

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF
COLUMBIA**

NEW TOUCH DIGITAL INC,

Plaintiff,

v.

VICTOR CHRISTOPHER CABRAL,

Defendant.

No. 20-cv-1878 (DLF)

MEMORANDUM OPINION AND ORDER

Before the Court is defendant Victor Cabral's Motion to Dismiss, Dkt. 12. For the reasons that follow, the Court will deny the motion.

This case arises out of a dispute between New Touch Digital and its former Chief Technology Officer, Victor Cabral. Compl. ¶ 1, Dkt. 1. While at New Touch Digital, Cabral used his personal laptop for company-related work. *Id.* ¶ 22. After he resigned from his position, he took important company data stored on the laptop with him. *Id.* ¶¶ 76–79. New Touch Digital repeatedly asked Cabral to return the company's intellectual property. *Id.* ¶¶ 79, 81, 85. However, Cabral did not turn over certain identification numbers and passwords. *Id.* ¶¶ 78–80, 82–83. Instead, his counsel responded to New Touch Digital with the following: “in response to your letter claiming [Cabral] tortuously retained Company property, he wiped his personal laptop clean of any and all New Touch data, passwords, and other claimed proprietary information.” *Id.* ¶¶ 86–87.

New Touch Digital alleges that it has suffered substantial harm because of this “wiping” of its data, including a significant delay in New Touch Digital's clinical trials for one of its products. *Id.* ¶ 91. Thus, New Touch Digital brought this suit alleging that Cabral

violated the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, along with several state law claims. Compl. ¶ 1.

Cabral has filed a motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure, alleging that New Touch Digital failed to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). To survive a Rule 12(b)(6) motion, a complaint must contain factual matter sufficient to “state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A facially plausible claim is one that “allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). This standard does not amount to a specific probability requirement, but it does require “more than a sheer possibility that a defendant has acted unlawfully.” *Id.*; *see also Twombly*, 550 U.S. at 557 (“Factual allegations must be enough to raise a right to relief above the speculative level.”). A complaint need not contain “detailed factual allegations,” but alleging facts that are “merely consistent with a defendant’s liability . . . stops short of the line between possibility and plausibility.” *Iqbal*, 556 U.S. at 678 (internal quotation marks omitted).

Well-pleaded factual allegations are “entitled to [an] assumption of truth,” *id.* at 679, and the court construes the complaint “in favor of the plaintiff, who must be granted the benefit of all inferences that can be derived from the facts alleged,” *Hettinga v. United States*, 677 F.3d 471, 476 (D.C. Cir. 2012) (internal quotation marks omitted). The assumption of truth does not apply, however, to a “legal conclusion couched as a factual allegation.” *Iqbal*, 556 U.S. at 678 (quotation marks omitted). An “unadorned, the defendant-unlawfully-harmed-me accusation” is not credited; likewise, “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* Ultimately, “[d]etermining whether a complaint states a plausible claim for relief [is] a context-specific task that requires the reviewing court to draw on its judicial

experience and common sense.” *Id.* at 679. When deciding a Rule 12(b)(6) motion, the court may consider only the complaint itself, documents attached to the complaint, documents incorporated by reference in the complaint, and judicially noticeable materials. *EEOC v. St. Francis Xavier Parochial Sch.*, 117 F.3d 621, 624 (D.C. Cir. 1997).

New Touch Digital alleges that Cabral violated section 1030(a)(5)(A) of the CFAA, which makes it unlawful to “knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer.” 18 U.S.C. § 1030(a)(5)(A). “The CFAA is a criminal statute; however, subsection (g) of the statute provides a civil cause of action to any person who suffers damage or loss by reason of a violation’ of the CFAA.” *Lewis-Burke Assocs., LLC v. Widder*, 725 F. Supp. 2d 187, 191 (D.D.C. 2010) (internal quotation marks omitted). The term “protected computer” is defined in the statute as “a computer” “which is used in or affecting interstate commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). Courts have agreed that “effectively all computers with Internet access” constitute “protected computers” under this broad definition. *See, e.g., United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc); *United States v. Yücel*, 97 F. Supp. 3d 413, 418–19 (S.D.N.Y. 2015) (noting “widespread agreement in the case law on the meaning of ‘protected computer’”); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 192 (D.D.C. 2017) (same). The term “damage” means “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8).

Cabral’s primary argument is that the “purpose of the CFAA is to target hackers,” Def.’s Mot. to Dismiss at 5, Dkt. 5-1 (quoting *Hedgeye*, 271 F. Supp. 3d at 195), and that the circuits are split over what it means for an employee to *access* a computer without authorization or in excess of authorization. *See* Def.’s Mot. to Dismiss. It is true that the circuits are split on this interpretive question. Some courts hold that an employee’s

authorization to access a computer only extends so far as the employee acts according to the interests of her employer. *See Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–421 (7th Cir. 2006); *see also Widder*, 725 F. Supp. 2d at 191 (noting this line of cases). Meanwhile, another line of cases takes a broader view of authorization to access, holding that the plain language of the CFAA requires that when “an employer gives an employee permission to use [a computer],” the employer is giving that “employee ‘authorization’ to access,” regardless of whether the employee acts contrary to the employer’s interest. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

Yet this circuit split on the meaning of authorized access under CFAA § 1030(a)(2) and (a)(4) is inapposite because New Touch Digital did not bring a suit under either of those statutory provisions. Rather, its federal claim centers solely on § 1030(a)(5)(A)—an entirely different provision. This distinction is important because while the other sub-sections make it unlawful simply to *access* a computer without authorization, section (a)(5)(A) does not. Instead, section (a)(5)(A) makes it unlawful to “intentionally cause[] damage without authorization.” *Id.* It has nothing to do with mere access. For this reason, any debate amongst the circuits over the meaning of authority to access a computer is not relevant. The relevant question is not whether Cabral had authorization to access his personal computer with company data on it, but whether he had authorization to damage it—defined by the statute as causing “impairment to the integrity or availability of data.” *Id.* § 1030(e)(8). Thus, although courts in this district have ruled along with the *Brekka* line of cases, *see, e.g., Widder*, 725 F. Supp. 2d at 194, defining authorization to access broadly, these cases concern a different question than the one currently before the Court and, as a result, provide no basis to dismiss the complaint.

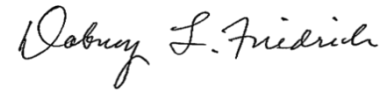
As to the supposed purpose of the CFAA, courts have held that the CFAA protects against *both* “attacks by virus and worm writers, on the one hand, which come mainly from the

outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other.” *Citrin*, 440 F.3d at 420. In any case, broad overtures to statutory purpose cannot narrow the CFAA's plain text.

Alternatively, Cabral argues that New Touch Digital has not adequately pled that it suffered a legal loss under the CFAA. *See* 18 U.S.C. § 1030(e)(11). Legal loss is defined as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Id.* New Touch Digital has adequately pled legal loss to survive a motion to dismiss. The complaint states that New Touch Digital “has suffered and will continue to suffer damages in the form of lost profits relating to the delay in clinical trials, delay in FDA approval, and delay in NTD's ability to bring, to market, NTD's mobile health and data analytics platform, and monetary damages for the costs and expenses incurred by NTD in replicating and replacing the passwords, code, and other intellectual property that Cabral failed and refused to return to NTD, and that he eventually destroyed by ‘wiping’ his computer clean of that intellectual property.” Compl. ¶ 107. This resulted in damages “over a one-year period, aggregating well in excess of \$5,000.00.” *Id.* ¶ 105. To the extent that Cabral raises potential factual disputes as to whether New Touch Digital indeed suffered that damage, *see* Def.'s Mot. to Dismiss at 6–8, those disputes are properly considered at a later stage of this litigation.

Accordingly, it is

ORDERED that the defendant's Motion to Dismiss, Dkt. 12, is **DENIED**.

A handwritten signature in cursive script, reading "Dabney L. Friedrich".

DABNEY L. FRIEDRICH
United States District Judge

October 7, 2020