R. 46, Order.)

3.) Defendant further argues that because the federal claims must be dismissed, this Court should relinquish jurisdiction over all of Plaintiffs' state law claims. (R. 40, Def.'s Mem. at 9.) Alternatively, Defendant argues that the ITSA claim fails as a matter of law, and that this Court lacks subject matter jurisdiction over the remaining state law claims because they do not arise from the same set of facts as Plaintiffs' federal claims. (*Id.* at 9-10.) Plaintiffs contest the dismissal of their case. (R. 43, Pls.' Resp.) In their view, they have adequately pled claims under the three federal statutes as well as under the ITSA. (*Id.* at 2-10.) They further argue that this Court has supplemental jurisdiction over the state common law claims pursuant to 28 U.S.C. § 1367. (*Id.* at 11-14.)

LEGAL STANDARD

A Rule 12(b)(6) motion "challenges the viability of a complaint by arguing that it fails to state a claim upon which relief may be granted." *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014). In deciding a Rule 12(b)(6) motion, the Court construes the complaint in the light most favorable to the non-movant, accepts all well-pleaded factual allegations as true, and draws all reasonable inferences in the non-movant's favor. *Vesely v. Armslist LLC*, 762 F.3d 661, 664-65 (7th Cir. 2014). The Court can consider "allegations set forth in the complaint itself, documents that are attached to the complaint, documents that are central to the complaint and are referred to in it, and information that is properly subject to judicial notice."[2] *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013). To survive dismissal, a complaint must "contain sufficient factual matter . . . to 'state a claim to relief that is plausible

[2] Plaintiffs attached a number of documents to their amended complaint: the three employment agreements entered into by the parties, LLS's current lease, various letters, incorporation documents for the Le Brocq Law Group, QuickPay records, domain name records for www.lebrocqlawgroup.com, printouts of LLS and KPI computer file folders, and an affidavit from an IT specialist who examined LLS's computer systems after Defendant's departure. (R. 36-1, Pls.' Exs. at 1-64.) These documents will be treated as part of the amended complaint for all intents and purposes. *See* FED. R. CIV. P. 10(c); *Williamson*, 714 F.3d at 436.

on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

Rule 12(b)(1) provides for dismissal of a case when the Court lacks subject matter jurisdiction. FED. R. CIV. P. 12(b)(1). In deciding a motion to dismiss for lack of subject matter jurisdiction, the Court "must accept as true all well-pleaded factual allegations and draw all reasonable inferences in favor of the plaintiff." *Long v. Shorebank Dev. Corp.*, 182 F.3d 548, 554 (7th Cir. 1999). The Court may also look beyond the pleadings to "view whatever evidence has been submitted on the issue to determine whether in fact subject matter jurisdiction exists." *Id.* (citation omitted). The party invoking jurisdiction bears the burden of establishing that jurisdiction exists. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

ANALYSIS

I. Federal Claims

A. SCA

Defendant first argues that Plaintiffs' SCA claim fails as a matter of law. (R. 40, Def.'s Mem. at 2-4; R. 44, Def.'s Reply at 2-3.) The SCA provides criminal and civil liability when an individual "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. §§ 2701(a), 2707. Congress enacted the SCA "to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers 'deliberately gaining access to, and sometimes

tampering with, electronic or wire communications' by means of electronic trespass." *Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026 (N.D. Ill. 2010) (quoting S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557)). The statute defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).[3] "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A), (B).

Numerous courts have held that the SCA does not apply to the act of simply hacking into a personal computer to download information stored on a hard drive, because a personal computer does not constitute "a facility through which an electronic communication service is provided." *See, e.g.*, *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (observing that hacking into personal computers to retrieve information stored therein does not violate the SCA); *Int'l Bhd. of Elec. Workers, Local 134 v. Cunningham*, No. 12 C 7487, 2013 WL 1828932, at *4 (N.D. Ill. Apr. 29, 2013) ("[S]imply accessing a personal computer to obtain stored data would not run afoul of § 2701."); *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 335 (D.D.C. 2011) (the SCA "clearly is not triggered when a defendant merely accesses a physical client-side computer and limits his access to documents stored on the computer's local hard drive or other physical media").

Although the amended complaint is somewhat vague on this point, to the extent Plaintiffs are resting any part of their claim on Defendant having accessed and copied materials on Lane's

[3] The SCA incorporates by reference the statutory definitions contained in the ECPA. *See* 18 U.S.C. § 2711(1) (adopting definitions contained in 18 U.S.C. § 2510).

hard drive, this allegation fails to state a claim under the SCA. However, Plaintiffs also allege that Defendant accessed electronic files stored on cloud-based servers that were connected to the internet. (R. 36, Am. Compl. ¶ 135.) They further allege that some of the data he accessed consisted of emails. (*Id.*) These allegations are sufficient to trigger the SCA. *See Joseph v. Carnes*, No. 13-cv-2279, 2013 WL 2112217, at *3-4 (N.D. Ill. May 14, 2013) (denying motion to dismiss SCA claim where the plaintiffs alleged that the defendants had searched and reviewed the plaintiffs' emails without proper approval); *Gaubatz*, 793 F. Supp. 2d at 335-36 (denying motion to dismiss SCA claim where the plaintiff alleged that the defendants had accessed its computer servers and networks).

Defendant nevertheless argues that Plaintiffs' SCA claim fails because it is clear from the amended complaint that "Defendant was given access to the servers and Lane's computer."[4] (R. 40, Def.'s Mem. at 2.) It is true, as Defendant points out, that the SCA "prohibits only unauthorized access and not the misappropriation or disclosure of information." *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000). Thus, "there is no violation of section 2701 [by] a person with authorized access to the database no matter how malicious or larcenous his intended use of that access." *Id.*; *see also WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (the SCA does not extend "to the improper *use* of information validly accessed"); *BI3 v. Hamor*, No. 08 C 2384, 2009 WL 2192801, at *3 (N.D. Ill. July 15, 2009) (the SCA "prohibits unauthorized access to the facility, and would not protect

[4] Defendant argues that the amended complaint "fails to plead any facts remotely suggesting that the Defendant had violated his duty of loyalty on January 13, 2014, nearly a year and a half prior to his departure." (R. 44, Def.'s Reply at 2). The Court disagrees. Plaintiffs allege that Defendant had improper intentions from the very start of his employment in May 2013, and that his "sole agenda had been to start working at LLS in order to gain Lane's trust, exploit Lane's firm by stealing Plaintiffs' trade secrets, skills, clients and funds and then to secretly abandon his workplace." (R. 36, Am. Compl. ¶ 65.) They further allege that he had been making plans to open his own law firm for quite some time prior to his departure. (*Id.* ¶¶ 62-64.) The Court must accept Plaintiffs' allegations as true and afford Plaintiffs all reasonable inferences arising from these allegations. *Vesely*, 762 F.3d at 664-65.

the plaintiffs against misuse of information or property if access to the facility was authorized"). Indeed, the statute expressly provides that it "does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1).

Therefore, Plaintiffs' allegations that Defendant *misused* information to which he had been given access fails to state a claim for relief under the SCA. But that is not the end of the matter, because Plaintiffs also allege that Defendant exceeded the authorization he had been given by accessing data from Lane's "old LLS files," "KPI files," and "personal files," even though he had been expressly forbidden from doing so. (*Id.* ¶¶ 98, 102.) That makes this case distinguishable from the line of cases cited by Defendant. *See Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg. & Consulting, LLC*, 600 F. Supp. 2d 1045, 1050 (E.D. Mo. 2009) (dismissing SCA claim where the defendants had general authorization to access the plaintiff's computers and the plaintiff failed to identify "any restricted information that Defendants supposedly accessed"); *Sherman*, 94 F. Supp. 2d at 821 (concluding that the plaintiff failed to state a claim under the SCA where the defendant allegedly misused information that he was authorized to access, but recognizing that the statute's "prohibition on intentional exceeding of authorized access anticipates that a person with authorization to a computer database or certain public portions of a database is not thereby authorized to visit 'private' zones of data in the system"); *see also Joseph*, 2013 WL 2112217, at *4 (denying motion to dismiss SCA claim where the plaintiff alleged that the defendants exceeded their authority by accessing emails without proper authorization).

In summary, while Plaintiffs' allegations that Defendant misused information that he was authorized to access does not state a claim under the SCA, their allegations that Defendant

exceeded his authority by intentionally accessing materials that he had been expressly forbidden from accessing adequately states a claim under the SCA. For these reasons, the motion to dismiss is granted in part and denied in part as to this claim.

B. ECPA

Defendant next argues that Plaintiffs' ECPA claim fails as a matter of law. (R. 40, Def.'s Mem. at 5-6; R. 44, Def.'s Reply at 5-7.) "The ECPA was passed by Congress in 1986 to amend the Omnibus Crime Control and Safe Streets Action of 1968, commonly known as the Wiretap Act, in order to 'update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.'" *In re Google Inc. St. View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1078 (N.D. Cal. 2011) (quoting S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.). The ECPA imposes criminal and civil liability when an individual "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The statute defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). This definition encompasses emails. *United States v. Szymuszkiewicz*, 622 F.3d 701, 705 (7th Cir. 2010) (observing that "[e]mail messages are transfers of writings" within the meaning of the ECPA).

Plaintiffs allege that Defendant violated the ECPA when he "secretly accessed Plaintiffs' Cook County E-File account using their login information, accessed the list of 'alternative E-

Mails' for that account, and substituted his personal E-mail address . . . for his LLS E-Mail address . . . with the intent of contemporaneously intercepting Plaintiffs' e-Notices, and directing them to his own E-Mail account." (R. 36, Am. Compl. ¶¶ 154, 156.) Defendant argues that the ECPA claim fails as a matter of law because "Plaintiffs have failed to allege—plausibly or otherwise—that they had a reasonable expectation of privacy in any of the E-Notifications that Plaintiff allegedly intercepted." (R. 40, Def.'s Mem. at 5.)

The Court finds no basis to dismiss Plaintiffs' claim on this ground. The statute itself does not require that a plaintiff establish a privacy interest in the communication at issue, and instead provides a civil cause of action whenever an individual "intentionally intercepts. . . . [an] electronic communication" meeting the statutory definitions. 18 U.S.C. § 2511(1)(a). Defendant cites out-of-Circuit cases pertaining to the interception of *oral* communications in support of his expectation-of-privacy argument, but these cases are distinguishable. (*See* R. 40, Def.'s Mem. at 5 (citing *Kee v. City of Rowlett*, 247 F.3d 206, 211 (5th Cir. 2001); *United States v. Curtis*, 513 F. App'x 823, 825 (11th Cir. 2013); *United States v. Jones*, 56 F. App'x 416, 419 (9th Cir. 2003)).) The ECPA defines an "oral communication" as "any oral communication uttered by a person *exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.*" 18 U.S.C. § 2510(2) (emphasis added). Because of this language, a claim pertaining to the interception of an oral communication necessarily requires an examination of the speaker's expectation of privacy. There is no comparable requirement for electronic communications. *See* 18 U.S.C. § 2510(12).

Defendant also cites to a Ninth Circuit case for the principle that the "legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private." (R. 40, Def.'s Mem. at 5 (citing *Konop v. Hawaiian Airlines, Inc.*, 302

F.3d 868, 875 (9th Cir. 2002).) As Plaintiffs point out, however, Defendant has not provided the entire quote from that case, which reads: "The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, *such as email* and private electronic bulletin boards." *Konop*, 302 F.3d at 875 (emphasis added). The quote in its entirety actually undercuts rather than supports Defendant's argument, and suggests that emails are presumed to be private under the ECPA. Defendant has not cited any cases from this Circuit, nor has this Court located any, where a court dismissed a plaintiff's ECPA claim based on the interception of an email due to the plaintiff's failure to allege that he had a reasonable expectation of privacy in that email.[5]

It is true that no liability attaches under the ECPA based on interception of an electronic communication that is "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the public." 18 U.S.C. § 2511(2)(g)(i). But here Plaintiffs allege that Defendant had to log into LLS's password-protected E-File account to substitute his email address (R. 36, Am. Compl. ¶ 154), which suggests that the system was not configured to be readily available to the public. *See Konop*, 302 F.3d at 875 (comparing public website with one that is password-protected). A Cook County general order further supports the conclusion that the system is not configured to be public, as it

[5] Defendant cites to *In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 891 (N.D. Ill. 2012), to argue that this case must be dismissed due to Plaintiffs' failure to allege that the emails at issue were private. (R. 40, Def.'s Mem. at 6; *see also* R. 44, Def.'s Reply at 6-7.) In *Innovatio*, the court was not deciding whether the plaintiff stated a claim under the ECPA. Instead, the court's consideration of the ECPA arose in an unusual procedural posture: In the midst of a multi-district patent case, the court *sua sponte* ordered the plaintiff to brief the issue of whether it had breached the ECPA in gathering data to prosecute its patent infringement claims. *Id.* at 890. The court determined, based on the record evidence and expert reports that had been submitted, that the plaintiff had accessed data on a system that was configured to allow ready access to the public. *See id.* at 891. The court specifically distinguished the determination it was making from the determination made at the Rule 12(b)(6) stage, and noted that it was not required to accept the plaintiff's allegations as true. *Id.* at 893. Given these factual distinctions, this Court is not persuaded that *Innovatio* supports a dismissal at the pleading stage in this case.

requires individuals to register and obtain a user identification and password to access the E-Filing system. COOK CTY. CIRC. CT. GEN. ADMIN. ORDER NO. 2014-02, "Electronic Filing (eFiling) of Court Documents." The order also specifies that the user identification and password must be kept confidential. *Id.* § 4(e). Further factual development may show that the E-File system was configured in a way that allows access by the public, but at this stage the Court must accept Plaintiffs' allegations as true and construe all reasonable inferences in their favor. Plaintiffs allege enough to survive dismissal of this claim.[6] *See In re Google*, 794 F. Supp. 2d at 1083-84 (denying motion to dismiss ECPA claim based on the plaintiff's allegation that intercepted data was transmitted over networks that were not configured to be readily accessible by the public). The motion to dismiss will be denied as to this claim.

C. CFAA

Defendant next argues that Plaintiffs' CFAA claim must be dismissed. (R. 40, Def.'s Mem. at 6-9; R. 44, Def.'s Reply at 4-5.) "The CFAA . . . is primarily a criminal anti-hacking statute." *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016). However, the statute also "provides a civil remedy for any person who suffers damage or loss due to a violation" of the CFAA. *Id.* Plaintiffs claim here that Defendant violated Sections 1030(a)(2) and 1030(a)(4) of the CFAA. (R. 36, Am. Compl. ¶¶ 171, 176.) An individual

[6] It is not entirely clear to the Court that Defendant's conduct, as alleged, qualifies as an "interception" of Plaintiffs' email. As this Court reads the amended complaint, Plaintiffs allege that Defendant substituted his personal email address for his work email address in LLS's account so that he could receive his own copy of E-Notices that were also sent to LLS. (R. 36, Am. Compl. ¶¶ 128, 155-56; *see also* R. 43, Pls.' Resp. at 9 n.14.) This would not seem to involve the "interception" of Plaintiffs' emails. *See* 18 U.S.C. § 2510(4) (defining "intercept" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device"); *Konop*, 302 F.3d at 878 (observing that the plain meaning of "intercept" is "to stop, seize, or interrupt in progress or course before arrival" (citation omitted)). However, Defendant has not requested dismissal of the ECPA claim on this ground, and the Court presumes that the precise actions Defendant took will be further distilled in discovery. So too will Defendant's argument that he updated his own *personal* E-File account, rather than an account belonging to LLS. (R. 40, Def.'s Mem. at 6 n.1.) This argument cannot be evaluated at this stage as it requires consideration of matters outside the complaint.

violates Section 1030(a)(2) when he "[i]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[7] 18 U.S.C. § 1030(a)(2). A violation of Section 1030(a)(4) occurs when an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." 18 U.S.C. § 1030(a)(4). In this context, "intent to defraud" means that the individual acted "willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another." *Fidlar*, 810 F.3d at 1079 (citation omitted). Congress intended this provision "to reach cases of computer theft" as opposed to "mere trespass." *Id.* at 1080.

Defendant argues that Plaintiffs' CFAA claim fails as a matter of law because Plaintiffs admit in their complaint that Defendant had authorization to use LLS's computer system. (R. 40, Def.'s Mem. at 7.) The CFAA distinguishes between accessing a computer "without authorization" and accessing a computer while "exceed[ing] authorized use," 18 U.S.C. § 1030(a)(2), although the difference between these two terms is "paper thin," *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006). In *Citrin*, the U.S. Court of Appeals for the Seventh Circuit was called to decide the meaning of "exceeding authorization" under the CFAA in the context of a defendant-employee who was given a laptop to use in the course of his duties. *Id.* at 419. At some point, the defendant decided to quit and go into business for himself, in

[7] "Protected computer" means "a computer . . . used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B), which is "effectively all computers with Internet access," *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015) (citation omitted). As an aside, the Court disagrees with Plaintiff that *Valle* and other criminal cases interpreting the CFAA, ECPA, and SCA are irrelevant to this civil case. (R. 43, Pls.' Resp. at 7 & n.11.) When a statute has provisions with both civil and criminal applications, it must be interpreted uniformly in both contexts. *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("[W]e must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context[.]"); *see also WEC Carolina Energy*, 687 F.3d at 204 (observing that the CFAA must be interpreted uniformly in both the civil and criminal contexts).

breach of his employment agreement. *Id.* Before returning the laptop, he deleted all the data, and also installed a secure-erasure program to ensure that the data could not be recovered. *Id.* The Seventh Circuit held that the plaintiffs adequately stated a claim for a violation of the CFAA based on the defendant's conduct, even though the defendant had "authorization" to use the laptop in a general sense. *Id.* at 420. The Seventh Circuit reasoned that the defendant's "authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit . . . he resolved to destroy files that incriminated himself and other files that were the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee." *Id.* In other words, the defendant's breach of his duty of loyalty "terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-21.

District courts in this Circuit have routinely interpreted *Citrin* to permit a claim under the CFAA against a disloyal employee who uses an employer's computer for his own purposes.[8] *See, e.g.*, *Dental Health Prods., Inc. v. Ringo*, No. 08-C-1039, 2011 WL 3793961, at *3 (E.D. Wis. Aug. 25, 2011) ("In short, *Citrin* makes clear that most employee disloyalty cases can be pled as CFAA cases, because a disloyal employee has forfeited his right to access his employer's computer."); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009) ("Allegations that an employee e-mailed and downloaded confidential information for an improper purpose are sufficient to state a claim that the employee exceeded her authorization

[8] Defendant is correct that other Circuits have adopted different approaches, and some have criticized *Citrin*. *See Valle*, 807 F.3d at 524-28 (noting the "sharp division" among the Circuits and rejecting the interpretation of the Seventh Circuit and others that an employee's authorization is revoked any time the employee accesses a computer for a purpose contrary to the employer's interests); *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (rejecting approach of "our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty" and observing that those Circuits "failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access'"). But this Court must follow the law of the Seventh Circuit, and *Citrin* remains binding precedent here.

[under the CFAA]."). That is precisely what Plaintiffs allege here: they claim that Defendant took a position with LLS solely to "gain Lane's trust, exploit Lane's firm by stealing Plaintiffs' trade secrets, skills, clients and funds and then to secretly abandon his workplace." (R. 36, Am. Compl. ¶ 65.) Defendant's accessing LLS's computer system in furtherance of these intentions, and for reasons that were adverse to LLS's interests, adequately states a claim for "exceeding authorized use" under *Citrin*.

Defendant independently argues that the CFAA claim fails due to the lack of allegations establishing damage or loss. (R. 40, Def.'s Mem. at 7-8.) To recover under either Section 1030(a)(2) or 1030(a)(4), either "damage" or "loss" must be proven. *Fidlar*, 810 F.3d at 1079. A plaintiff need not allege both, however, and either will suffice. *See Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782, 791 (N.D. Ill. 2014) ("Plaintiff need only plead damage or loss to adequately plead a private right of action [under the CFAA]."); *Motorola*, 609 F. Supp. 2d at 767 ("[A] plaintiff alleging violations of sections 1030(a)(2) or (a)(4) need only allege damage or loss, not both.").

"Damage" is defined by the CFAA as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). This definition encompasses "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." *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011) (citation and internal quotation marks omitted). Courts have held that merely accessing, copying, or disseminating a company's trade secrets or other sensitive information does not satisfy the "damage" requirement. *Fidlar*, 810 F.3d at 1085 ("[B]y using the word 'damage,' . . . Congress intended this provision reach actual disruptions in service, not mere access, even if trespassory.");

Farmers, 823 F. Supp. 2d at 852 ("[T]he disclosure of trade secrets misappropriated through unauthorized computer access does not qualify as damage under the CFAA's definition of the term."); *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 994 (E.D. Wis. 2010) ("There is virtually no support for the proposition that merely accessing and disseminating information from a protected computer suffices to create a cause of action under the CFAA."); *U.S. Gypsum Co. v. Lafarge N. Am.*, 670 F. Supp. 2d 737, 744 (N.D. Ill. 2009) ("[T]he CFAA is not intended to expansively apply to all cases where a trade secret has been misappropriated by use of a computer.").

Put simply, the CFAA was meant to punish hackers, not "the disloyal employee who walks off with confidential information." *Kluber Skahan & Assoc., Inc. v. Cordogan, Clark & Assoc., Inc.*, No. 08-cv-1529, 2009 WL 466812, at *8 (N.D. Ill. Feb. 25, 2009) (citation omitted); *see also Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 813 (N.D. Ill. 2009) ("The CFAA should not be used to prosecute employees who are merely disloyal."). That is precisely the scenario described in Plaintiffs' complaint—a disloyal employee who allegedly "walked off" with confidential information. Although Plaintiffs claim that the theft of this information caused general "damage to their business and client relationships," (R. 36, Am. Compl. ¶ 181), they have not alleged the type of destruction or impairment to the integrity of their data that is covered by the CFAA. They have thus failed to allege "damage" for purposes of the CFAA.[9] *See Farmers*, 823 F. Supp. 2d at 852; *U.S. Gypsum Co.*, 670 F. Supp. 2d at 744.

[9] The Court is unpersuaded by Plaintiffs' citation to *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008), for the proposition that merely placing files on an unsecured server constitutes "damage" for purposes of the CFAA. (R. 43, Pls.' Resp. at 4 n.6.) The Court is persuaded instead by cases within this Circuit holding that some type of destruction, corruption, or diminution of the usability of data is required, as this interpretation best effectuates the purposes of the CFAA. *See Farmers*, 823 F. Supp. 2d at 852.

The CFAA defines "loss" as:

> [A]ny 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). The plaintiff must have suffered a loss in excess of $5,000 within a one-year period. 18 U.S.C. § 1030(c)(4)(A)(i)(I). Plaintiffs allege here that they "suffered losses in excess of $5,000 since May 11, 2015, to date, to investigate the extent of [Defendant's] breach [and] to re-secure their computer systems." (R. 36, Am. Compl. ¶ 181.) As Defendant points out, some courts in this District have taken the view that losses incurred from an investigation or assessment must themselves relate to an impairment or interruption of services to be covered by the CFAA. *Del Monte*, 616 F. Supp. 2d at 812-13 (in the absence of an impairment or unavailability of computerized data, costs incurred for a "damage assessment" are not recoverable under the CFAA); *Mintel Int'l Grp., Ltd. v. Neergheen*, No. 08-cv-3939, 2010 WL 145786, at *10 (N.D. Ill. Jan. 12, 2010) ("The alleged loss must relate to the investigation or repair of a computer or computer system following a violation that caused impairment or unavailability of data or interruption of service.").

However, more recently, courts in this District have permitted CFAA claims to proceed when the plaintiff has incurred costs due to an investigation, without regard to whether the investigation pertained to an actual disruption of service or impairment to the plaintiff's data. *See Epic Sys. Corp. v. Tata Consultancy Servs. Ltd.*, No. 14-CV-748, 2015 WL 7301245, at *6 (W.D. Wis. Nov. 18, 2015) (denying motion to dismiss where plaintiff alleged "loss" associated with the costs of an investigation even in the absence of actual damage to the computer system); *Pascal Pour Elle*, 75 F. Supp. 3d at 791 (recognizing "a split within the Circuit" but allowing

CFAA claim to proceed where plaintiff alleged that it paid $5,000 in "investigation and security assessment costs associated with the intrusion" notwithstanding a lack of allegations regarding damage or disruption to the system). Given the broad meaning of loss under the statute, the Court finds these cases persuasive, and concludes that Plaintiffs have alleged enough to proceed further with this claim.

II. State Claims

Turning to the state law claims, Defendant first argues that this Court should exercise its discretion to relinquish jurisdiction over all of Plaintiffs' state law claims. (*See* R. 40, Def.'s Mem. at 9-10.) Such action may have been warranted if the Court were dismissing all of Plaintiffs' federal claims. *See* 28 U.S.C. § 1367(c) ("The district courts may decline to exercise supplemental jurisdiction over a [state law] claim . . . [if] the district court has dismissed all claims over which it has original jurisdiction[.]"); *Harvey v. Town of Merrillville*, 649 F.3d 526, 533 (7th Cir. 2011) ("[I]t is the well-established law of this circuit that the usual practice is to dismiss without prejudice state supplemental claims whenever all federal claims have been dismissed prior to trial." (citation omitted)). But as outlined above, two of Plaintiffs' federal claims are proceeding. Accordingly, this argument has become moot. The Court turns to Defendant's remaining arguments pertaining to the state law claims.

A. ITSA Claim

Defendant argues that Plaintiffs' ITSA claim fails as a matter of law. (R. 40, Def.'s Mem. at 10-12.) Under the ITSA, an individual is entitled to recover damages for "misappropriation" of a "trade secret." 765 ILL. COMP. STAT. 1065/4(a), 1065/2. "Misappropriation" means:

> (1) acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means; or

(2) disclosure or use of a trade secret of a person without express or implied consent by another person who:

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was:

(I) derived from or through a person who utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

765 ILL. COMP. STAT. 1065/2(b).

"Trade secret," in turn, is defined as "information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers." 765 ILL. COMP. STAT. 1065/2(d). To qualify for protection, the information must be "sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use," and must also be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality." 765 ILL. COMP. STAT. 1065/2(d)(1)-(2). "The existence of a trade secret [under the ITSA] ordinarily is a question of fact," which "is best resolved by a fact finder after full presentation of evidence from each side." *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 723 (7th Cir. 2003) (citation and internal quotation marks omitted). "At the pleading stage, plaintiffs need only describe the information and efforts to maintain the confidentiality of the information in general

terms." *Scan Top Enter. Co. v. Winplus N. Am., Inc.*, No. 14 C 7505, 2015 WL 4945240, at *3 (N.D. Ill. Aug. 19, 2015).

In the amended complaint, Plaintiffs allege that Defendant misappropriated the following trade secrets when he left the firm:

> a) Client contact information and lists that contain confidential client information, representing Plaintiffs' considerable efforts to develop and maintain client relationships and loyalty over the course of many years, and that are of significant value to Plaintiffs' law firm;
>
> b) Memorandum detailing attorney mental impressions regarding legal strategies and issues;
>
> c) Templates and forms for drafting litigation documents, such as motions, briefs and settlement agreements, including templates and forms purchased by Plaintiffs from commercial vendors;
>
> d) Templates and forms for drafting transactional documents, such as wills, including templates and forms purchased by Plaintiffs from commercial vendors;
>
> e) Videos of past/present clients for mock depositions and trial preparation; and
>
> f) Materials for trial strategies, such as opening statements and closing arguments.

(R. 36, Am. Compl. ¶ 188.)

Defendant argues that Plaintiffs' ITSA claim fails because "Plaintiffs have not actually alleged the Defendant has yet used any of the supposed trade secrets *in his business* . . . much less that they have suffered any damages from such use." (R. 40, Def.'s Mem. at 10 (emphasis in original).) While proving unauthorized "use" of a trade secret is one means of establishing liability under the ITSA, it is not the only means; liability also attaches for improper "acquisition" or "disclosure" of a trade secret. 765 ILL. COMP. STAT. 1065/2(b)(1)-(2); *see also Parus Holdings, Inc. v. Banner & Witcoff, Ltd.*, 585 F. Supp. 2d 995, 1004-05 (N.D. Ill. 2008) (observing that "use is just one of three ways—improper acquisition, unauthorized use, or unauthorized disclosure—in which misappropriation can be shown" under the ITSA); *Destiny*

Health, Inc. v. Conn. Gen. Life Ins. Co., 39 N.E.3d 275, 282 (Ill. App. Ct. 2015) ("Under the Trade Secrets Act, misappropriation can be shown in one of three ways: by improper acquisition, unauthorized disclosure, or unauthorized use."). In their complaint, Plaintiffs clearly allege that Defendant wrongfully *acquired* its trade secrets through improper means[10] when he stole the information upon leaving the firm. (R. 36, Am. Compl. ¶ 202(a).) This allegation, if true, could establish a violation of the ITSA. 765 ILL. COMP. STAT. 1065/2(b)(1)-(2); *Destiny Health*, 39 N.E.2d at 282. Accordingly, the Court finds no basis to dismiss on this ground.

Defendant also argues that the claim fails because "none of the materials allegedly stolen qualify as trade secrets under the Act." (R. 40, Def.'s Mem. at 10.) In their response, Plaintiffs concede that "items purchased from commercial vendors may not constitute trade secrets." (R. 43, Pls.' Resp. at 9 n.15.) This concession is warranted, as "there generally can be no trade secret protection for a product that is available in the market." *U.S. Gypsum Co.*, 508 F. Supp. 2d at 623. The Court concludes that the items identified in subsections (c) and (d)—templates and forms "purchased by Plaintiffs from commercial vendors"—do not constitute trade secrets under the ITSA. (*See* R. 36, Am. Compl. ¶ 188(c), (d).)

Plaintiffs nevertheless argue that they have adequately alleged the existence of a trade secret with respect to their "client information and lists, legal memorandum, videos of past/present clients, and materials for trial strategies." (R. 43, Pls.' Resp. at 9.) As to the client information, Defendant argues that "an attorney or law firm's list of clients or their contact information" cannot possibly constitute a trade secret. (R. 40, Def.'s Mem. at 11.) As Plaintiffs point out, however, the statute itself defines trade secrets as including a "list of actual or potential

[10] "Improper means" for purposes of the ITSA includes "theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means." 765 ILL. COMP. STAT. 1065/2(a). Defendant does not dispute that Plaintiffs have adequately alleged this element.

customers." 765 ILL. COMP. STAT. 1065/2(d). It is worth noting again that whether information constitutes a trade secret is ordinarily a factual determination that should be made based on record evidence. *Learning Curve Toys*, 342 F.3d at 723. Specifically, courts have held that whether a customer list constitutes a trade secret depends upon factual issues that cannot be decided at the pleading stage, including the amount of effort expended to develop the list and the steps taken to keep it secret. *See Bankers Life & Cas. Co. v. Miller*, No. 14 CV 3165, 2015 WL 515965, at *7 (N.D. Ill. Feb. 6, 2015) (whether a customer list constituted a trade secret under the ITSA was "a question that cannot be answered without factual development"); *Buckley v. Abuzir*, 8 N.E.3d 1166, 1180 (Ill. App. Ct. 2014) (reversing dismissal of ITSA claim and observing that customer lists are entitled to trade secret protection "where they are sufficiently secret to derive economic value from being unknown to others and are the subject of reasonable efforts to maintain their secrecy"); *Liebert Corp. v. Mazur*, 827 N.E.2d 909, 922 (Ill. App. Ct. 2005) ("Whether customer lists are trade secrets depends on the facts of each case."); *see also RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 874-75 (N.D. Ill. 2001) (after a bench trial, concluding that the plaintiff's customer information constituted a "trade secret" within the meaning of the ITSA because it was not readily ascertainable from a public source and had been developed over a period of years).

Plaintiffs allege here that their client lists took "considerable efforts to develop" over the course of "many years." (R. 36, Am. Compl. ¶ 192.) They further allege that they derive economic value from this information not being readily available, and that they took pains to keep this information secret by password-protecting their accounts and providing access only to the firm's attorneys and staff, which during the relevant period consisted of fewer than five people. (*Id.* ¶¶ 189, 192.) Defendant suggests that anyone could obtain the client information

simply by examining Plaintiffs' public court filings. (R. 44, Def.'s Reply at 9.) However, it is not apparent from the complaint that every client on that list was represented by Plaintiffs in an actual court case, and if they were, it seems unlikely that the clients' personal contact information would have been included in court filings in which they were represented by counsel. At this stage, the Court must construe all reasonable inferences in Plaintiffs' favor, and Plaintiffs assert that it took them considerable time to amass this information. (R. 36, Am. Compl. ¶ 192.)

Defendant also argues that the client information was of no use to him because of the Illinois Rules of Professional Conduct, under which, he argues, "it is impermissible for attorneys to solicit clients." (R. 44, Def.'s Reply at 9 (citing ILL. R. PROF. CONDUCT 7.3)). Although unclear, Defendant may be trying to argue that the list had no economic value, *see* 765 ILL. COMP. STAT. 1065/2(d)(1), but the Rule that he cites does not prove that the client list was useless. The Rule only prohibits solicitation of clients through "in-person, live telephone or real-time electronic contact," and even then, it does not apply if the person being solicited had a "prior professional relationship with the lawyer." *See* ILL. R. PROF. CONDUCT 7.3(a). Presumably this exception would encompass anyone Defendant represented or developed a relationship with while working at LLS. In short, the Court concludes that Plaintiffs have adequately alleged the existence of a trade secret with respect to their customer lists. Whether the lists are ultimately entitled to trade secret protection will turn on factual determinations made at a later stage of the litigation.

Defendant next argues that there is no plausible basis to conclude that Plaintiffs' "legal memorandum, videos of past/present clients, and materials for trial strategies" constitute trade secrets. (R. 40, Def.'s Mem. at 11-12.) In Defendant's view, "[t]he legal world is swimming with

. . . trial strategy materials; they are readily available on Westlaw and Lexis Nexis; and any second year law student or paralegal can create them from scratch." (*Id.* at 12.) It is true that materials will not be considered trade secrets if they can be developed by those with expertise in the industry with "very little time, money, or effort." *Web Commc'ns Grp. v. Gateway 2000, Inc.*, 889 F. Supp. 316, 320 (N.D. Ill. 1995). However, Plaintiffs allege here that their trial strategy materials were the product of "substantial effort" by Lane over the course of "many years." (R. 36, Am. Compl. ¶ 98.) They further allege that they derive economic value from this information because it allows them "to save time and resources when providing legal services, which is necessary for the Plaintiffs to be competitive in the Illinois legal market." (*Id.* ¶ 191.) As with the customer lists, they allege that they made considerable efforts to keep this information secret. (*Id.* ¶ 189.) The Court concludes that Plaintiffs have adequately alleged a claim with respect to their trial strategy materials. For these reasons, the motion to dismiss will be granted regarding the templates and other commercially purchased materials, but denied as to Plaintiff's customer lists and trial strategy materials.

B. State Common Law Claims

Defendant's final argument is that this Court lacks supplemental jurisdiction over Plaintiffs' common law claims alleged in Counts V through XI (for conversion, fraud in the inducement, breach of fiduciary duty, breach of contract, unjust enrichment, promissory estoppel, and tortious interference with contract) because they do not arise from the same set of facts as Plaintiffs' federal claims. (R. 40, Def.'s Mem. at 12-15.) When a district court has original jurisdiction over a claim, it may exercise supplemental jurisdiction "over all other claims that are so related . . . that they form part of the same case or controversy under Article III." 28 U.S.C. § 1367(a). For supplemental jurisdiction to exist, the federal and state law claims must

"derive from a common nucleus of operative facts." *City of Chi. v. Int'l Coll. of Surgeons*, 522 U.S. 156, 164-65 (1997) (quoting *United Mine Workers v. Gibbs*, 383 U.S. 715, 725 (1966)). "To satisfy this requirement, a loose factual connection between the claims is generally sufficient." *McCoy v. Iberdrola Renewables, Inc.*, 760 F.3d 674, 683 (7th Cir. 2014) (citation and internal quotation marks omitted). "Different causes of action between the same parties that arise from the same contract and same events will ordinarily be part of the same case or controversy." *Id.*

The claims at issue here all involve the same parties and the same common nucleus of operative facts: Defendant's employment and departure from LLS. The federal claims focus on his theft of electronic information, but they are closely linked to the allegations underlying the state law claims for breach of fiduciary duty, breach of contract, conversion, and other common law violations. The basic theory underlying all of Plaintiffs' claims is that Defendant took a position with LLS, worked to gain Lane's trust, and then stole whatever he could—be it electronic information, trade secrets, or other firm property—in order to start his own legal practice. While there may not be a complete overlap in the facts relevant to the state and federal claims, there is at least a "loose factual connection" between them. *McCoy*, 760 F.3d at 683. That is all that is required. *See Healy v. Metro. Pier & Exposition Auth.*, 804 F.3d 836, 842 n.1 (7th Cir. 2015) (court had supplemental jurisdiction over state law claims because "all six counts in the lawsuit are . . . designed to address the alleged collusion between Defendants, which ultimately led to Plaintiffs' termination"); *McCoy*, 760 F.3d at 683-84 (in federal antitrust case, court had supplemental jurisdiction over state law claims for breach of contract and defamation where these claims "had a basis in at least a portion of those facts" underlying the federal antitrust claim); *Int'l Sports Mgmt., Inc. v. Stirling Bridge Grp., Inc.*, No. 03 C 9027, 2004 WL 1114760, at *3-4 (N.D. Ill. May 17, 2004) (in federal trademark case, court exercised

supplemental jurisdiction over state law claims for breach of contract, breach of duty of loyalty, unjust enrichment, and related claims because "all of Plaintiff's claims concern Defendants' alleged orchestrated scheme to poach [Plaintiff's] clients and start a competing company" (citation and internal quotation marks omitted)). Accordingly, the Court will exercise supplemental jurisdiction over Counts V through XI.

Before concluding, the Court must note that Defendant argues throughout his filings that the amended complaint is "full of perjury" and "made-up" allegations that were "fabricated" to harass him. (*See* R. 39, Mot. to Dismiss at 1-3; R. 40, Def.'s Mem. at 1.) Such arguments cannot afford Defendant any relief in connection with the present motion, because at this stage the Court must accept Plaintiffs' allegations as true. *Vesely*, 762 F.3d at 664; *Long*, 182 F.3d at 554. But if it is proven at a later stage of the litigation that Plaintiffs' allegations have no basis in fact, Defendant is free to renew his request for sanctions under Federal Rule of Civil Procedure 11.

CONCLUSION

For the foregoing reasons, the motion to dismiss (R. 39) is GRANTED in part and DENIED in part as stated herein. The parties are directed to reevaluate their settlement positions in light of this opinion and to exhaust all efforts to settle this case. The parties shall appear for a status hearing on May 3, 2016, at 9:45 a.m.

ENTERED:

Chief Judge Rubén Castillo
United States District Court

Dated: March 28, 2016