IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

GSP FINANCIAL SERVICES, LLC, *

Plaintiff, *

v. **Case No.: GJH-18-2307**

*

LATASHA NICOLE HARRISON,

*

Defendant.

*

* * * * * * * * * * * *

MEMORANDUM OPINION

Plaintiff GSP Financial Services, LLC ("GSP") brings this action against Defendant Latasha Nicole Harrison, alleging violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("Count I"), tortious interference with economic or contractual relationships ("Count II"), and trespass ("Count III"). ECF No. 1. Following Defendant's failure to answer or otherwise defend in this action, the Clerk entered default against Defendant on October 16, 2020. ECF No. 32. Now pending before the Court is Plaintiff's Motion for Default Judgment pursuant to Fed. R. Civ. P. 55(b). ECF No. 36. No hearing is necessary. *See* Loc. R. 105.6 (D. Md. 2018). For the following reasons, Plaintiff's Motion for Default Judgment is granted, and judgment is entered against Defendant in the amount of $16,999.50.

I. BACKGROUND

The following facts are established by the Complaint, ECF No. 1, and evidentiary exhibits in support of the Motion for Default Judgment, ECF Nos. 36-1, 36-2, 36-3, 36-4. GSP is an accounting and financial advisory firm specializing in servicing startup and technology

businesses. ECF No. 1 ¶ 6; ECF No. 36-1 ¶ 2. [1] GSP maintains sensitive and confidential financial information of its clients, including information about their revenues, profits, expenses, and projections, and also has access to clients' financial institution accounts, including their bank accounts. ECF No. 1 ¶ 7; ECF No. 36-1 ¶ 2. Defendant Latasha Nicole Harrison worked for GSP as a Senior Accounting Strategist until, at approximately 1:00 pm on Friday, July 20, 2018, she was informed that she was terminated effective immediately after failing to participate in a client conference call on July 19, 2018, and to show up for work on July 20, 2018. ECF No. 1 ¶¶ 10–11; ECF No. 36-1 ¶¶ 3–4. Plaintiff also provided Defendant with a written notice of termination. ECF No. 1 ¶ 11; ECF No. 36-1 ¶ 4. Although during her employment she had access to clients' sensitive and confidential financial information, according to Plaintiff, upon Defendant's termination, she was no longer authorized to access any GSP data or systems. ECF No. 1 ¶¶ 9, 12; ECF No. 36-1 ¶ 5. However, her access to GSP's systems and accounts was not immediately cut off. *See* ECF No. 1 ¶ 13.

On or about Sunday, July 22, 2018, Defendant used her GSP access credentials to log into GSP's LastPass account. *Id.* ¶ 14. LastPass is a cloud-based system that serves as a centralized password and data management and encryption service. *Id.*; ECF No. 36-1 ¶ 6. Defendant moved several shared folders into another folder to which other GSP personnel do not have access. ECF No. 1 ¶¶ 15, 19; ECF No. 36-1 ¶ 7. One of these folders, called "GSP Client Passwords," contained the login information for clients' bank and other financial accounts. ECF No. 1 ¶ 15; ECF No. 36-1 ¶ 7. Using the information in that folder, Defendant changed the login information for accounts used or owned by GSP at FreshBooks (a cloud-based accounting software system), SunTrust Bank, ADP (a payroll processor), PNC Bank, Chase Bank, American

[1] Pin cites to documents filed on the Court's electronic filing system (CM/ECF) refer to the page numbers generated by that system.

Express, Booker (an online booking, payment, and customer management system), PrismHR, Bank of America, PayPal (an online payment processing system), United Bank, and SurePayroll. ECF No. 1 ¶ 16; ECF No. 36-1 ¶ 8. The following morning, at approximately 10:26 am on July 23, 2018, Defendant logged into GSP's DropBox cloud-based document storage account, where she accessed at least 17 files, many of which contained sensitive or confidential information. ECF No. 1 ¶¶ 21–23; ECF No. 36-1 ¶ 11.

After the close of business on July 23, 2018, GSP discovered Defendant's activity and took steps to investigate the nature and extent of it, notify clients of the breach, regain access to the accounts, consult with cybersecurity professionals, and consult with legal counsel regarding GSP's obligations under the laws of the states in which affected clients may reside. ECF No. 1 ¶¶ 24–25; ECF No. 36-1 ¶ 12. Those steps took three full-time employees, who would otherwise have been performing billable work for clients, three days of time to complete. ECF No. 1 ¶ 26. On July 24, 2018, counsel for GSP emailed a letter to Defendant demanding that she cease and desist from the activity, identify the accounts and systems that she had accessed or deleted since her employment was terminated, provide the new login information for accounts that she had altered, and surrender for forensic investigation computers or devices used to access GSP's systems or onto which she had transmitted GSP or GSP clients' data. *Id.* ¶ 27. Defendant did not respond. *Id.* ¶ 28.

Plaintiff filed the instant Complaint against Defendant on July 27, 2018. ECF No. 1. Along with the Complaint, Plaintiff filed an Emergency Motion for Temporary Restraining Order ("TRO"). ECF No. 2. A hearing was held on July 30, 2018, and Defendant did not appear. ECF No. 6. This Court granted the TRO and entered it on July 31, 2018. ECF No. 9. Defendant was properly served with the TRO as well as GSP's Complaint and the Court's Summons on

August 1, 2018. *See* ECF No. 15. On August 7, 2018, GSP filed an Emergency Motion to Hold Defendant in Contempt for Failure to Comply with the Temporary Restraining Order. ECF No. 10. The Court entered an Order to Show Cause and set a hearing for August 14, 2018. ECF No. 11. Defendant again failed to appear, and the Court rescheduled the Show Cause Hearing, first to August 21, 2018, ECF No. 16, and then to August 28, 2018, ECF No. 18. The Show Cause Hearing was held on August 28, 2018. ECF No. 21. Defendant failed to appear, and this Court issued an arrest warrant for her. ECF No. 22. The arrest warrant is outstanding. On September 12, 2018, this Court held a Preliminary Injunction hearing. ECF No. 23. Defendant did not appear. This Court entered a Preliminary Injunction Order on October 3, 2018. ECF No. 26.

On April 24, 2020, Plaintiff filed a Motion for Clerk's Entry of Default. ECF No. 31. The Clerk entered default against Defendant on October 16, 2020. ECF No. 32. On November 13, 2020, Plaintiff filed a Motion for Default Judgment. ECF No. 36. Plaintiff seeks default judgment against Defendant in the amount of $1,952.00 for legal fees to ascertain its notification obligation under the laws of various states of residence of affected clients;[2] $7,847.50 for consulting fees to analyze and ascertain the extent of the breach; $2,942.00 in salaries for full-time employees who had to cease performing their usual duties to investigate and address the breach; and $7,200.00 in lost billable time for those same full-time employees—for a total of $19,941.50. *Id.* at 2.

II. STANDARD OF REVIEW

"When a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise, the clerk must enter the party's default." Fed. R. Civ. P. 55(a). "A defendant's default does not automatically

[2] Plaintiff states that this amount does not include fees relating to this litigation. ECF No. 36 at 2.

entitle the plaintiff to entry of a default judgment; rather, that decision is left to the discretion of the court." *Educ. Credit Mgmt. Corp. v. Optimum Welding*, 285 F.R.D. 371, 373 (D. Md. 2012). Although "[t]he Fourth Circuit has a 'strong policy' that 'cases be decided on their merits,'" *Choice Hotels Intern., Inc. v. Savannah Shakti Carp.*, No. DKC-11-0438, 2011 WL 5118328, at *2 (D. Md. Oct. 25, 2011) (citing *United States v. Shaffer Equip. Co.*, 11 F.3d 450, 453 (4th Cir. 1993)), "default judgment may be appropriate when the adversary process has been halted because of an essentially unresponsive party[.]" *Id.* (citing *S.E.C. v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005)).

"Upon default, the well-pled allegations in a complaint as to liability are taken as true, although the allegations as to damages are not." *Lawbaugh*, 359 F. Supp. 2d at 422; *see also Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001) (noting that "[t]he defendant, by [its] default, admits the plaintiff's well-pleaded allegations of fact," which provide the basis for judgment); *Lary v. Trinity Physician Fin. & Ins. Servs.*, 780 F.3d 1101, 1106 (11th Cir. 2015) ("It is well settled that . . . '[t]he defendant is not held to admit facts that are not well-pleaded.'" (quoting *Nishimatsu Constr. Co. v. Houston Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975)). Upon a finding of liability, "[t]he court must make an independent determination regarding damages[.]" *Int'l Painters & Allied Trades Indus. Pension Fund v. Capital Restoration & Painting Co.*, 919 F. Supp. 2d 680, 684 (D. Md. 2013). Fed. R. Civ. P. 54(c) limits the type of judgment that may be entered based on a party's default: "A default judgment must not differ in kind from, or exceed in amount, what is demanded in the pleadings." While the Court may hold a hearing to prove damages, it is not required to do so; it may rely instead on "detailed affidavits or documentary evidence to determine the appropriate sum." *Adkins v. Tesco*, 180 F. Supp. 2d 15, 17 (2001) (citing *United Artists Corp. v. Freeman*, 605 F.2d 854, 857 (5th Cir. 1979)).

III. DISCUSSION

The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 (federal question), and 28 U.S.C. § 1367(a) (supplemental jurisdiction). *See Tech Sys., Inc. v. Pyles*, 630 F. App'x 184, 188 (4th Cir. 2015). Venue is proper under 28 U.S.C. § 1391(b)(1) because GSP is a Maryland corporation and Defendant resides in Maryland. ECF No. 1 ¶ 1–2, 5.

A. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1986 ("CFAA"), Pub. L. No. 99–474, 100 Stat. 1213, is primarily a criminal statute designed to combat hacking, but it also creates a private cause of action. 18 U.S.C. § 1030(g). The statute provides, in pertinent part:

> 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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).

Id. Thus, a private plaintiff must prove that the defendant violated one of the provisions of § 1030(a)(1)–(7), and that the violation involved one of the factors listed in § 1030(c)(4)(A)(i). Plaintiff claims that Defendant's conduct involved the factor described in subsection (c)(4)(A)(i)(I), which proscribes conduct that causes "loss to 1 or more persons during any 1–year period . . . aggregating at least $5,000 in value." Plaintiff further claims that Defendant violated sections 1030(a)(2)(A), 1030(a)(2)(C), 1030(a)(5)(B), and 1030(a)(5)(C), which prohibit any person from:

1. Intentionally accessing any computer without authorization or in excess of authorized access and thereby obtaining information contained in a financial record of a financial institution, 18 U.S.C. § 1030(a)(2)(A);
2. Intentionally accessing any computer without authorization or in excess of authorized access and thereby obtaining information from a protected computer, 18 U.S.C. § 1030(a)(2)(C);
3. Intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage, 18 U.S.C. § 1030(a)(5)(B); or,

4. Intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage or loss, 18 U.S.C. § 1030(a)(5)(C).

Therefore, to bring an action successfully under 18 U.S.C. § 1030(g) based on a violation of 18 U.S.C. § 1030(a)(2), Plaintiff must allege that Defendant: (1) intentionally accessed a computer (2) without authorization or exceeding authorized access, (3) thereby obtaining information (4) either (a) contained in a financial record of a financial institution or (b) from any protected computer. To bring an action based on a violation of 18 U.S.C. § 1030(a)(5), Plaintiff must allege that Defendant: (1) intentionally accessed a protected computer (2) without authorization—exceeding authorized access will not suffice—and that she (3) caused damage or loss.[3] Per the CFAA, a "computer" is a "high-speed processing device . . . and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). A computer becomes a "protected computer" when it "is used in or affecting interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B).

First, Plaintiff sufficiently alleges that Defendant intentionally accessed a "protected computer," as "[t]he GSP computer and information systems accessed by Harrison . . . are (i) connected to the Internet which is an element of interstate commerce and communication, (ii) used by GSP to service and communicate with clients located across the country, and (iii) maintained by financial institutions and cloud-based service providers who are based in other states and themselves operate in interstate commerce." ECF No. 1 ¶ 35; *see also id.* ¶¶14–16, 19, 21–22, 34 (alleging Defendant accessed the computers intentionally). Plaintiff also sufficiently alleges that Defendant obtained access to financial records maintained by financial institutions

[3] "Violations of subsections (a)(2) and (a)(5) do not need to be pled with particularity." *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 833 (N.D. Cal. 2014) (quoting *Prop. Rights Law Grp., P.C. v. Lynch*, No. 13–00273, 2013 WL 4791485, at *4 (D. Haw. Sep. 16, 2013)).

including SunTrust Bank, PNC Bank, Chase Bank, American Express, Bank of America, United Bank, and Capital One Bank. ECF No. 1 ¶ 34.

Plaintiff must therefore show this access was unauthorized or, for the purposes of 18 U.S.C. § 1030(a)(2), exceeded authorization. Plaintiff alleges that "[a]t all times following the termination of [Defendant's] employment with GSP at 1:00pm on Friday, July 20, 2018, Harrison was not authorized to access any of GSP's computer or information systems or accounts," ECF No. 1 ¶ 32, but her ability to access to GSP's systems and accounts was not immediately cut off, *see id.* ¶ 13. In the Fourth Circuit, "the fact that [the defendant] no longer worked for [the plaintiff] when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed." *United States v. Steele*, 595 F. App'x 208, 211 (4th Cir. 2014) (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009) ("There is no dispute that if [the defendant] accessed [the plaintiff]'s information . . . after he left the company . . . , [the defendant] would have accessed a protected computer 'without authorization' for purposes of the CFAA."); Restatement (Third) of Agency § 3.09 (2006) (Actual authority terminates "upon the occurrence of circumstances on the basis of which the agent should reasonably conclude" that authority is revoked.)); *see also Tech Sys., Inc. v. Pyles*, 630 F. App'x 184, 186 (4th Cir. 2015) ("[The defendant's] authorization to access the Blackberry terminated with her employment."). Although one court in this district found, prior to *Steele* and *Tech Sys., Inc.*, that an employee acts with authorization when her credentials or access have not been revoked, even if she had been terminated, *Intern. Ass'n of Machinists v. Werner-Matsuda*, 390 F. Supp. 2d 479 (D. Md. 2005),[4] other courts have determined that "if a

[4] *But see NRT Mid-Atl., Inc. v. Walker*, No. WDQ-05-CV-3350, 2006 WL 8456620, at *4 (D. Md. Jan. 30, 2006) (stating that the "*Werner-Masuda* decision adopted a narrow view of the CFAA because the Court looked at the early stages of the law and its primary focus as a criminal statute" and noting that the decision "criticized" *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), as "construing the

former employee accesses information without permission, *even if his prior log-in information is still operative as a technical matter*, such access would violate the CFAA," *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 831 (N.D. Cal. 2014) (quoting *Weingand v. Harland Financial Solutions, Inc.*, No. C–11–3109 EMC, 2012 WL 2327660, 2012 U.S. Dist. LEXIS 84844 (N.D. Cal. June 19, 2012)) (emphasis in *NetApp*). This Court agrees, and accordingly finds that, because Plaintiff alleges that Defendant accessed its computers after she was terminated, Plaintiff has shown this access was unauthorized.[5]

Finally, Plaintiff must establish that Defendant's actions caused loss to satisfy the final element of 18 U.S.C. § 1030(a)(5)(C), and that the loss was greater than $5,000 in a one-year period to satisfy 18 U.S.C. § 1030(c)(4)(A)(i)(I). The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]" 18 U.S.C. § 1030(e)(11). "Loss" includes "costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The Fourth Circuit in *iParadigms* went on to quote with approval a district court's holding that the value of "many hours of valuable

statute too broadly" while, "[o]n the other hand, this Court in *Role Models America, Inc. v. Jimmie Jones*, 305 F. Supp. 2d 564 (D. Md. 2004) cited *Shurgard* with approval," indicating a split within the District).

[5] Plaintiff alleges, in the alternative, that "to the extent Harrison ever had any access to authorize any of GSP's computer or information systems or accounts, she was never authorized to change the log-in information of those accounts," ECF No. 1 ¶ 33, and therefore Defendant accessed GSP's computers and information systems in excess of any authorization. However, the Fourth Circuit construes the statute narrowly, and in literally interpreting the statute, finds that it prohibits unauthorized access, not unauthorized use. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204, 206 (4th Cir. 2012); *see also Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669 (E.D. Pa. 2018) (noting that the Fourth Circuit "construe[s] the statute narrowly"). "Thus, according to this narrow view, an employee cannot be liable for misusing the information she was authorized to obtain." *Teva Pharm.*, 291 F. Supp. 3d at 669. Applied to this case, if Defendant had access to GSP's login information, she would not breach the statute by using that access in an improper and unauthorized way. Nevertheless, the Court's ultimate finding that Defendant violated the CFAA remains unaffected, as Plaintiff sufficiently alleged she acted without authorization.

time away from day-to-day responsibilities" falls within the § 1030(e)(11) definition of "loss." *Id.* (quoting *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980–81 (N.D. Cal. 2008)).

Once a qualified CFAA loss is shown, the plaintiff must also show that the costs were reasonably foreseeable—that they were caused by the CFAA violation—and that they were reasonably necessary. *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010) (citing *iParadigms, LLC*, 562 F.3d at 646); *see also United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000) (holding that jury instructions in CFAA criminal prosecution "correctly stated the applicable law" in requiring (i) that losses were "natural and foreseeable result" of any damage, and (ii) that losses included only cost of "what measures were reasonably necessary" to restore and resecure the system). Here, Plaintiff specifically alleges that Defendant's actions "caused loss to GSP in the form of substantial business interruption in investigating and addressing her unauthorized actions, lost revenues from billable time spent by GSP professionals in investigating and addressing her unauthorized actions, and legal fees (not including fees incurred in connection with this litigation) in satisfying GSP's legal obligations from the breach," and that those losses amounted to more than $5,000 at the time of filing, less than a week after the breach. *Id.* ¶¶ 38–39.

Thus, assuming the truth of the well-pleaded allegations in the Complaint, Plaintiff has established each of the elements of 18 U.S.C. § 1030(a)(2)(A), 18 U.S.C. § 1030(a)(2)(C), and 18 U.S.C. § 1030(a)(5)(C).[6] Plaintiff has also established the elements of 18 U.S.C. § 1030(c)(4)(A)(i). Accordingly, Plaintiff has sufficiently shown Defendant's liability under 18 U.S.C. § 1030(g) for accessing GSP's systems and altering the login information for its accounts.

[6] The Court need not determine whether the damage caused was reckless such that it amounts to a violation of 18 U.S.C. § 1030(a)(5)(B).

Cf., e.g., *Just Be Inc. v. Brisendine*, No. 3:18-CV-00537-SB, 2019 WL 2274990, at *2 (D. Or. May 3, 2019), report and recommendation adopted, No. 3:18-CV-00537-SB, 2019 WL 2270592 (D. Or. May 28, 2019) ("By altering the login credentials to [the plaintiff]'s Instagram account and subsequently using his unauthorized access to delete content from the account, [the defendant] intentionally caused damage to a protected computer without authorization."); *United States v. Grupe*, No. 17CR00901PJSDTS, 2018 WL 775358, at *1–2 (D. Minn. Feb. 8, 2018) (affirming criminal CFAA conviction of employee who used his former employer's laptop to change login credentials for, and subsequently delete, accounts used to access the employer's computer network); *Sewell v. Bernardin*, 795 F.3d 337, 338 (2d Cir. 2015) (discussing the plaintiff's civil CFAA claim against defendant ex-boyfriend who altered the login credentials for her Facebook account and used the unauthorized access to post malicious content).

B. Tortious Interference with Business Relationships

As a federal court exercising supplemental jurisdiction, this Court must apply the forum state's choice-of-law rules. *See Glennon v. Dean Witter Reynolds, Inc.*, 83 F.3d 132, 136 (6th Cir. 1996). In tort actions, Maryland courts apply the substantive law of the place where the wrong occurred. *Erie Ins. Exch, v. Heffernan*, 399 Md. 598, 624–25 (2007) (citing *Hauch v. Connor*, 295 Md. 120, 123–24 (1983)). Because Plaintiff's principal place of business is in the District of Columbia, District of Columbia law will apply. *See Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 696 (D. Md. 2011) ("[B]ecause the injury from the alleged tortious interference occurred in New York, where [the plaintiffs] maintain their business, New York tort law applies.").[7]

[7] However, Maryland and District of Columbia law impose essentially the same requirements to recover for tortious interference with business relationships. Under Maryland law, the elements of tortious interference with business relationships are: (1) intentional and willful acts; (2) calculated to cause damage to the plaintiffs in their lawful business; (3) done with the unlawful purpose to cause such damage and loss, without right or justifiable cause on the

To state a claim for tortious interference with a contract or business relationship under District of Columbia law, Plaintiff must plead "(1) the existence of a valid business relationship or expectancy, (2) knowledge of the relationship or expectancy on the part of the interferer, (3) intentional interference inducing or causing a breach or termination of the relationship or expectancy, and (4) resultant damage." *Browning v. Clinton*, 292 F.3d 235, 242 (D.C. Cir. 2002) (quoting *Bennett Enters. v. Domino's Pizza, Inc.*, 45 F.3d 493, 499 (D.C. Cir. 1995)) (applying D.C. law); *see also, e.g.*, *Whitt v. Am. Prop. Constr., P.C.*, 157 A.3d 196, 202 (D.C. 2017).

"[G]eneric allegations about the existing and prospective business relations affected are insufficient to plead plausibly tortious interference in the District." *Precision Contracting Sols., LP v. ANGI Homeservices, Inc.*, 415 F. Supp. 3d 113, 124 (D.D.C. 2019). Courts applying District law have regarded allegations of interference with "unspecified relationships," *Williams v. Fed. Nat. Mortg. Ass'n*, No. CIV 05-1483 (JDB), 2006 WL 1774252, at *8 (D.D.C. June 26, 2006), or with "hypothetical categories of business relationships" as inadequate to plead the existence of a business relationship or expectancy, *MiMedx Grp., Inc. v. DBW Partners LLC*, No. CV 17-1925 (JDB), 2018 WL 4681005, at *8 (D.D.C. Sept. 28, 2018); *see also Sharpe v. Am. Acad. of Actuaries*, 285 F. Supp. 3d 285, 292 (D.D.C. 2018) (requiring the plaintiff to "plead the specific contracts or expectancies that the [p]laintiff claims were interfered with").[8]

---

part of the defendants (which constitutes malice); and (4) actual damage and loss resulting. *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 703 (D. Md. 2011) (citing *Kaser v. Fin. Prot. Mktg., Inc.*, 376 Md. 621, 628–29 (2003)). Maryland law includes an additional element—that the interference occur through improper means, or, in other words, that the defendant's conduct must be "independently wrongful or unlawful, quite apart from its effect on the plaintiff's business relationships," *Alexander & Alexander Inc. v. B. Dixon Evander & Assocs., Inc.*, 336 Md. 635, 657, 650 A.2d 260, 271 (1994)—but because the Court finds Defendant's conduct violated the CFAA, this element is satisfied, meaning that this difference will not affect the Court's determination here.

[8] The same is true under Maryland law. *See Baron Fin. Corp. v. Natanzon*, 471 F. Supp. 2d 535, 546 (D. Md. 2006) (dismissing a tortious interference claim that alleged "some damage to [the plaintiff's] relationship with some unidentified [third-parties] at some future time in some future business [the plaintiff] might have"); *Nordstrom, Inc. v. Schwartz*, No. GJH-18-3080, 2019 WL 4221475, at *2–3 (D. Md. Sept. 5, 2019) ("Plaintiff does not identify, however, any specific transactions with bona fide purchasers that did not occur due to Defendant's conduct.").

Plaintiff's allegations of interference with relationships with unspecified "clients" are conclusory and insufficient. *See* ECF No. 1 ¶ 45 ("Harrison willfully and maliciously interfered with GSP's performance of its contractual and economic relationships by seeking to deprive GSP of access to financial accounts that is required for GSP to service its clients."); *id.* ¶ 48 ("GSP has incurred additional costs and damages in redressing Harrison's interference with GSP's performance of its contractual and economic relationships."). Thus, the Complaint does not sufficiently plead a claim for tortious interference with business relationships, and the Court does not find Defendant liable for Count II.

C. Trespass

As in the case of tortious interference with a contract or business relationship, this Court will apply Maryland choice-of-law rules and, accordingly, apply the law of the place of the harm. *See Glennon v. Dean Witter Reynolds, Inc.*, 83 F.3d 132, 136 (6th Cir. 1996); *Erie Ins. Exch, v. Heffernan*, 399 Md. 598, 624–25 (2007). "The place of the harm for a trespass to chattel claim has not been specifically discussed by Maryland courts." *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 696 (D. Md. 2011). In the context of the tort of conversion, recognized as similar to trespass to chattels but where the interference with the property interest is more substantial, Maryland courts have stated:

> [T]he gist of a conversion is not the acquisition of the property by the wrongdoer, but the wrongful deprivation of a person of property to the possession of which he is entitled. Accordingly, a conversion occurs at such time as a person is deprived of property which he is entitled to possess.

Staub v. Staub, 37 Md.App. 141, 143, 376 A.2d 1129 (1977) (citing *Saunders v. Mullinix,* 195 Md. 235, 240 (1950). "Following this logic, the location where the harm occurs would be the location of the plaintiff when he is deprived of the property. Where the harm is not a deprivation of possession, however, but an impairment to the object, the harm may occur where the tangible

object is located." *Ground Zero Museum Workshop*, 813 F. Supp. 2d at 696. Although the Complaint does not specify the location of the Lastpass or Dropbox servers affected, because Plaintiff's principal place of business is the District of Columbia, its law will apply. *See Skapinetz v. CoesterVMS.com, Inc.*, No. CV PX-17-1098, 2018 WL 805393, at *4–5 (D. Md. Feb. 9, 2018) (taking judicial notice of the fact that Google stores email communications on servers located throughout the United States and abroad and finding that, because the court cannot practically apply the law where the property is located, as that is unknown and potentially involves multiple Google servers at the time of the trespass, the law of the state where the plaintiff was located when his personal property interest was harmed by the defendants' trespass would apply); *see also Ground Zero Museum Workshop*, 813 F. Supp. 2d at 696 (finding that either the "law of the place where the chattel was located" or "the place where Plaintiffs were located at the time of the alleged trespass" would apply).

A defendant commits a trespass to a chattel under District of Columbia law by "intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another." *Hornbeck Offshore Transp., LLC v. United States*, 563 F.Supp.2d 205, 212 n. 8 (D.D.C. 2008) (quoting Restatement (Second) of Torts § 217 (1965)); *see also Pearson v. Dodd*, 410 F.2d 701, 707 n. 30 (D.C. Cir. 1969) (quoting Restatement language). "Although websites are not tangible property in the traditional sense, courts in Maryland, New York, and elsewhere have been willing to recognize claims for conversion or trespass to chattels involving certain digital things, such as websites and domain names and computer networks." *Ground Zero Museum Workshop*, 813 F. Supp. 2d at 697; *see also Mey v. Got Warranty, Inc.*, 193 F. Supp. 3d 641, 647 (N.D.W. Va. 2016) (noting that "[a] number of

courts have held that temporary electronic intrusion upon another person's computerized electronic equipment constitutes trespass to chattels" and listing cases).

Plaintiff alleges that Defendant "interfered with and trespassed upon GSP's possessory interest in its systems and accounts by accessing those systems and accounts without authorization and changing log-in information so as to deny GSP's own access." ECF No. 1 ¶ 53. Plaintiff further alleges that Defendant's actions "were undertaken without GSP's consent," *id.* ¶ 54, and that Defendant "undertook her actions of trespass with actual malice and an intention to injure GSP's business and reputation," *id.* ¶ 56. Plaintiff therefore sufficiently alleges the elements set out in *Hornbeck Offshore Transp. See* 563 F.Supp.2d at 212 n. 8.

However, under District of Columbia law, "liability for trespass to chattels exists only on a showing of actual damage to the property interfered with." *Pearson v. Dodd*, 410 F.2d 701, 707 (D.C. Cir. 1969). "The measure of damages in trespass is not the whole value of the property interfered with, but rather the actual diminution in its value caused by the interference." *Id.* Plaintiff alleged generally that Defendant's actions "caused, and will continue to cause, damages," but did not sufficiently allege that Defendant's actions caused a diminution in value of its systems and accounts, ECF No. 1 ¶ 55, and did not request damages for trespass in its Motion for Default Judgment, *see generally* ECF No. 36. Therefore, the Court does not find Defendant liable for Count III.

D. Damages

The CFAA enables a person who suffers damage or loss by reason of a violation of the statute to maintain a civil action against the violator to obtain compensatory damages. *See* 18 U.S.C. § 1030(g). In support of its request for damages for Defendant's violations of the CFAA, Plaintiff submits the Affidavit of Zachary Giegel, ECF No. 36-1, an invoice from Kivu

Consulting, ECF No. 36-3, and an invoice from Paley Rothman, ECF No. 36-4. Among its losses, Plaintiff claims:

> a. $1,952.00 for legal fees in ascertaining its notification obligation under the laws of various states of residence of affected clients;
>
> b. $7,847.50 for consulting fees to analyze and ascertain the extent of the breach;
>
> c. $2,942.00 in salaries for full-time employee who had to cease performing their usual duties to investigate and address the breach; and
>
> d. $7,200.00 in lost billable time for those same full-time employees.

ECF No. 36 at 2; *see also* ECF No. 36-1 ¶ 12; ECF No. 36-3; ECF No. 36-4 at 1. The Court finds the expenses for legal counsel, cybersecurity consulting, and employees' time are reasonably foreseeable and necessary losses associated with investigating and remedying the harm caused by Defendant's actions. *See Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010) (citing *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009)). However, it appears the final two items each account for the value of the three days' time that three employees spent investigating these issues. Allowing Plaintiff to recover the value of that time expressed both in terms of the employees' salaries and in terms of their billable time double counts this loss. Therefore, the Court will award Plaintiff $16,999.50—the summed value of the legal fees, consulting fees, and lost billable time—as damages for Defendant's violations of the CFAA.

IV. CONCLUSION

For the foregoing reasons, Plaintiff's Motion for Default Judgment, ECF No. 36, is granted against Defendant in the total amount of $16,999.50. Additionally, post-judgment interest shall accrue until the judgment is satisfied pursuant to 28 U.S.C. § 1961. A separate Order shall issue.

Date: January 28, 2021

/s/
GEORGE J. HAZEL
United States District Judge