EFiled: May 10 2019 02:23PM EDT
Transaction ID 63254025
Case No. 2018-0600-KSJM

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

ALIXPARTNERS, LLP, and ALIXPARTNERS HOLDINGS, LLP, Plaintiffs,	)	
v.	)	C.A. No. 2018-0600-KSJM
DAVID BENICHOU, Defendant.	)	

OPINION

Date Submitted: January 31, 2019
Date Decided: May 10, 2019

Bradley R. Aronstam, Eric D. Selden, R. Garrett Rice, ROSS ARONSTAM & MORITZ LLP, Wilmington, Delaware; Robert S. Berezin, Nicholas J. Pappas, WEIL, GOTSHAL & MANGES LLP, New York, New York; *Counsel for Plaintiffs AlixPartners, LLP and AlixPartners Holdings, LLP*.

John P. DiTomo, Matthew R. Clark, Barnaby Grzaslewicz, MORRIS, NICHOLS, ARSHT & TUNNELL LLP, Wilmington, Delaware; *Counsel for Defendant David Benichou*.

McCORMICK, V.C.

The plaintiffs operate a global corporate restructuring advisory firm. The defendant was the managing partner of the plaintiffs' Paris office. As a partner, the defendant had access to the plaintiffs' confidential information. When he became a partner, the defendant also became party to a limited liability partnership agreement that contained confidentiality obligations. The defendant resigned from his position in early 2017. Shortly before his resignation, the defendant connected a personal data drive to his work-issued computer and accessed the plaintiffs' business files. Shortly after his resignation, the defendant repeated this act.

After his resignation, the defendant began working for one of the plaintiffs' competitors. Concerned that defendant may use their confidential information to benefit the competitor, the plaintiffs sought assurances from the competitor regarding the defendant's confidentiality obligations. The plaintiffs were dissatisfied with the competitor's response and initiated an investigative proceeding in Paris courts seeking targeted data searches of certain devices. The plaintiffs then sued in this court for breach of the confidentiality provisions of the limited liability partnership agreement. They also asserted three non-contractual claims for relief: for violating the Delaware Uniform Trade Secrets Act (or "DUTSA"), for common law conversion, and for violating the federal Computer Fraud and Abuse Act (or the "CFAA"). The defendant moved to dismiss each of the non-contractual claims.

The defendant's motion to dismiss the CFAA claim raises an issue of first

impression for this Court. The provision of the CFAA on which the plaintiffs rely renders liable a person who "intentionally accesses a computer *without authorization, or exceeds authorized access,* and thereby obtains . . . information from any protected computer[.]"[1] The plaintiffs argue that the defendant "exceeded authorized access" by using information in violation of the plaintiffs' limited partnership agreement and policies. The defendant argues that this language provides a narrow cause of action under which he can be liable for *unauthorized* access of protected computers only, not for *misuse* of information that he was authorized to access.

Federal courts split on the interpretation of the CFAA disputed by the parties, the Third Circuit has not weighed in, and district courts in the Third Circuit diverge. Relying on principles of statutory construction, this decision adopts the narrow approach first set forth by the Ninth Circuit in *LVRC Holdings LLC v. Brekka*.[2] Under the narrow approach, the defendant's actions while he was employed by the plaintiffs and had authorized access to the plaintiffs' confidential information do not support a claim under the CFAA. By contrast, it is reasonably conceivable that the defendant did not have authorized access to the documents he allegedly transferred after his resignation. As to the defendant's post-resignation conduct, the plaintiffs'

[1] 18 U.S.C. § 1030(a)(2)(C) (emphasis added).

[2] 581 F.3d 1127 (9th Cir. 2009).

CFAA claim is legally viable. The motion to dismiss the CFAA claims is thus granted, but only in part.

The Court denies dismissal for the remainder of the plaintiffs' non-contractual claims. Because all of the alleged acts of misappropriation occurred in France, the defendant moves to dismiss the plaintiffs' claim under DUTSA based on the presumption against extraterritoriality. The parties' extraterritoriality analysis involves a fact-intensive inquiry. Nearly all states have adopted the Uniform Trade Secrets Act. It is reasonably conceivable that some state's Uniform Trade Secrets Act applies given the plaintiffs' global brand. Under Delaware's liberal pleading standard, the plaintiffs need not identify which law applies at the pleadings stage.

The defendant's other dismissal arguments likewise fail. The defendant argues that the plaintiffs have not adequately alleged the elements of a trade secrets claim, but the complaint easily meets the plaintiff-friendly pleading standard. The defendant argues that the plaintiffs' conversion claim is duplicative of the contractual claim, but those claims arise from different obligations and appropriately stand alone. The defendant argues that DUTSA preempts the plaintiffs' conversion claim, but that conclusion depends on which state's trade secrets laws—if any—apply. Such a determination is premature and as a result, dismissal of the plaintiffs' conversion claim is inappropriate.

I. FACTUAL BACKGROUND

The facts are drawn from the complaint[3] and matters not subject to reasonable dispute.

A. Defendant's Employment by Plaintiffs

AlixPartners, LLP and AlixPartners Holdings, LLP (collectively, "Plaintiffs"), are a corporate restructuring advisory firm and its holding company parent, respectively. Both entities are organized as Delaware limited liability partnerships. Plaintiffs were founded in 1981 and now have a "global reputation" built through work with "multinational clients" in a range of industries.[4]

Defendant David Benichou ("Defendant") joined Plaintiffs on February 27, 2006. He served as Managing Director in Plaintiffs' Paris offices from January 1, 2013 to October 25, 2017. In that position, Defendant was responsible for: building and maintaining client relationships; leading complex engagements; recruiting top talent; and developing intellectual property for the firm. In carrying out these responsibilities, Defendant had access to Plaintiffs' confidential and proprietary information.

When Defendant became a Partner, he signed as a party to Plaintiffs' January 12, 2017 Second Amended and Restated LLP Agreement (the "LLP

[3] C.A. No. 2018-0600-KSJM Docket ("Dkt.") 1, Verified Compl. ("Compl.").

[4] Compl. ¶ 13.

Agreement"). The LLP Agreement includes confidentiality requirements protecting Plaintiffs' non-public information. Plaintiffs also have a written data policy on the acceptable use of Plaintiffs' "data, networks, systems, devices, and applications."[5]

B. Defendant Accesses Plaintiffs' Confidential Information

During his employment with Plaintiffs, Defendant kept thousands of Plaintiffs' confidential documents on the local C drive of his work-issued computer in a folder titled "BatDocuments."[6] These documents included "numerous PowerPoint presentations related to Defendant's work on behalf of [Plaintiffs], reports, revenue assessments, studies prepared by [Plaintiffs], notes from meetings, pricing analyses, and other strategic documents," Plaintiffs allege.[7]

The complaint sets out in granular detail facts from which this Court can infer that Defendant transferred these confidential documents to a personal data device before and after his resignation. The complaint alleges that, around March 8, 2017, "Defendant connected a Western Digital 250 GB personal external hard drive to his Computer."[8] Then,

> [a]t approximately 7:31 AM CEST (Paris local time), Defendant accessed the subfolder "Presentation" within a matter-named subfolder in the "BatDocuments" folder on the C drive of Defendant's Computer with the pathname

[5] *Id.* ¶ 18.

[6] *Id.* ¶ 45.

[7] *Id.* ¶ 50.

[8] *Id.* ¶ 46.

> C:\Users\dbenichou\Documents\Batdocuments\39-[Matter Name]\Presentation.
>
> . . . [O]ne minute later, at 7:32 AM CEST, Defendant accessed a subfolder on his personal external hard drive, with the identically named pathname D:\Batdocuments\39-[Matter Name]\Presentation.[9]

Defendant resigned from his position with Plaintiffs in 2017, providing notice on May 1, 2017. Plaintiffs dismissed Defendant from his duties on July 25, 2017, and he stopped performing work for Plaintiffs around that time. Three days later, on July 28, 2017, "Defendant again connected his personal external hard drive to his Computer."[10] The complaint alleges:

> At 8:22 AM (CEST) on July 28, 2017, [Defendant] created the folder entitled "Personnel et confidentiel 2" on the local C drive of his Computer. Defendant then copied folders containing hundreds of files from the "BatDocuments" folder on the C drive of his Computer into the "Personnel et confidentiel 2" folder on his Computer. At or around 10:54 AM local time, Defendant cut and pasted the "Personnel et confidentiel 2" folder—which then contained those hundreds of files—from his Computer onto his personal external hard drive. Defendant proceeded to review other files on his Computer, and placed some files in the Recycle Bin on the Computer.
>
> . . . Defendant also accessed another folder on his Computer entitled "Personnel et confidentiel," which he had created on or around April 13, 2017 and accessed a number of times between then and July 28, 2017. He

[9] *Id.* ¶¶ 46–47 (footnotes omitted).

[10] *Id.* ¶ 51.

> deleted the "Personnel et confidentiel" folder at or after 12:40 PM CEST on July 28, 2017.[11]

Defendant never informed Plaintiffs of his personal data drive, disclosed that he had transferred these documents to it, or returned any confidential information it contained.

Defendant started working for the corporate restructuring division of Boston Consulting Group ("BCG") around October 2017. BCG's restructuring division directly competes with Plaintiffs, according to the complaint.

Plaintiffs allege that BCG employees contacted Defendant in early 2017 before he resigned. Plaintiffs also allege that Defendant disclosed Plaintiffs' confidential information to BCG employees in the first half of 2017, and that Defendant "decided to take [Plaintiffs'] confidential information with him when he left in order to use that confidential information at [BCG] for his benefit and for the benefit of BCG . . . ."[12]

C. Procedural Posture

On August 10, 2018, Plaintiffs initiated this action. The complaint asserts four causes of action. Count I alleges that Defendant breached the confidentiality provisions of the LLP Agreement. Count II alleges that Defendant breached the Delaware Uniform Trade Secrets Act. Count III alleges that Defendant committed

[11] *Id.* ¶¶ 51–52.

[12] *Id.* ¶ 22.

common law conversion. Count IV alleges that Defendant violated the federal CFAA.

On September 28, 2018, Defendant responded by moving to dismiss Counts II through IV of the complaint. The parties completed briefing on the motion on January 22, 2019,[13] and the Court heard oral argument on January 31, 2019.[14]

II. LEGAL ANALYSIS

Defendant moves to dismiss pursuant to Court of Chancery Rule 12(b)(6). On a Rule 12(b)(6) motion, the Court "accept[s] all well-pleaded factual allegations in the [c]omplaint as true," and "draw[s] all reasonable inferences in favor of the plaintiff . . . ."[15] The Court denies the motion "unless the plaintiff could not recover under any reasonably conceivable set of circumstances susceptible of proof."[16] The Court neither "accept[s] conclusory allegations unsupported by specific facts, Court

[13] Dkt. 14, Def.'s Opening Br. in Supp. of His Mot. to Stay or in the Alternative Dismiss the Verified Compl. ("Def.'s Opening Br."); Dkt. 18, Pls.' Answering Br. in Opp'n to Defendant's Mot. to Dismiss the Verified Compl. ("Pls.' Ans. Br."); Dkt. 23, Def.'s Reply Br. in Supp. of His Mot. to Stay or in the Alt. Dismiss the Verified Compl. and Mot. to Stay Disc.; Dkt. 26, Pls.' Sur-Reply in Opp'n to Def.'s Mot. to Dismiss the Verified Compl.

[14] Dkt. 30, Oral Arg. on Mot. to Dismiss and Mot. to Stay before V.C. McCormick. In the alternative to his dismissal arguments, Defendant sought to dismiss or stay the Delaware proceedings pursuant to *McWane Cast Iron Pipe Corp. v. McDowell-Wellman Eng'g Co.*, 263 A.2d 281, 283 (Del. 1970), pending resolution of the French proceedings. The Court denied the motion by an Order issued on February 7, 2018. Dkt. 31, Order Addressing Def.'s *McWane* Mot. to Dismiss or Stay.

[15] *Cent. Mortg. Co. v. Morgan Stanley Mortg. Capital Hldgs. LLC*, 27 A.3d 531, 536 (Del. 2011) (citing *Savor, Inc. v. FMR Corp.*, 812 A.2d 894, 896–97 (Del. 2002)).

[16] *Id.*

neither "accept[s] conclusory allegations unsupported by specific facts, nor . . . draw[s] unreasonable inferences in the plaintiff's favor."[17]

A. Count II—Delaware Uniform Trade Secrets Act

Count II asserts that Defendant misappropriated hundreds of Plaintiffs' documents, some of which contained trade secrets, in violation of the Delaware Uniform Trade Secrets Act (or "DUTSA"). Defendant argues that Count II should be dismissed because the complaint fails to plead a DUTSA claim, and because DUTSA does not apply extraterritorially to conduct alleged to have occurred solely in France.

1. Plaintiffs adequately allege the elements of a trade secrets claim.

A claim for misappropriation of trade secrets under DUTSA requires allegations sufficient to show: (1) the existence of a trade secret (*i.e.*, information with commercial utility arising from its secrecy and reasonable steps to maintain this secrecy); (2) which the plaintiff communicated to the defendant; (3) under an express or implied understanding that the defendant would respect the secrecy of the matter; and that (4) the defendant used or disclosed the secret information in breach of that understanding to the injury of the plaintiff.[18]

---

[17] *Clinton v. Enter. Rent-A-Car Co.*, 977 A.2d 892, 895 (Del. 2009).

[18] *Wilm. Tr. Co. v. Consistent Asset Mgmt. Co., Inc.*, 1987 WL 8459, at *3 (Del. Ch. Mar. 25, 1987).

Defendant argues that Plaintiffs have not adequately pled the first element, the existence of a trade secret. To show the existence of a trade secret, a plaintiff must allege that the information "[d]erives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use" and that the information is "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[19] "Trade secrets should be given an expansive meaning and interpretation."[20]

The complaint sufficiently alleges the existence of a trade secret. According to the complaint, Plaintiffs have "developed numerous methods, techniques, and processes for conducting and marketing its consulting business that derive independent economic value from not being generally known to others who might use or disclose them for economic gain."[21] That information includes documents like "revenue assessments, studies prepared by [Plaintiffs], notes from meetings, pricing analyses, and other strategic documents."[22] The alleged categories of

[19] 6 *Del. C.* § 2001(4).

[20] *Sanirab Corp. v. Sunroc Corp.*, 2002 WL 1288732, at *3 (Del. Super. Apr. 29, 2002) (emphasis omitted).

[21] Compl. ¶ 67.

[22] *Id.* ¶ 50.

documents are not overly vague or so broad as to be meaningless.[23] It is reasonably conceivable that these documents have independent economic value.[24]

Plaintiffs also took reasonable steps to guard the secrecy of these documents. Under Delaware law, the existence of a confidentiality agreement satisfies this requirement.[25] The acceptable use policy provided an added layer of protection. Plaintiffs also protect their confidential information with passwords, restrict rights and access to those employees with a need to know, and include confidentiality provisions in their employment agreements.[26]

Next, Defendant argues that Plaintiffs have not adequately pled the fourth element, that Defendant used or disclosed the trade secrets. It is the rare misappropriation case in which Plaintiffs have first-hand knowledge of this element

---

[23] *Compare id.* ¶¶ 45, 50 (describing the organization and nature of the documents containing trade secrets) *with MHS Capital LLC v. Goggin*, 2018 WL 2149718, at *14 (Del. Ch. May 10, 2018) (dismissing trade secret claim where complaint vaguely referred to "potential returns" and "strategies").

[24] *GWO Litig. Tr. v. Sprint Sols., Inc.*, 2018 WL 5309477, at *9–10 (Del. Super. Oct. 25, 2018) (A DUTSA claim will survive a motion to dismiss where the documents in question are "*conceivably* of independent economic value." (emphasis added)).

[25] *See GWO Litig.*, 2018 WL 5309477, at *10 (holding that the "reasonable efforts" prong "is not a high bar" and that "confidentiality provisions or policies intended to prevent unauthorized disclosure are sufficient").

[26] *Compare* Compl. ¶ 68 (describing minimum necessary rights and access provided only to employees "with a need to know") *with Goggin*, 2018 WL 2149718, at *14 (granting a motion to dismiss a trade secrets claim on where the complaint simply repeated as an allegation and in conclusory form the language of the statute, that "ECM took reasonable steps to maintain secrecy").

at the pleadings stage.[27] Typically, the Complaint must rely on inferences or circumstantial evidence. Here, the Complaint alleges the following facts. Defendant transferred documents containing confidential information and trade secrets onto a personal hard drive right before and after he left to work for a competitor. Defendant never disclosed the hard drive to Plaintiffs. Defendant never accounted for the documents he transferred onto the hard drive when he began working at BCG. And Defendant refused to confirm his compliance with his contractual obligations despite Plaintiffs' requests. It is reasonable to infer, based on the facts alleged, and under a plaintiff-friendly standard, that Defendant has used or disclosed these documents.

2. Defendant's extraterritoriality argument is not appropriately addressed at the pleadings stage.

In the alternative, Defendant argues that Count II should be dismissed because DUTSA does not apply on its face to actions taken outside Delaware, and each of Defendant's alleged actions occurred in France.[28] Plaintiffs respond that "this case does not . . . require consideration of extraterritoriality,"[29] that the extraterritorial application of DUTSA is more appropriately framed as a choice-of-law question,[30]

[27] *See Accenture Glob. Servs. GMBH v. Guidewire Software Inc.*, 581 F. Supp. 2d 654, 662 (D. Del. 2008) ("It is not common for a trade secret misappropriation plaintiff to know, prior to discovery, the details surrounding the purported theft.").

[28] Def.'s Opening Br. at 30.

[29] Pls.' Ans. Br. at 32.

[30] *Id*. at 32–33.

and that such an analysis is necessarily fact intensive so the Court should not conduct it on the pleadings. If the Court does conduct the choice-of-law analysis, Plaintiffs argue that the analysis should focus on the place of Plaintiffs' injury, which Plaintiffs say favors applying Delaware law, and not Defendant's conduct.

This decision assumes that the presumption against extraterritoriality analysis applies, and that it precludes applying the DUTSA to the conduct at issue, as Defendant argues. Even assuming these premises, Count III survives Defendant's motion to dismiss. Delaware's liberal notice pleading rules require only "a short and plain statement of the claim showing that the pleader is entitled to relief[.]"[31] Consequently, a plaintiff need not identify the precise law on which it relies.[32] Plaintiffs operate in a global market, and nearly all of the states have adopted the Uniform Trade Secrets Act. The standard is "reasonable conceivability."[33] It is reasonably conceivable that the law of Plaintiffs' principal place of business (Michigan) or another state's law applies.

B. Count III—Conversion

Count III alleges that if any of the documents taken by Defendant do not rise to the level of a trade secret, they still constitute confidential and proprietary

[31] Ct. Ch. R. 8(a)(1).

[32] *Dow Chem. Co. v. Organik Kimya Hldg. A.S.*, 2018 WL 2382802, at *4 (Del. Ch. May 25, 2018).

[33] *Cent. Mortg.*, 27 A.3d at 537 (citation and internal quotation marks omitted).

information.[34] Plaintiffs contend that Defendant took possession of these documents and never returned them.[35]

As with Count II, Count III hinges on issues that are inappropriate to decide on a motion to dismiss. For example, Defendant argues that Count III should be dismissed because the DUTSA preempts Plaintiffs' conversion claim.[36] Some states interpret the Uniform Trade Secrets Act as preempting all common law claims for conversion of confidential information;[37] other states do not.[38] Whether Plaintiffs' trade secrets claim preempts the conversion claim will depend on what law applies. As discussed above, what law applies is not a pleadings-stage issue. Neither, therefore, is preemption.[39]

---

[34] Compl. ¶ 75.

[35] *Id.* ¶ 76.

[36] *See generally* 6 *Del. C.* § 2007(a) ("[T]his chapter displaces conflicting tort, restitutionary and other law of this State providing civil remedies for misappropriation of a trade secret."); *Alarm.com Hldgs. Inc. v. ABS Capital P'rs*, 2018 WL 3006118, at *9–11 (Del. Ch. June 15, 2018), *aff'd on other grounds*, 204 A.3d 113 (Del. 2019).

[37] *See generally Alarm.com*, 2018 WL 3006118, at *11 n.67.

[38] *See, e.g.*, *Am. Biomedical Gp., Inc. v. Techtrol, Inc.*, 374 P.3d 820, 827 (Okla. 2016) ("By its unambiguous language, Section 92(A) of the [Oklahoma Uniform Trade Secrets Act] displaces conflicting tort claims only for 'misappropriation of a trade secret.' It does not displace tort claims for information not meeting this definition."); *Int'l Paper Co. v. Gilliam*, 2003 WL 23573613, at *4 (Va. Cir. Ct. Dec. 23, 2003) ("The [Virginia Uniform Trade Secrets Act] does not preempt alternative tort recovery unless it is clear that the [confidential information at issue] falls within the confines of the Act.").

[39] Plaintiffs have identified a potentially applicable French law, which they describe as the French Civil Code equivalent to Delaware's common law claim of conversion. *See* Pls.' Ans. Br. at 45–47. This decision does not resolve whether Plaintiffs have or must state a claim under French law.

As an independent basis for dismissal, Defendant argues that Count III should be dismissed because it is duplicative of Count I's breach of contract claim.[40] It is not clear that the "only confidentiality obligation" pleaded derives from the LLP Agreement, as Defendant contends.[41] It is reasonably conceivable that Plaintiffs have a separate property interest in the confidential information.[42] The Counts were asserted in the alternative, as permitted under Delaware law.[43]

For these reasons, Defendant's motion to dismiss Count III is denied.

C. Count IV—Computer Fraud and Abuse Act

Count IV alleges that Defendant violated the CFAA.[44] Congress passed the CFAA in 1984 as the first piece of federal legislation directed solely at computer

---

[40] Def.'s Opening Br. at 46–47.

[41] *Id.* at 47.

[42] *See, e.g.*, *Rockwell Automation, Inc. v. Kall*, 2004 WL 2965427, at *4 (Del. Ch. Dec. 15, 2004) (observing that the plaintiff "has a property interest in its confidential information"); *Sustainable Energy Generation Gp., LLC v. Photon Energy Projects BV*, 2014 WL 2433096, at *14 (Del. Ch. May 30, 2014) (holding that it was reasonably conceivable that plaintiff could prove a property interest in confidential information); *Overdrive, Inc. v. Baker & Taylor, Inc.*, 2011 WL 2448209, at *5 (Del. Ch. June 17, 2011) (allowing a claim based on conversion of confidential information to survive a motion to dismiss along with a separate claim for breach of a contractual confidentiality obligation).

[43] *Israel Disc. Bank of New York v. First State Depository Co., LLC*, 2012 WL 4459802, at *13 (Del. Ch. Sept. 27, 2012), *aff'd*, 86 A.3d 1118 (Del. 2014) ("I note that [p]laintiff is permitted under [Court of Chancery] Rule 8(e)(2) to plead claims in the alternative. Therefore, even if [the plaintiff's] breach of contract and conversion claims were mutually exclusive, that would not preclude [the plaintiff] from pursuing both claims in the alternative.").

[44] 18 U.S.C. § 1030(a)(2)(C).

crime.[45] Originally, the CFAA was a criminal statute intended to protect a limited set of federal computers and financial institutions.[46] It was later expanded to include a broad category of computers "used in or affecting interstate or foreign commerce of communication"[47] and amended to add a civil cause of action.[48] As a result, violations of the statute expose offenders to both civil and criminal liability.

Plaintiffs allege that Defendant violated Section 1030(a)(2)(C) of the CFAA by misappropriating information stored on Defendant's work-issued computer. Section 1030(a)(2)(C) renders liable a person who "intentionally accesses a

---

[45] H.R. Rep. No. 98–894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691 ("There is [n]o specific federal legislation in the area of computer crime.").

[46] *Brekka*, 581 F.3d at 1130 ("The CFAA was enacted . . . to enhance the government's ability to prosecute computer crimes."); Shawn E. Tuma, *What Does CFAA Mean and Why Should I Care?*, 63 S.C. L. Rev. 141, 155 (2011) ("This first statute was very narrow. This statute was limited to 'three specific scenarios: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. Government computers' . . . . The CFAA's general purpose, originally, was to address the growing problems of computer crime and hacking directed at government interest computers." (citations and footnotes omitted)).

[47] Economic Espionage Act, Pub. L. No. 104–294, 110 Stat. 3488 (1996); 18 U.S.C. § 1030(e)(2).

[48] Proof of one of five additional factors is necessary to maintain a civil action. 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."); S. Rep. No. 104–357, at 11–12, 14 (1996) ("The amendment to section 1030(g) provides that victims of computer abuse can maintain a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief."); Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 Tulsa L. Rev. 677, 693 (2009) ("Originally enacted exclusively as a criminal statute, the CFAA was amended in 1994 to add a private civil cause of action with fairly broad jurisdictional reach." (citations and footnote omitted)).

computer *without authorization, or exceeds authorized access*, and thereby obtains . . . information from any protected computer."[49]

Defendant's motion to dismiss Count IV focuses on the meaning of the words emphasized above—"without authorization" and "exceeds authorized access." Defendant argues that the CFAA provides a narrow cause of action under which Plaintiffs can hold Defendant liable for *unauthorized* access of protected computers.[50] Defendant argues that the CFAA does not protect against *misuse* of information by a person otherwise authorized to access the information at issue. Plaintiffs respond that the CFAA creates liability for misusing information obtained through authorized access to a protected computer.[51]

1. The split in federal authority: the broad and narrow approaches.

The parties' dispute parallels a nationwide split of federal authority over the proper interpretation of the terms "without authorization" and "exceeds authorized access" in the CFAA.

The first line of cases interprets "accesses a computer without authorization" and "exceeds authorized access" broadly. First promulgated by the First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*, and advanced by Plaintiffs here, the broad

[49] 18 U.S.C. § 1030(a)(2)(C) (emphasis added).

[50] Def.'s Opening Br. at 49.

[51] Pls.' Ans. Br. at 51–52.

interpretation holds that accessing a computer or information in violation of one's use obligations can give rise to liability under the "exceeds authorized access" provision.[52] In *EF Cultural*, the Court held that the complaint states a claim that the defendant violated the CFAA by disclosing proprietary information in breach of a confidentiality agreement and policy.[53] Later, in *Citrin*, the Seventh Circuit adopted the First Circuit's broad interpretation, but framed the analysis as an agency relationship issue.[54] The Court reasoned when an employee uses information in a manner adverse to his employer, the employee violates loyalty duties, thereby implicitly terminating the agency relationship, and losing any authority to access the computer or any information on it.[55] Appellate courts in the Fifth and Eleventh Circuits have also adopted a broad interpretation of the CFAA.[56]

The second line of cases interprets "accesses a computer without authorization" and "exceeds authorized access" narrowly. First adopted by the Ninth Circuit in *Brekka*, the narrow approach does not consider an individual's intended

[52] 274 F.3d 577, 582–83 (1st Cir. 2001).

[53] *Id.* ("[The plaintiff] is likely to prove . . . excessive access based on the confidentiality agreement between [a defendant] and [the plaintiff].").

[54] *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006).

[55] *Id.*

[56] *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010).

or actual misuse of accessed information.[57] Appellate courts in the Second and Fourth Circuits have adopted the narrow approach.[58]

2. This decision adopts the narrow approach.

The meaning of "accesses a computer without authorization" and "exceeds authorized access" as used in the CFAA is an issue of first impression for Delaware courts. No authority that binds this Court has addressed the issue. No Delaware state court has encountered the question presented.[59] In interpreting federal statutes absent binding precedent, this Court gives great weight to the rulings of the Third Circuit and Delaware district court.[60] But neither the Third Circuit nor the Delaware

---

[57] 581 F.3d 1127. *See also United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (applying *Brekka*).

[58] *United States v. Valle*, 807 F.3d 508, 527–28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012).

[59] Delaware has a statutory counterparty to the CFAA—the Misuse of Computer System Information Statute, 11 *Del. C.* § 935 *et seq.* Unlike the CFAA, that statute expressly prohibits "unauthorized use." 11 *Del. C.* § 935(1) ("A person is guilty of the computer crime of misuse of computer system information when . . . [a]s a result of accessing or causing to be accessed a computer system, the person intentionally makes or causes to be made an unauthorized display, use, disclosure or copy . . . ."). Given its distinguishable language, cases interpreting Section 935(1) are not instructive to the issue at hand.

[60] *See, e.g.*, *Johnson v. State*, 983 A.2d 904, 917 (Del. 2009) ("After reviewing the varied approaches taken by the Circuit courts in light of somewhat unclear United States Supreme Court precedents, we adopt the approach taken by the Third Circuit[.]"); *Cosby v. Correct Care Sols., LLC*, 2016 WL 7103387, at *6 (Del. Super. Dec. 6, 2016) ("The language of the DDEA is virtually identical to 42 U.S.C. § 2000(e) of the federal Civil Rights Act of 1964 (Title VII). Accordingly, when construing the DDEA, Delaware courts look to how the federal courts in the Third Circuit and the District of Delaware have construed Title VII cases."); *Fusco v. Dauphin*, 75 A.2d 701, 702 (Del. Super. 1950) ("[O]ur own Federal District Court has held that a party is not required to admit facts not within his personal knowledge. . . . While not actually binding upon me, this decision is entitled to the utmost

district court has ruled on the matter. And non-Delaware district courts within the Third Circuit diverge in their approach.[61]

Without clear guidance from state or federal authorities, this Court looks to principles of statutory interpretation to discern the CFAA's meaning, and concludes that the narrow approach is best supported. The analysis starts with the plain language of the statute.[62] If the plain language is clear and unambiguous, the

---

respect." (citation omitted)). *See also Red Maple Props. v. Zoning Comm'n of Town of Brookfield*, 610 A.2d 1238, 1242 n.7 (Conn. 1992) ("'The decisions of the federal circuit in which a state court is located are entitled to great weight in the interpretation of a federal statute.'" (alteration omitted)); *Pignato v. Great W. Bank*, 664 So. 2d 1011, 1015 (Fla. Dist. Ct. App. 1995) ("[A]ccording unusual weight to a decision on an issue rendered by a federal circuit in which the state is located is an appropriate method for deciding federal questions where there is no Supreme Court authority[.]"); *Littlefield v. State*, 480 A.2d 731, 737 (Me. 1984) ("[I]n the interests of existing harmonious federal-state relationships, it is a wise policy that a state court of last resort accept, so far as reasonably possible, a decision of its federal circuit court on . . . a federal question."); *Abbott v. Goodwin*, 804 P.2d 485, 490 (Or. Ct. App. 1991) (stating that although not bound by lower federal court decisions, "under principles of federalism, we not only defer to federal court precedents, we should give weight to those of the Ninth Circuit, in which Oregon lies"), *modified on other grounds*, 809 P.2d 716 (Or. 1991).

[61] *Compare Beauty Plus Trading, Co. v. Adamo*, 2018 WL 846918, at *1–2 (D.N.J. Feb. 13, 2018) (adopting narrow approach), *Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669–70 (E.D. Pa. 2018) (same), *Tactical Pers. Leasing, Inc. v. Hajduk*, 2018 WL 4740195, *2–3 (W.D. Pa. Oct. 2, 2018) (same), and *Adv. Fluid Sys., Inc. v. Huber*, 28 F. Supp. 3d 306, 329 (M.D. Pa. 2014) (same) *with Chubb Ina Hldgs. Inc. v. Chang*, 2017 WL 499682, at *6–7 (D.N.J. Feb. 7, 2017) (denying dismissal of CFAA claims and citing *Citrin* favorably) and *Spinello Cos. v. Silva*, 2014 WL 4896530, at *3–4 (D.N.J. Sept. 30, 2014) (same).

[62] *Jimenez v. Quarterman*, 555 U.S. 113, 118 (2009) ("As with any question of statutory interpretation, our analysis begins with the plain language of the statute."); *Zhurbin v. State*, 104 A.3d 108, 110 (Del. 2014) ("Our analysis of the parties' arguments begins with the plain language of the statute[.]").

analysis ends.[63] If the plain language is susceptible to multiple meanings, the Court ascertains the meaning of the statute by reviewing the statute's purpose and legislative history.[64] When a statute has both civil and criminal applications, the rule of lenity applies.[65] That rule requires this Court to construe criminal statutes strictly to avoid interpretations not "clearly warranted by the text."[66] The concept behind it is that the legislature should not decree punishment without making clear what conduct incurs that punishment.[67]

---

[63] *See Nat'l Ass'n of Mfrs. v. Dep't of Def.*, 138 S. Ct. 617, 631 (2018); *see also BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004) (plurality opinion) ("The preeminent canon of statutory interpretation requires us to presume that the legislature says in a statute what it means and means in a statute what it says there. Thus, our inquiry begins with the statutory text, and ends there as well if the text is unambiguous." (internal quotation marks, alteration, and citation omitted)); *Zhurbin*, 104 A.3d at 110 ("Where a statute contains unambiguous language that clearly reflects the intent of the legislature, then the language of the statute controls." (citing *Hoover v. State*, 958 A.2d 816, 820 (Del. 2008))); *Bd. of Adjustment of Sussex Cty. v. Verleysen*, 36 A.3d 326, 331 (Del. 2012) ("[W]hen a statute is clear and unambiguous there is no need for statutory interpretation." (citing *State v. Skinner*, 632 A.2d 82, 85 (Del. 1993))).

[64] *Parker v. NutriSys., Inc.*, 620 F.3d 274, 277 (3d Cir. 2010); *Clark v. State*, 184 A.3d 1292 (Del. 2018) (TABLE) ("When a statute is ambiguous, a court may refer to the legislative history to interpret the statute." (citing *Arnold v. Soc'y for Sav. Bancorp, Inc.*, 650 A.2d 1270, 1287 (Del. 1994))).

[65] *U.S. v. Thompson/Ctr. Arms Co.*, 504 U.S. 505, 518 n.10 (1992) (observing that the rule of lenity applies to statutes having both criminal and civil applications, even where the application at issue is civil in nature); *Miller*, 687 F.3d at 203–04 (applying rule of lenity in interpreting the CFAA); *Dixon v. State*, 673 A.2d 1220, 1225 n.3 (Del. 1996) (analyzing the "general rule" that "ambiguous penal statutes should be strictly construed against the State").

[66] *Crandon v. United States*, 494 U.S. 152, 160 (1990).

[67] *Russello v. United States*, 464 U.S. 16, 29 (1983) ("The rule of lenity, which this Court has recognized in certain situations of statutory ambiguity . . . has no application here. That rule comes into operation at the end of the process of construing what Congress has

Turning to the plain language of the statute, the CFAA distinguishes between "without authorization" and "exceeds authorized access."[68] The former is not defined by the statute; the latter is defined as "access to a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[69] The concepts are closely related; their distinction is "paper thin."[70] The concepts hinge on the words "access" and "authorization." Because the CFAA does not define those terms specifically, the terms must be interpreted in accordance with their "ordinary, contemporary, common meaning."[71]

---

expressed, not at the beginning as an overriding consideration of being lenient to wrong-doers. . . . Here, the language of the RICO forfeiture provision is clear, and the rule of lenity does not come into play." (internal quotation marks and citations omitted)); *see also Moskal v. United States*, 498 U.S. 103, 107 (1990) ("We have repeatedly emphasized that the touchstone of the rule of lenity is statutory ambiguity." (citation and internal quotation marks omitted)); *United States v. Bass*, 404 U.S. 336, 348 (1971) (suggesting that the rule of lenity derives from constitutional requirements of fair notice and separation of powers: "[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity.").

[68] 18 U.S.C. § 1030(a).

[69] 18 U.S.C. § 1030(e)(6).

[70] *Citrin*, 440 F.3d at 420 (citation omitted). In *Citrin*, the Court explained that an employee exceeded authorized ac6cess to a public website by using his programming knowledge to obtain confidential information from the public portal. *Id.*

[71] *Perrin v. United States*, 444 U.S. 37, 42 (1979); *French v. State*, 38 A.3d 289, 291 (Del. 2012) ("[I]f the words [of the statute] are not defined, they are given their commonly understood, plain meaning." (citing *Dickerson v. State*, 975 A.2d 791, 798 (Del. 2009))).

Dictionary definitions define "authorizing" as granting permission,[72] and "accessing" as "to obtain or acquire" or "to gain admission to."[73] Putting the definitions together, an employee "accesses a computer 'without authorization' when he gains admission to a computer without approval."[74] An employee

[72] *Authorization*, Black's Law Dictionary (10th ed. 2014) ("Official permission to do something; sanction or warrant."); *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595 (E.D. Pa. 2016) ("The Oxford English Dictionary defines 'Authorization' as 'the action of authorizing a person or thing' or 'formal permission or approval.' The term, 'to authorize,' in turn, ordinarily means 'to give official permission for or formal approval to (an action, undertaking, etc.).' Therefore, based on the ordinary meaning of the word, to act 'without authorization' is to act without formal permission or approval." (citations omitted)); *Valle*, 807 F.3d at 524 ("The dictionary defines 'authorization' as 'permission or power granted by authority.' Thus, common usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all." (quoting Random House Unabridged Dictionary 139 (2001))); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303–04 (6th Cir. 2011) ("The plain meaning of 'authorization' is '[t]he conferment of legality; . . . sanction.'" (quoting 1 Oxford English Dictionary 798 (2d ed. 1989)); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 191–92 (S.D.N.Y. 2010) ("'Authorization' is generally defined as the 'act of authorizing' or 'permission or power granted by an authority.' . . . Based on the ordinary meaning of 'authorization,' then, a person who 'accesses a computer without authorization' does so without any permission at all. By contrast, a person who 'exceeds authorized access' has permission to access the computer, but not the particular information on the computer that is at issue." (quoting The Random House Dictionary of the English Language 100 (Unabridged ed. 1970))).

[73] *Access*, Black's Law Dictionary (10th ed. 2014) ("A right, opportunity, or ability to enter, approach, pass to and from, or communicate with."); *Miller*, 687 F.3d at 204 ("Thus, we note at the outset that 'access' means '[t]o obtain, acquire,' or '[t]o gain admission to.'" (quoting Oxford English Dictionary (3d ed. 2011))); *Synthes, Inc. v. Emerge Med., Inc.*, 2012 WL 4205476, at *17 (E.D. Pa. Sept. 19, 2012) ("[O]ther courts have used the common meaning of the word 'access' and defined it as 'gaining admission to.'" (citing *Miller*, 687 F.3d at 204)); *Sw. Airlines Co. v. BoardFirst, LLC*, 2007 WL 4823761, at *12 (N.D. Tex. Sept. 12, 2007) (using the "dictionary definition" of "access" as "mean[ing] 'to get at' or 'gain access to'" (quoting Merriam-Webster's Collegiate Dictionary 6 (10th ed. 1998))).

[74] *Miller*, 687 F.3d at 204 (citing *Brekka*, 581 F.3d at 1133).

"'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access."[75] Under these definitions, an employee does not exceed authorized access by misusing the information the employee had a right to access. This definition accords with the narrow interpretation.

Although dictionary definitions favor the narrow interpretation, the federal split suggests that the CFAA's plain language is susceptible to multiple meanings.[76] This decision therefore reviews the CFAA's purpose and legislative history.

Turning to a review of statutory purpose and history, Congress adopted the CFAA to combat computer hacking, as discussed above. In *Citrin*, the Seventh Circuit speculated that this purpose targeted not just "long-distance attacks" from outsiders without authorized access to a system, but also "inside attack[s]" by "disgruntled programmers who decide to trash the employer's data system on the way out . . . ."[77] To reach the disgruntled programmer, the statute must be interpreted broadly, according to the Seventh Circuit. In *Miller*, however, the Fourth Circuit set forth a compelling counterargument interpreting Congressional intent in favor of the

---

[75] *Id.*

[76] *See, e.g.*, *Valle*, 807 F.3d at 524–25 ("If this sharp division means anything, it is that the statute is readily susceptible to different interpretations.").

[77] *Citrin*, 440 F.3d at 420.

narrow interpretation.[78] The Court did so by positing the following example: An employee downloads information from her work computer in violation of office policy, for the commendable purpose of progressing on a project from home.[79] Under the Seventh Circuit's interpretation of the CFAA, by violating the corporate use policy, the employee "exceeded her authorized access," implicitly terminated her agency relationship, and exposed herself to civil and as well as criminal liability. This is an extreme outcome that criminalizes banal moments of misuse common in the modern work force. These "far-reaching effects" seem "unintended by Congress."[80] To avoid these clearly unintended consequences, a court must follow the narrow approach.

Last, the rule of lenity tips decidedly in favor of the narrow approach. As illustrated by the Fourth Circuit's example, the broad interpretation of the CFAA creates criminal liability in multiple common scenarios. The narrow interpretation avoids that result. Given the criminal application of the CFAA, and the expansive potential criminal liability created by the broad interpretation, "authorized access" and "exceeds authorized access" must be narrowly construed.[81]

---

[78] *Miller*, 687 F.3d at 206.

[79] *Id.*

[80] *Id.*

[81] *See, e.g.*, *Valle*, 807 F.3d at 528 (adopting narrow approach to avoid "'unintentionally turn[ing] ordinary citizens into criminals'" (citing *Nosal*, 676 F.3d at 863)); *Miller*, 687 F.3d at 204 (adopting narrow approach and observing "[w]here, as here, our analysis

In sum, principles of statutory interpretation weigh in favor of adopting the narrow view of "without authorization" and "exceeds authorized access." That language applies only when an individual accesses a computer or information on that

---

involves a statute whose provisions have both civil and criminal application, our task merits special attention because our interpretation applies uniformly in both contexts." (citations omitted)); *Brekka*, 581 F.3d at 1134 (adopting narrow approach and observing that although the case arose in the civil context, the court's interpretation is equally applicable in the criminal context, and recognizing that ambiguity must be resolved in favor of lenity); *Mathey Dearman, Inc. v. H&M Pipe Beveling Mach. Co.*, 2018 WL 4224897, at *5 (N.D. Okla. Sept. 5, 2018) (adopting narrow approach, citing the discussion *Brekka* for its discussion of the rule of lenity); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 195 (D.D.C. 2017) (adopting narrow approach, citing *Valle* for its discussion of the rule of lenity); *Giles Const., LLC v. Tooele Inventory Sol., Inc*., 2015 WL 3755863, at *3 (D. Utah June 16, 2015) (adopting narrow approach and reasoning that "[i]n the CFAA, Congress has not clearly criminalized the *misuse* of lawfully obtained computer information. And if that conduct is not criminal under the statute, the conduct cannot provide a basis for a civil cause of action." (emphasis original)); *Enhanced Recovery Co., LLC v. Frady*, 2015 WL 1470852, at *8 (M.D. Fla. Mar. 31, 2015) (adopting narrow approach "'so that Congress will not unintentionally turn ordinary citizens into criminals.'" (citing *Nosal*, 676 F.3d at 863)); *JBCHldgs. NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 524 (S.D.N.Y. 2013) (adopting narrow approach and observing that "the broad reading of 'exceeds authorized access' has breathtaking implications. It would federalize, and potentially subject to federal criminal law, quotidian abuses by employees that have historically been the sole ambit of state employment and criminal law." (citation omitted)); *Sebrite Agency, Inc. v. Platt*, 884 F. Supp. 2d 912, 918 (D. Minn. 2012) (adopting narrow approach and observing that "the broader interpretation would . . . expose employees who violate their employers' computer-use restrictions to criminal liability . . ." (citations omitted)); *Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n*, 2012 WL 2522963, at *3 (D.N.H. June 29, 2012) (adopting narrow approach and observing that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." (citation omitted)). *See also Brand Energy & Infrastructure Servs., Inc. v. Irex Contr. Gp.*, 2017 WL 1105648, at *15 (E.D. Pa. Mar. 24, 2017) (rejecting the broad view in part based on the scope of persons who might be subject to liability, observing "the [broad] view would subject too wide a class of individuals—such as family members of employees—to CFAA liability . . . . This was not the intent of the CFAA." (citations omitted)).

computer without permission. The statute does not impose liability for misusing information to which the individual had authorized access.

In adopting the narrow approach, this Court acts consistently with the current trend. The majority of courts deciding this issue since *Brekka* have adopted the narrow approach. Since 2009, district courts in the Sixth,[82] Eighth,[83] Tenth,[84] and D.C. Circuits[85] have applied Defendant's "narrow" interpretation of the Act. Within circuits that initially adopted the broad approach, support for that view is eroding.[86]

---

[82] *Cranel Inc. v. Pro Image Consultants Gp., LLC*, 57 F. Supp. 3d 838, 845 (S.D. Ohio 2014) ("The Court agrees with these courts that the narrow interpretation is proper under the CFAA."); *see also Ajuba Int'l v. Saharia*, 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 613, 615 (M.D. Tenn. 2010); *Black & Decker (U.S.), Inc. v. Smith*, 568 F. Supp. 2d 929, 934–35 (W.D. Tenn. 2008).

[83] *Sebrite*, 884 F. Supp. 2d at 917–18 ("The Court continues to believe that the narrower interpretation of the CFAA is more consistent with statutory text, legislative history, and the rule of lenity.").

[84] *Mathey Dearman, Inc. v. H&M Pipe Beveling Mach. Co.*, 2018 WL 4224897, *5 (N.D. Okla. Sept. 5, 2018) ("[D]istrict courts in this Circuit uniformly apply the narrow inquiry . . . ."); *accord Tank Connc'n, LLC v. Haight*, 161 F. Supp. 3d 957, 969 (D. Kan. 2016), *appeal dismissed* (10th Cir. July 18, 2016); *Cloudpath Networks v. SecureW2 BV*, 157 F. Supp. 3d 961, 983–984 (D. Colo. 2016); *Cent. Bank & Tr. v. Smith*, 215 F. Supp. 3d 1226, 1232–33 (D. Wyo. 2016); *Giles*, 2015 WL 3755863, at *3.

[85] *Hedgeye*, 271 F. Supp. 3d at 194–95 ("Although the Court recognizes that the statutory definition of 'exceeds authorized access' is not crystal clear, the Second, Fourth and Ninth Circuits have identified the more persuasive reading of that phrase. . . . Thus, the CFAA prohibits the authorized computer user from accessing 'information' that he is not 'authorized' to obtain or alter. The statute says nothing about the *misuse* of information that the user was authorized to access." (emphasis original)); *see also Lewis-Burke Assocs., LLC v. Widder*, 725 F. Supp. 2d 187, 193–94 (D.D.C. 2010).

[86] Some district courts in the First Circuit treat the relevant appellate court language as dicta. *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 218–19 (D. Mass. 2013) ("At the time of this order, the First Circuit has not clearly articulated its position on this issue. Some district judges have read [*EF Cultural*] as an endorsement of the broader

Although this decision does not rest on the national trend as a basis for adopting the narrow approach, the fact that the country appears to be moving toward a narrow approach does provide some assurance of its wisdom.

3. Applying the narrow approach leads to partial dismissal of the CFAA claim.

Applying the narrow approach requires denying part of Plaintiffs' CFAA claim.

The Complaint alleges that, before his termination, Defendant was authorized

---

interpretation . . . . Others have read [*EF Cultural*] as supporting a broad interpretation only in dicta, and have adopted a narrower interpretation. . . . It is not clear to me that [*EF Cultural*] is a plain endorsement of a broad interpretation." (citations omitted)). Some district courts in the Eleventh Circuit reject the relevant precedent. *See, e.g.*, *Frady*, 2015 WL 1470852, at *6 ("Other courts, including the majority of district courts in this Circuit that have considered the question, have adopted a narrower definition of 'exceeds authorized access.'"); *Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc.*, 953 F. Supp. 2d 1290, 1296 (S.D. Ga. 2013) ("exceeds authorized access simply means that, while an employee's initial access was permitted, the employee accessed information for which the employer had not provided permission"); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010) (finding that the broad interpretation "ignores the plain language of the statute" and the narrow interpretation "is buoyed by the nature of the statute itself . . . Because the seven employees who resigned had valid permission to utilize the Bell Aerospace computers, they were acting with authorization when they accessed the computers up until the time they each were escorted from the facility."); *but see Aquent LLC v. Stapleton*, 65 F. Supp. 3d 1339, 1346 (M.D. Fla. 2014) ("In 2010, the Eleventh Circuit joined circuits that take a broader view, holding that when the employer had a policy limiting an employee's computer access to that done for business purposes, an employee who accessed a database for an improper purpose exceeded authorized access. . . . Accordingly, under *Rodriguez* [the plaintiff] sufficiently stated a cause of action . . . ." (citation omitted)). The Eleventh Circuit has observed this trend, noting the broad interpretation's "lack of acceptance" and that "several of our sister circuits have roundly criticized [broad interpretation] decisions . . . ." *EarthCam, Inc. v. OxBlue Corp.*, 703 Fed. Appx. 803, 808 n.2 (11th Cir. 2017).

to access the information at issue. Plaintiffs expressly allege that "[i]n carrying out [his] responsibilities, *Defendant had access* to AlixPartners' trade secrets and other confidential and proprietary information."[87] Plaintiffs describe the information accessed on a "laptop used by Defendant *during his employment*," and they describe "thousands of *his* work-related files in a folder."[88] Plaintiffs describe how Defendant "organized *his* files containing confidential information into subfolders entitled with the names of sensitive matters related to AlixPartners from the time of his employment on behalf of AlixPartners."[89] They explain that the "folders generally contain additional subfolders *relevant to the work Defendant performed for AlixPartners*."[90] These allegations reveal that Defendant was authorized to fully access the computer's contents. Thus, Plaintiffs' CFAA claim relating to Defendant's March 8, 2017 access is dismissed.

Plaintiffs also allege that Defendant accessed his work computer and its contents on July 28, 2017, "*after* AlixPartners provided Defendant notice of his dismissal by registered letter on July 25, 2017 and *after* he had ceased to perform work on behalf of AlixPartners."[91] It is reasonably conceivable that Defendant was

[87] Compl. ¶ 14 (emphasis added).

[88] *Id.* ¶ 45 (emphasis added).

[89] *Id*. (emphasis added).

[90] *Id*. (emphasis added).

[91] *Id.* ¶ 51 (emphasis added).

not authorized to access that information after his resignation. Thus, Defendant's motion to dismiss Count IV as to alleged conduct that occurred after Defendant's departure from the Company is dismissed.[92]

III. CONCLUSION

For these reasons, Defendant's motion to dismiss Count IV is GRANTED IN PART. The remainder of Defendant's motion is DENIED.

IT IS SO ORDERED.

[92] *See Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 407–08 (E.D. Pa. 2009) ("It also appears that after leaving the company, [a defendant] retained [the plaintiff's] computer for several weeks and accessed its contents, transferring some or all of them to a [the corporate defendant's] computer. Some of the information she transferred was allegedly proprietary customer data. There is, at the very least, a genuine issue of material fact as to whether she was authorized to access [the plaintiff's] computer at this time in this fashion, which precludes summary judgment as to the CFAA claim against her. Because questions of fact exist regarding the nature and extent of [the individual defendants'] authorization to alter or access the [plaintiff's] information they allegedly accessed, summary judgment will be denied on Plaintiffs' CFAA claim.").