

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X  
STEVEN FISCHKOFF, :

Plaintiff, :

-v.- :

IOVANCE BIOTHERAPEUTICS, INC. and  
MARIA FARDIS, :

Defendants. :

-----X

**GABRIEL W. GORENSTEIN, United States Magistrate Judge**

OPINION AND ORDER  
17 Civ. 5041 (AT) (GWG)

Steven Fischkoff brought this suit against Iovance Biotherapeutics, Inc. and Maria Fardis (collectively “Iovance”) alleging that Iovance breached a contractual employment agreement, failed to pay him wages, and retaliated against him. Iovance counterclaimed asserting that Fischkoff violated his employment agreements and that he misappropriated trade secrets. Iovance now moves to amend its answer to add counterclaims for conversion, trespass to chattels, violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, and violation of New Jersey’s Theft and Related Offenses Act, N.J.S.A. § 2C:20-7; 20-20.<sup>1</sup> For the reasons stated

---

<sup>1</sup> See Defendant’s Notice of Motion for Leave to Amend Answer and Counterclaims, filed July 27, 2018 (Docket # 106); Memorandum of Law in Support of Defendants’ Motion for Leave to Amend Answer and Counterclaims, filed July 27, 2018 (Docket # 106-1); Declaration of Kimberly Lunetta in Support of Defendants’ Motion for Leave to Amend Answer and Counterclaims, filed July 27, 2018 (Docket # 106-2) (“Lunetta Decl.”); Plaintiff’s Memorandum of Law in Opposition to Defendants’ Motion for Leave to Amend Their Answer and Counterclaims, filed August 17, 2018 (Docket # 113) (“P. Opp.”); Affirmation of Megan H. Daneshrad in Opposition to Defendant’s Motion for Leave to Amend Their Answer and Counterclaims, filed August 17, 2018 (Docket # 114); Defendants’ Reply Memorandum of Law in Support of Defendants’ Motion for Leave to Amend Answer and Counterclaims, filed September 7, 2018 (Docket # 123) (“D. Reply”).

below, Iovance's motion is denied.

## I. BACKGROUND

### A. Factual Allegations in the Proposed Counterclaims

Because the resolution of Iovance's motion turns on whether its proposed counterclaims state a claim for relief, we "accept[] all factual allegations [in its proposed counterclaims] as true and draw[] all reasonable inferences in favor of the [counterclaimant]." Empire Merchants, LLC v. Reliable Churchill LLLP, 902 F.3d 132, 139 (2d Cir. 2018) (citation and internal quotation marks omitted). We also consider all "documents attached to the [proposed amended answer] as exhibits, and documents incorporated by reference in the [proposed amended answer]." DiFolco v. MSNBC Cable L.L.C., 622 F.3d 104, 111 (2d Cir. 2010). We thus ignore the lengthy counter-recitation of facts contained in Fischkoff's opposition to the motion to amend. See P. Opp. at 2-5.

The proposed counterclaims allege in pertinent part as follows:

Iovance is a bio-pharmaceutical company with offices in California, Florida, and New York, that specializes in the development of drugs to treat cancer. Proposed Amended Answer and Counterclaims (annexed as Ex. A to Lunetta Decl.) ("PAA"), ¶¶ 12-13, 16. In February 2016, Fischkoff began working at Iovance as Chief Medical Officer and signed multiple documents and agreements reflecting the "importance of maintaining the confidentiality" of Iovance proprietary information. Id. ¶¶ 20-22. "[E]arly in his tenure," Fischkoff failed to meet certain "fundamental" employment obligations, including missing "operations goals, provid[ing] low quality outputs," and failing to "adequately manage clinical operations activities." Id. ¶ 25. Iovance terminated his employment on March 28, 2017. Id. ¶ 31.

Iovance alleges that, before his termination, Fischkoff sent a number of confidential

Iovance documents to his personal email addresses and also mounted a personal hard drive onto his work computer that he used to receive uploaded confidential files. Id. ¶¶ 32-33. Included in these files were tax materials that contained “approximately 285 files” containing social security numbers of others, as well as the entire contents of Fischkoff’s email inbox. Id. ¶ 35. Iovance alleges that Fischkoff never had authorized access to the documents he copied, and that he violated the Company Employee Handbook and the Employee Conduct Policy, which limited Fischkoff’s access to company documents. Id. ¶¶ 36-38.

Iovance alleges that the copied files include materials that “represent a significant portion of the intangible value of the Company, as they relate to its two most important clinical trials as well as its overall strategy and business.” Id. ¶ 41. It alleges that Fischkoff was later hired by a competitor and that his possession of company materials “would likely have resulted” in their disclosure to the competitor. Id. ¶ 45. “Despite numerous requests and obligations to do so, Plaintiff did not return all Confidential Materials and Human Resources, Finance, and Personal Information . . . for a period of at least 15 months.” Id. ¶ 58; accord id. ¶ 60.

#### B. Procedural History

The case began in June 2017 when Fischkoff filed breach of contract and New York Labor Law claims against Iovance in New York state court. See Complaint, Steven Fischkoff v. Lion Biotechnologies, Inc. et al., Index No. 653231 / 2017 (N.Y. Sup. Ct.) (annexed as Ex. A to Notice of Removal) (Docket # 1). After Iovance removed the action to federal court, it filed an answer that included counterclaims for (1) breach of contract; (2) breach of the covenant of good faith and fair dealing; (3) breach of fiduciary duty/duty of loyalty; and (4) misappropriation of trade secrets under 18 U.S.C. § 1836 and New York common law. See Defendants’ Partial Answer and Defenses to Plaintiff’s Complaint and Lion’s Counterclaims Against Steven

Fischkoff, filed July 13, 2017 (Docket # 7).

Iovance's proposed amended answer includes four additional counterclaims: conversion; trespass to chattels; violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030; and violations of New Jersey's Theft and Related Offenses Act, N.J.S.A. §§ 2C:20-7; 20-20. See PAA ¶¶ 84-111.

## II. LAW GOVERNING MOTIONS TO AMEND

Fed. R. Civ. P. 15(a)(2) provides that leave to amend a pleading should be “freely give[n] . . . when justice so requires.” See Foman v. Davis, 371 U.S. 178, 182 (1962). A court must have “good reason” to deny leave to amend. See Acito v. IMCERA Grp., 47 F.3d 47, 55 (2d Cir. 1995). Leave to amend may be denied in situations of “undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, [or] undue prejudice to the opposing party.” Foman, 371 U.S. at 182. An amendment may also be denied if it is futile. Id. Here, plaintiff argues only that the proposed amendment is “futile.” See P. Mem. at 1, 6.

When a party argues that an amendment to a pleading would be futile, the court must determine whether the “proposed claim could . . . withstand a motion to dismiss pursuant to [Federal Rule of Civil Procedure] 12(b)(6).” Dougherty v. Town of N. Hempstead Bd. of Zoning Appeals, 282 F.3d 83, 88 (2d Cir. 2002) (citing Ricciuti v. N.Y.C. Transit Auth., 941 F.2d 119, 123 (2d Cir. 1991)). Pursuant to Rule 12(b)(6), a party may move to dismiss the opposing party's pleading on the ground that it “fail[s] to state a claim upon which relief can be granted.” In deciding such a motion, a court must accept as true all of the allegations contained in the pleading, see Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009), but that principle does not apply to legal conclusions. Id.; see Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007) (“[A

party's] obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.") (internal quotation marks, citation, and alteration omitted). In other words, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," Iqbal, 556 U.S. at 678 (citation omitted), and thus a court's first task is to disregard any conclusory statements in the pleading, see id. at 679.

Next, a court must determine if the pleading contains "sufficient factual matter" which, if accepted as true, state a claim that is "plausible on its face." Id. at 678 (internal quotation marks and citation omitted); accord Port Dock & Stone Corp. v. Oldcastle Ne., Inc., 507 F.3d 117, 121 (2d Cir. 2007) ("[A pleading] must allege facts that are not merely consistent with the conclusion that the [adverse party] violated the law, but which actively and plausibly suggest that conclusion.") (citations omitted).

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. The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.

Iqbal, 556 U.S. at 678 (internal quotation marks and citations omitted). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct," [a pleading] is insufficient under Fed. R. Civ. P. 8(a) because it has merely "alleged" but not "show[n]"— "that the pleader is entitled to relief." Id. at 679 (second alteration in original) (quoting Fed. R. Civ. P. 8(a)(2)).

### III. DISCUSSION

Because we analyze the proposed counterclaims under the Rule 12(b)(6) standard of review, we turn to the question of whether the each of the proposed counterclaims could survive

a motion to dismiss.<sup>2</sup>

A. Conversion

The Second Circuit has summarized New York law of conversion as follows:

According to New York law, “[c]onversion is the unauthorized assumption and exercise of the right of ownership over goods belonging to another to the exclusion of the owner’s rights.” Vigilant Ins. Co. of Am. v. Hous. Auth., 87 N.Y.2d 36, 44, 637 N.Y.S.2d 342, 660 N.E.2d 1121 (1995) (internal quotation marks omitted). This includes a “denial or violation of the plaintiff’s dominion, rights, or possession” over her property. Sporn [v. MCA Records], 58 N.Y.2d [482,] 487, 462 N.Y.S.2d 413, 448 N.E.2d 1324 [(1983)]. It also requires that the defendant exclude the owner from exercising her rights over the goods. New York v. Seventh Regiment Fund, Inc., 98 N.Y.2d 249, 259, 746 N.Y.S.2d 637, 774 N.E.2d 702 (2002).

Thyroff v. Nationwide Mut. Ins., 460 F.3d 400, 403-404 (2d Cir. 2006). “[W]here possession of property is initially lawful, conversion occurs when there is a refusal to return the property upon demand.” Salatino v. Salatino, 64 A.D.3d 923, 925 (3d Dep’t 2009). “Returning property to the rightful owner does not absolve defendants of all liability from the alleged conversion,” and a claim “will exist even when the deprivation is partial or temporary.” Okyere v. Palisades Collection, LLC, 961 F. Supp. 2d 522, 534 (S.D.N.Y. 2013) (discussing New York conversion law) (citations and alteration omitted). Finally, damages will be calculated from any “loss flowing from the wrongful withholding of” the property. Silverstein v. Marine Midland Tr. Co. of N.Y., 1 A.D.2d 1037, 1038 (2d Dep’t 1956). The New York Court of Appeals has held that “electronic records that [a]re stored on a computer and [a]re indistinguishable from printed documents” are the sort of property that may be the subject of a claim of conversion. Thyroff v.

---

<sup>2</sup> The parties’ briefs assume that New York law applies to defendants counterclaims with the exception of the statutory claim arising under New Jersey law. Accordingly, we apply New York law to those counterclaims and New Jersey law to the New Jersey statutory claim. See IBM Corp. v. Liberty Mut. Fire Ins., 303 F.3d 419, 423 (2d Cir. 2002).

Nationwide Mut. Ins., 8 N.Y.3d 283, 292-93 (2007); accord Apple Mortg. Corp. v. Barenblatt, 162 F. Supp. 3d 270, 284 (S.D.N.Y. 2016).

In this case, we are presented with the question of whether the pure copying of electronic files without more satisfies the elements of a claim of conversion. The dispute between the parties is whether the counterclaims plausibly allege the “denial or violation of the [defendant’s] dominion, rights, or possession” over Iovance’s property and that plaintiff “exclude[d]” Iovance from “exercising [its] rights over the goods.” Thyoff, 460 F.3d at 406 (citations omitted). This element has also been phrased as an inquiry into whether the “defendant exercised an unauthorized dominion over the thing in question, to the alteration of its condition or to the exclusion of the plaintiff’s rights.” Apple Mortg. Corp., 162 F. Supp. 3d at 284 (emphasis added and citation omitted).

None of this language suggests that pure copying is sufficient to state a claim of conversion. The counterclaims make no allegation that Fischkoff’s copying resulted in any “alteration” of the files in Iovance’s position or that Iovance was in any way “exclude[d]” from using the original files in any way Iovance saw fit.

Our examination of case law involving cases of pure copying supports the conclusion that the counterclaim has not stated the required elements of conversion. In Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 813 F. Supp. 2d 489 (S.D.N.Y. 2011), the court found that a defendant who downloaded business documents onto a thumb drive was not liable for conversion because defendant “possessed only a copy of the client list and did not, in any way, limit or otherwise deprive [plaintiff] of possession or use of that list.” Id. at 536. Similarly, in Reis, Inc. v. Spring11 LLC, 2016 WL 5390896 (S.D.N.Y. Sept. 26, 2016), the unauthorized downloading of files was held not constitute conversion because the plaintiff was

never deprived of access. Id. at \*10-11. As Reis noted, “[w]hile New York courts have recognized that conversion can be predicated on the loss of intangible electronic data, that case law has not altered the traditional rule requiring the exercise of unauthorized dominion and control to the complete exclusion of the rightful possessor.” Id. at \*10 (alterations and citations omitted). Numerous other cases have found that mere copying does not permit a claim of conversion. See, e.g., Sell It Soc., LLC v. Strauss, 2018 WL 2357261, at \*8 (S.D.N.Y. Mar. 8, 2018) (“Because a conversion claim is dependent on the unauthorized possession of the property at issue interfering with the rightful owner’s right of possession, courts in this Circuit have routinely rejected conversion claims predicated on a defendant’s possession of an electronic copy of the property”) (citing cases); accord Broker Genius, Inc. v. Seat Scouts LLC, 2018 WL 2214708, at \*6 (S.D.N.Y. May 14, 2018); Hyo Jung v. Chorus Music Studio, Inc., 2014 WL 4493795, at \*8 (S.D.N.Y. Sept. 11, 2014); SBIW, Inc. v. Gen. Elec. Co., 2013 WL 5338525, at \*13 (S.D.N.Y. Sept. 24, 2013); Geo Grp., Inc. v. Cmty. First Servs., 2012 WL 1077846, at \*8-9 (E.D.N.Y. Mar. 30, 2012). While we are aware of scattered decisions that suggest that copying of data may constitute conversion, see Clark St. Wine & Spirits v. Emporos Sys. Corp., 754 F. Supp. 2d 474, 484 (E.D.N.Y. 2010); Astroworks, Inc. v. Astroexhibit, Inc., 257 F. Supp. 2d 609, 618 (S.D.N.Y. 2003); N.Y. Racing Ass’n v. Nassau Reg’l Off-Track Betting Corp., 29 Misc. 3d 539, 545-46 (Sup. Ct. 2010),<sup>3</sup> we cannot square these decisions with the New York Court of

---

<sup>3</sup> We do not include Comprehensive Cmty. Dev. Corp. v. Lehach, 223 A.D.2d 399 (1st Dep’t 1996), in this list because it held only that “[r]etention of copies may be found to be conversion under the circumstances, especially if the originals were missing.” Id. at 399 (emphasis added). Here, of course, there is no allegation that originals went missing. Notably, in a case involving paper materials, the Second Circuit, interpreting New York law, held that even the temporary removal of materials is not enough to state a conversion claim. In Harper & Row Publishers, Inc. v. Nation Enters., 723 F.2d 195 (2d Cir. 1983), rev’d on other grounds, 471 U.S. 539 (1985), the Court dismissed a New York state conversion claim on the ground that



Appeals' statement in Thyoff that a conversion claim lies where the defendant's exercise of control was "to the exclusion of the owner's rights." 8 N.Y.3d at 288-89.

Iovance's argument relies in large part on an interpretation of Thyoff as expressed in N.Y. Racing. D. Reply at 4. The reasoning of N.Y. Racing on this point was contained in the following two sentences:

In Thyoff, the Court of Appeals suggest[ed] that plaintiff may maintain an action for conversion where its electronically stored data is misappropriated, regardless of whether plaintiff has been excluded from access to its intangible property. The Court noted that it is the information which is stored in the computer that has "intrinsic value," rather than the "physical nature" of the document.

N.Y. Racing, 29 Misc. 3d at 545-46 (quoting Thyoff, 8 N.Y.3d at 292). In Thyoff, however, the Court of Appeals considered only the issue of whether a claim for conversion of electronic data is cognizable under New York law under any circumstances. Thyoff, 8 N.Y.3d at 285-86. Thyoff did not address any of the elements of conversion. Thus, in the second sentence in the above quote, Thyoff simply highlights the intrinsic value of electronic information. It did so without regard to the question of whether a copier of electronic information does so "to the exclusion of the owner's rights." Thyoff, 8 N.Y.3d at 288-89.

Accordingly, because the conversion counterclaim cannot survive a motion to dismiss, it cannot be permitted in the amended complaint.

#### B. Trespass to Chattels

Under New York Law,

[a] trespass to chattel occurs when a party intentionally damages or interferes with the use of property belonging to another. Interference may be accomplished

---

"[m]erely removing one of a number of copies of a manuscript (with or without permission) for a short time, copying parts of it, and returning it undamaged, constitutes far too insubstantial an interference with property rights to demonstrate conversion." Id. at 201.

by [1] dispossessing another of the chattel or [2] using or intermeddling with a chattel in the possession of another. Traditionally, courts have drawn a distinction between interference by dispossession, which does not require a showing of actual damages, and interference by unauthorized use or intermeddling which requires a showing of actual damages.

Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 437 (2d Cir. 2004) (internal quotation marks and citations omitted). Stated otherwise, “[t]he elements of trespass to chattel are (1) intent, (2) physical interference with (3) possession, resulting in (4) harm.” Amos Fin., LLC v. H & B & T Corp., 48 Misc. 3d 1205(A), 2015 WL 3953325, \*8 (Sup. Ct. 2015) (emphasis added) (citation, internal quotation marks, and brackets omitted); accord Chevron Corp. v. Donziger, 871 F. Supp. 2d 229, 258 (S.D.N.Y. 2012). The “harm” at issue is “harm to the condition, quality or material value of the chattels at issue” and the showing of such harm is “an essential element” in pleading trespass to chattels. “J. Doe No. 1” v. CBS Broad. Inc., 24 A.D.3d 215, 215 (1st Dep’t 2005); accord Kronos, Inc. v. AVX Corp., 81 N.Y.2d 90, 95 (1993) (to state claim for trespass to chattels, “actual loss must be demonstrated”).

Here, there is no allegation that Iovance’s computers or electronic files were affected in any way and thus the “harm” element has not been met. This is clearly explained in Twin Securities, Inc. v. Advoc. & Lichtenstein, LLP, 113 A.D.3d 565, 565 (1st Dep’t 2014), in which a defendant copied files from a hard drive without permission. The First Department squarely held that a claim of trespass to chattels was “not viable since there is no indication that the condition, quality or value of the computer, its hard drive, or any of the information on the computer was diminished as a result of defendants’ duplication of the hard drive.” Id. at 565-66; accord Hecht v. Components Int’l, Inc., 22 Misc. 3d 360, 370 (Sup. Ct. 2008) (“Interference with information stored on a computer may give rise to trespass to chattel if plaintiff is dispossessed of the information or the information is impaired as to its condition, quality or value.”)

(emphasis added).

Iovance argues that the mere fact of copying in fact “impaired the value” of its files because the copied material contained sensitive personal information of employees and investors and thus the copying “affected [Iovance’s] reporting duties under state and federal law.” D. Reply at 5-6 (citing PAA ¶ 92). The problem with this argument is that the tort of trespass to chattels requires a showing of “harm to the condition, quality or material value of the chattels at issue.” “J. Doe No. 1”, 24 A.D.3d at 215 (emphasis added). In other words, it is not enough to show that the owner of the materials was harmed in some way by the challenged conduct. Rather, the owner must show some type of harm to the chattels themselves. As one court put it, in “the online context, trespass ‘does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning.’” Mount v. PulsePoint, Inc., 2016 WL 5080131, at \*9 (S.D.N.Y. Aug. 17, 2016) (quoting Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347 (2003)) (no trespass to chattels claim where there were “no particularized allegations of diminished device performance”), aff’d, 684 F. App’x 32 (2d Cir. 2017); cf. Sch. of Visual Arts v. Kuprewicz, 3 Misc. 3d 278, 282 (Sup. Ct. 2003) (trespass action viable where there are allegations of “depleted hard disk space, drained processing power, [or when the conduct] adversely affected other system resources”).

The two cases Iovance relies on, see D. Reply at 5-6, are consistent with this principle and thus offer Iovance no help. In Davidoff v. Davidoff, 12 Misc.3d 1162(A), 2006 WL 1479558 (Sup. Ct. May 10, 2006), the defendant “caus[ed] a depletion or deletion of information” from plaintiff’s website, “thereby adversely affecting [its] effectiveness.” Id. at \*10. In the other case, Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004), the defendant used a search robot to access the plaintiff company’s computer systems without

authorization. Id. at 396. Register found that a trespass to chattels claim could proceed because “(1) Register.com’s computer systems are valuable resources of finite capacity, (2) unauthorized use of such systems depletes the capacity available to authorized end-users, [and] (3) unauthorized use of such systems by software robot [sic] creates risks of congestion and overload that may disrupt Register.com’s operations.” Id. at 438. In other words, Register’s holding relied on harm to the actual chattel at issue — that is, the plaintiff’s computer system. Here, as Iovance recognizes, the PAA merely alleges that plaintiff’s actions “damaged or destroyed [the] confidential nature” of Iovance’s computer files. D. Reply at 6. Because Iovance has not alleged harm to its computer system or files, its trespass to chattels claim fails.

### C. Computer Fraud and Abuse Act Violation

The Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, in pertinent part, punishes an individual who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C).<sup>4</sup> The CFAA was initially enacted solely as a criminal statute to address the “then-novel problem of [computer] hacking.” Hancock v. Cty. of Rensselaer, 882 F.3d 58, 63 (2d Cir. 2018). Ten years later, see id., it was amended to permit a civil cause of action allowing, among other things, “any person who suffers damage or loss by reason of a violation of this section” of at least \$5,000 to bring a claim. 18 U.S.C. § 1030(g); § 1030(c)(4)(A)(i)(I); accord Sewell v. Bernardin, 795 F.3d 337, 339-40 (2d Cir. 2015).

---

<sup>4</sup> Iovance’s counterclaims do not specify which subsection of the CFAA it alleges Fischkoff has violated. However, because its papers refer repeatedly to the question of “authorized access,” e.g., D. Reply at 7, we have assumed Iovance intends to rely on one of the provisions of the CFAA that uses that language. The provision most pertinent to the allegations in the complaint is § 1030(a)(2)(C).

Here, it is alleged that the Iovance “Employee Handbook” placed restrictions on Fischkoff’s access to Iovance’s electronic materials. PAA ¶ 21. Specifically, the handbook “restricted Plaintiff’s access to confidential information on a ‘need to know basis’ subject to the approval of his supervisor, the Chief Executive Officer.” Id.; accord id. ¶ 38. The counterclaim alleges that Fischkoff copied emails and other company documents “without authorization and without informing his supervisor or other Company employees or seeking or obtaining their consent.” Id. ¶ 35; accord id. ¶ 39. It is alleged that Fischkoff’s copying allowed him to “obtain[] confidential and proprietary information from the Company’s protected computers, . . . including folders or files pertaining to Human Resources, Finance, and Personal Information of the Company’s employees and investors.” Id. ¶ 97.

Because Fischkoff was authorized to “enter” Iovance’s computer system, whether Fischkoff violated the CFAA turns on the question of whether he “exceed[ed] authorized access” within the meaning of the CFAA.

The meaning of this phrase arose in a similar context in the criminal case of United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015), in which the defendant police officer used his employer’s database for personal purposes. The defendant conceded that he had “violated the terms of his employment by putting his authorized computer access to personal use.” Id. at 523. He contended that he had not “exceeded authorized access,” however, because he was authorized in a general sense to look at the database he accessed. Id. at 523-24. The Government contended that Valle “exceeded authorized access” because “his authorization to access [the database] was limited to law enforcement purposes and he conducted a search . . . with no such purpose.” Id. at 524. Valle summarized the ambiguity in the statutory language as follows: “While ‘authorization’ could refer, as the Government contends, to the purposes for which one is

authorized to access a computer, it could alternatively refer to the particular files or databases in the computer to which one's authorization extends." Id.

Applying the rule of lenity, see id. at 526-28, Valle interpreted the statute "in spatial terms, namely, an employee going beyond the parameters of his access rights." Id. at 526. It found that the purpose of the access was not relevant. Id. It concluded that a person "'exceeds authorized access' only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access." Id. at 511. While Valle was a criminal case, the Supreme Court has noted that courts, when analyzing a statute that "has both criminal and noncriminal applications. . . . must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context." Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004)

Following Valle's reasoning, it has been held that the CFAA "does not apply to a 'so-called faithless or disloyal employee' — that is, an employee who has been granted access to an employer's computer and misuses that access, either by violating the terms of use or by breaching a duty of loyalty to the employer." Chefs Diet Acquisition Corp. v. Lean Chefs, LLC, 2016 WL 5416498, at \*6 (S.D.N.Y. Sept. 28, 2016); accord Apple Mortg. Corp., 162 F. Supp. 3d at 286 ("If an employer has given an employee access to the computer and to the relevant files, the employee's subsequent misuse of the information or misappropriation with the intent to compete with his employer is not sufficient to violate the CFAA."). In other words, "to prevail on its claim under the CFAA, [a plaintiff] must show that [d]efendants accessed its computer system without approval; it is not enough to prove access to information beyond the scope of approval." Chefs Diet, 2016 WL 5416498, at \*6.

The allegations in the PAA are that of a "faithless or disloyal employee." In other words,

Iovance alleges that Fischkoff accessed materials that his credentials permitted him to access but that the Employee Handbook instructed him not to access. In light of Valle and subsequent case law, we cannot find that these allegations support a claim under the CFAA.

Defendant also argues that Fischkoff “is alleged to have accessed these files following his termination.” D. Reply at 8 (emphasis omitted). Certainly, an employee may be liable under the CFAA where access to a computer system “occurs after the employee is terminated or resigns.” Sell It Soc., LLC v. Strauss, 2018 WL 2357261, at \*3 (S.D.N.Y. Mar. 8, 2018). But the complaint here does not allege access to Iovance’s computer system after Fischkoff’s termination. Instead, in the paragraph cited by defendants in support of this argument, PAA ¶ 55, the complaint alleges only that Fischkoff accessed his own internal hard drive. Because Iovance does not and cannot allege that Iovance was responsible for granting access to Fischkoff’s own hard drive, there can be no CFAA violation for his doing so.

None of the cases cited by Iovance to support its argument suggest a different result. Apple Mortgage Corp. v. Barenblatt, 162 F. Supp. 3d 270 (S.D.N.Y. 2016), involved employees who accessed email on their employer’s computer after they had resigned. Id. at 286. In Jensen v. Cablevision Systems Corp., 2017 WL 4325829 (E.D.N.Y. Sept. 27, 2017), the plaintiff alleged in detail how defendants accessed without authorization plaintiff’s Optimum Online Wi-Fi router in order to broadcast a separate public Optimum Wi-Fi network. Id. at \*1-3. In Jensen, the court allowed the CFAA claim to proceed “[b]ecause a genuine issue of material fact exist[ed] as to whether the Defendants accessed the Plaintiff’s wireless router without authorization.” Id. at \*12. While some of the reasoning in Khazarian v. Gerald Metals, LLC, 2017 WL 5240868 (D. Conn. Nov. 9, 2017), is not entirely clear, it appears that the court concluded that the allegations in the complaint alleged that defendants “accessed information

unrelated to [plaintiff's] work computer," id. at \*8-9, and that they had no authority to do so.

In sum, Iovance has not stated a violation under the CFAA.

D. New Jersey Theft and Related Offenses Act Violation

Iovance alleges that Fischkoff has possessed and received stolen property in the form of Iovance's confidential materials including clinical data, medical studies, and clinical protocols in violation of New Jersey's Theft and Related Offenses Act, N.J.S.A. § 2C:20-7; 20-20 (the "Theft Act"). See PAA ¶ 103. It alleges that plaintiff "frequently worked from his home in the State of New Jersey." Id.

New Jersey's Theft Act makes it unlawful for a person to "knowingly receive[] or bring[] into [the state of New Jersey] movable property of another knowing that it has been stolen, or believing that it is probably stolen." N.J.S.A. § 2C:20-7(a); accord State v. Hodde, 181 N.J. 375, 384 (2004). Subsection 2C:20-20 "creates a civil right of action where the conduct in question violates the penal statute," including § 2C:20-7(a). A & G Research, Inc. v. GC Metrics, Inc., 19 Misc. 3d 1136(A), 2008 WL 2150110, at \*19 (Sup. Ct. 2008). "Movable property" is defined under the statute as "property the location of which can be changed, including things growing on, affixed to, or found in land, and documents, although the rights represented thereby have no physical location." § 2C:20-1(e).

Iovance's claim under the Theft Act fails because accepting, arguendo, that Iovance's electronic data existed in some physical form at Iovance's offices or on its computer servers, and also accepting, arguendo, that this data constituted "moveable" property, it is not alleged that Fischkoff moved the physical manifestation of Iovance's electronic data at any time. See PAA ¶¶ 103-109. Rather, all that is alleged is that Iovance's data was copied. In other words, the complaint does not allege that the location of Iovance's original electronic files, to the extent



they exist in physical form, was ever changed. As a consequence, Iovance has not alleged that Fischkoff “receive[d] or br[ought]” into the State of New Jersey, the only actual “movable property” that could be the subject of a claim under the statute.

Certainly, Fischkoff’s act of copying caused him to possess a copy of Iovance’s electronic files in some physical form. But by alleging that these files were copied from Iovance’s servers, see, e.g., PAA ¶¶ 34, 42, 98, the PAA by implication alleges that Fischkoff created an entirely new electronic file on his hard drive or on the email server of his service provider. In any event, there is no allegation that a physical file in Iovance’s possession was ever transported from Iovance’s offices or servers to New Jersey. Iovance’s claim thus fails for the same reasons as would a claim by Iovance that Fischkoff took photographs of confidential Iovance information and brought those photographs to New Jersey.

While this interpretation of the statute seems obvious, it is bolstered by the fact that, under New Jersey law, where a criminal statute is subject to a broad and a narrow interpretation, the court is “constrained to apply the narrow one.” State v. Morrison, 227 N.J. 295, 314 (2016) (citing State v. Shelley, 205 N.J. 320, 328 (2011)). Notably, as A&G Research recognized, “to the extent that any New Jersey court has applied Sections 20–20 and 20–7 to computers, it is only with respect to the physical stealing of computer equipment.” 2008 WL 2150110, at \*20 (citing cases).

Iovance points to the result reached in A& G Research as supporting its position. Indeed, A& G Research, like our case, involved a claim that the defendant had copied plaintiff’s computer files. Id. at \*5-8. After discussing the arguments for and against the application of the statute to this conduct, the court asserted merely that “it is apparent that questions of fact exist as to whether the New Jersey Theft and Related Offenses statute applies on these facts and, further,

as to whether Defendants are liable under the statute . . . for their conduct in downloading and using computer data from A & G's computers." Id. at \*21. The court gave no explanation as to why the claim actually fit into the Theft Act's elements. In light of the lack of reasoning, and given the fact that Iovance's data remained where it was after Fischkoff committed the conduct complained of in the counterclaim, we decline to follow A & G Research.

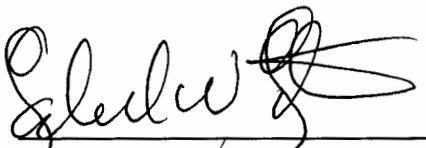
Because Iovance has not stated a claim under the Theft Act, assertion of the proposed counterclaim in an amended complaint would be futile.

#### IV. CONCLUSION

For the foregoing reasons, defendant's motion to amend (Docket # 106) is denied.

Dated: October 17, 2018

New York, New York

  
\_\_\_\_\_  
GABRIEL W. GORENSTEIN  
United States Magistrate Judge