UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

X

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Minnesota Corporation, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

X

REPORT & RECOMMENDATION

23-CV-2447 (RER) (LKE)

LARA K. ESHKENAZI, United States Magistrate Judge:

Plaintiffs Microsoft Corporation ("Microsoft"), Fortra, LLC ("Fortra"), and Health-ISAC, Inc. ("H-ISAC") brought this case against John Doe Defendants 1-16 (collectively "Defendants") for, *inter alia*, trademark infringement, violations of the Computer Fraud and Abuse Act, and violations of the Electronic Communications Privacy Act. Microsoft is "one of the world's leading technology companies" (Compl., ECF No. 1 ¶ 28), Fortra is "a technology company that manufactures, distributes and sells a variety of software products and services…" (*id.* ¶ 33), and H-ISAC is "a membership organization comprised of public and private hospitals, ambulatory providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical schools, medical R&D organizations…[that] represents

the interests of its health care and public health industry members in combating and defending against cyber threats that pose risk and loss to the industry." (*Id.* ¶ 34.) "John Doe Defendants are prolific cybercriminals who purposefully obfuscate their identities as they launch cyberattacks against domestic and foreign victims with a special focus on the health care industry." (Pls' Mem. in Supp. of Mot. for Default J., ECF No. 50-1 at 2.) The Complaint broadly alleges that Defendants hacked a program (Cobalt Strike) developed by Fortra to infect Microsoft Windows operating systems and extort money and steal data from healthcare providers who are members of H-ISAC. (*See generally* Compl.)

Before the Court is Plaintiffs' motion for default judgment and a permanent injunction against Defendants. For the reasons set forth below, the Court respectfully recommends granting Plaintiffs' motion for default judgment and converting the preliminary injunction into a permanent injunction as outlined in Microsoft's proposed order.

I. BACKGROUND

A. Factual Allegations

Defendants have defaulted, so the court "is required to accept all…factual allegations as true and draw all reasonable inferences in [Plaintiffs'] favor." *Finkel v. Romanowicz*, 577 F.3d 79, 84 (2d Cir. 2009). Cobalt Strike is a commercial security testing tool made by Plaintiff Fortra that executes targeted attacks for the purpose of testing the resilience of an organization's cyber defenses. (Compl., ECF No. 1 ¶ 35.) Legitimate users of Colbalt Strike use the application to test an organization's system for potential weaknesses to malware. (*Id.* ¶ 36.) Defendants worked together to help create a compromised version of Cobalt Strike, known as a "cracked" version, which can be used to engage in illegal activities once the malware enters an organization's system. (*Id.* ¶¶ 37, 54.) When Defendants developed cracked versions of Cobalt Strike, they reproduced

hundreds of lines of Microsoft's copyrighted code without authorization because the license agreement to use Microsoft's software development kit ("SDK")[1] explicitly prohibits the use of their code in any malicious software. (*Id.* ¶ 69.) Defendants used the internet to transmit that code and reproduce it in infected computers. (*Id.*)

Working together, Defendants distributed cracked versions of Cobalt Strike to victims' computers through various means such as exploiting victims' computers and using malicious spam email and phishing campaigns. (*Id.* ¶¶ 45, 54; *see also* Decl. of Jason Lyons ("Lyons Decl."), ECF No. 2-3 at Fig. 8.) Once a cracked version of Cobalt Strike enters a victim's machine, it effectively places the infected computer under the command of Defendants. (Declaration of Christopher Coy ("Coy Decl."), ECF No. 2-2 ¶ 17.) The cracked versions of Cobalt Strike are programmed to connect and communicate with "command and control" servers operated by Defendants, allowing the servers to upload stolen information from the infected computers. (Coy Decl. ¶¶ 26, 31.) The command and control infrastructure is composed of various "IP addresses and domains maintained on an interconnected network" that operates in many different countries. (*Id.* ¶¶ 5-6, 30.) To create the command and control servers, "Defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities." (*Id.* ¶ 32.) Microsoft and Fortra conducted thorough investigations to identify cracked versions of Cobalt Strike and the IP addresses and domains used by Defendants. (*See* Decl. of Jonathan Gross ("Gross Decl."), ECF No. 2-5; Decl. of Rodel Fiñones ("Fiñones Decl."), ECF No.

[1] Microsoft's SDK "is a package of programming tools including creative and original APIs, header files, libraries, documentation, code samples, processes, and guides that developers can use and integrate into their own applications. Microsoft's SDKs are required when developing any application, program, or tool for Microsoft Windows." (Compl. ¶ 29.) Microsoft's SDK code is copyrighted. (*Id.* ¶ 30.) Microsoft makes an SDK License available to the public so third-party developers can use it to create applications. (*Id.* ¶ 31.)

2-4; Lyons Decl.; Compl. ¶ 41, App. A.) The set of IP addresses and domains used by Defendants is constantly changing, making it challenging to dismantle the command and control infrastructure. (Coy Decl. ¶ 37.) Plaintiffs do not know the identities or specific locations of Defendants, but they have identified email addresses used by Defendants with the hosting companies and domain registrars Defendants have used to conduct their scheme. (*Id.* ¶ 5; Br. in Supp. of Plaintiffs' TRO App., ECF No. 3 at 47.)

Once infected with a cracked version of Cobalt Strike, a victim's computer will contact the command and control infrastructure via the internet, and the infrastructure will add or remove capabilities from the computer, such as removing security features, harvesting emails, and further propagating the cracked version of Cobalt Strike to other computers. (Coy Decl. ¶¶ 16-17.) Once a computer and a network are infected, Defendants are able to use the victim's computer to extort money from them, gather their personal information, and attack other computers through the victim's computer. (*Id.* ¶ 43; Compl. ¶ 72.) The cracked versions damage the computing devices of Microsoft's customers and the software installed on those devices. (Compl. ¶ 76; Coy Decl. ¶¶ 54-55.)

Based on Microsoft's investigation, over 1.5 million computers in 24 months have been infected with cracked versions of Cobalt Strike. (Coy Decl. ¶ 28.) Defendants have extorted victims, including healthcare institutions in the United States and European Union, by targeting network systems and requiring payments of millions of dollars before victims could regain access and control to their systems and data. (Compl. ¶¶ 66-67, 73.) Defendants leveraged cracked versions of Cobalt Strike to force their way into victims' machines in Brooklyn, Queens, and other areas within this district. (*Id.* ¶ 26; Coy Decl., Fig. 2.)

B. Procedural History

On March 30, 2023, Plaintiffs filed this suit and applied *ex parte* for a temporary restraining order ("TRO"). (Compl.; TRO Application, ECF Nos. 2-3.) On March 31, 2023, the Honorable Nina R. Morrison granted Plaintiffs' *ex parte* motion for a TRO. (TRO, ECF No. 13.) The TRO permitted Plaintiffs to take over control of the domains listed in Appendix A by directing the "third party Internet registries, registrars, data centers, and hosting providers with a presence in the United States to assist plaintiffs in the implementation" of the Order, without providing prior notice to Defendants. (TRO ¶¶ 11-18; Compl. App. A.) On April 6, 2023, Plaintiffs executed the TRO by working with the third-party registries and IP hosting companies and transferring the infrastructure operated by Defendants to Microsoft. (Decl. of Anna Saber dated 4/13/2023 ("Saber Decl."), ECF No. 19-2 ¶ 3.) Plaintiffs then served the Complaint, TRO and Preliminary Injunction ("PI") application, and TRO on Defendants via the emails associated with the domains in Appendix A. (*Id.* ¶ 4; Compl. App. A.) Plaintiffs also used a program called ReadNotify which tracked the email correspondence to see when it was received and viewed, if it was viewed at all. (Saber Decl. ¶ 5.) Plaintiffs received notice that the emails were delivered. (*Id.* ¶ 7.) Plaintiffs also published the relevant documents on a public website, Notice of Pleadings, and engaged in "widespread press relations and media activity announcing this action." (*Id.* ¶¶ 9,11.)

On April 19, 2023, the Honorable LaShann DeArcy Hall held a hearing and granted Plaintiffs' motion for a PI, which has substantially similar terms to the TRO. (Prelim. Inj., ECF No. 20.) The Order also permitted alternative service by email and publication on a publicly available website. (*Id.*) Subsequently, Defendants attempted to rebuild their technical infrastructure by expanding to new domains and IP addresses, so Plaintiffs filed supplemental requests for preliminary injunctions to transfer additional website domains to Microsoft. (First

Mot. to Suppl. Prelim. Inj., ECF No. 23; Second Mot. to Suppl. Prelim. Inj., ECF No. 30; Third Mot. to Suppl. Prelim. Inj., ECF No. 39.) The Court granted each of these motions. (Suppl. Prelim. Inj. Orders, ECF Nos. 24, 32, 41.) In each instance, Plaintiffs served Defendants with the relevant documents via email and publication, and Defendants never appeared or responded.

Despite Plaintiffs' best efforts to ensure that notice was reasonably calculated to reach Defendants, Defendants have not answered the Complaint of otherwise appeared before this Court. The Clerk of Court entered default (ECF No. 47), and Plaintiffs subsequently moved for entry of default judgment seeking only injunctive relief. (ECF No. 50.) The Honorable Ramón E. Reyes, Jr. referred the motion to the undersigned for a report and recommendation. (ECF Order dated 10/02/2024.)

II. DISCUSSION

A. Jurisdiction

"The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States." 28 U.S.C. § 1331. Here, Plaintiffs assert claims under various federal laws including the Lanham Act (15 U.S.C. §§ 1114, 1125(a)), the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030), and the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2701). (Compl. ¶ 1.) Given that this action arises under the laws of the United States, the Court has subject matter jurisdiction over this action. *See, e.g., Rocha v. Bakhter Afghan Halal Kababs, Inc.*, 44 F. Supp. 3d 337, 345 (E.D.N.Y. 2014).

"For a federal court to exercise personal jurisdiction over a defendant, the plaintiff's service of process upon the defendant must have been procedurally proper." *Windward Bora LLC v. Valencia*, No. 19-CV-4147 (NGG) (RER), 2020 WL 6470293, at *2 (E.D.N.Y. Oct. 16, 2020), *adopted by* 2020 WL 6450286 (E.D.N.Y. Nov. 3, 2020). "Courts are authorized to enter default

judgment even against anonymous defendants as long as service of process is reasonably calculated to give notice." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *4 (E.D.N.Y. May 28, 2021), *report and recommendation adopted*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4260665 (E.D.N.Y. Sept. 20, 2021) (internal quotation omitted) (citing Fed. R. Civ. P. 4(f)(2), (3); *Navika Capital Grp., LLC v. Doe*, No. 14-CV-5968 (DLI) (CLP), 2017 U.S. Dist. LEXIS 2926, at *11–14 (E.D.N.Y. Jan. 6, 2017), *report and recommendation adopted*, 2017 U.S. Dist. LEXIS 40820 (Mar. 20, 2017); *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017); *Microsoft Corp. v. John Does 1–39*, No. 12-CV-1335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012)).

Federal Rule of Civil Procedure 4(f)(1) permits Plaintiffs to serve Defendants pursuant to the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents (the "Hague Convention"). "However, the Hague Convention is inapplicable when 'the address of the person to be served ...is not known.'" *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (quoting Hague Conv. On the Serv. Abroad of Judicial and Extrajudicial Docs., Nov. 15, 1965, 20 U.S.T. 361) (citing *United States v. Besneli*, No. 14-CV-7339 (JFK), 2015 WL 4755533 (S.D.N.Y. Aug. 12, 2015), at *2 (noting that the Hague Convention applies to physical addresses, but not email addresses)). Federal Rule of Civil Procedure 4(f)(2) provides that when a defendant's address is unknown, plaintiffs may serve defendants "by a method that is reasonably calculated to give notice." Fed. R. Civ. P. 4(f)(2).

"[D]ue process demands only what is reasonable, not what... is impossible or impracticable." *DPWN Holdings (USA) Inc. v. United Air Lines. Inc.*, 871 F. Supp. 2d 143, 157 (E.D.N.Y. 2012). "Service by email may be appropriate 'where the [defendant] has made service by other means impossible.'" *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB)

(E.D.N.Y. Mar. 31, 2017) (quoting *Jackson v. Lowe's Companies, Inc*., No. 15-CV-4167 (ADS) (ARL), 2016 WL 6155937, at *3 (E.D.N.Y. Oct. 21, 2016)). Additionally, courts may permit service by publication "[w]here the plaintiff can show that deliberate avoidance and obstruction by the defendant have made the giving of notice impossible." *S.E.C. v. Tome*, 833 F.2d 1086,1092 (2d Cir. 1987). Service by publication may be appropriate when "the identities of individuals to be served are unknown," *Hausler v. JP Morgan Chase Bank. N.A.*, 141 F. Supp. 3d 248, 252 (S.D.N.Y. 2015) (citing *Tome*, 833 F.2d at 1094), and "particularly when the defendant is otherwise on notice that there may be a case pending against him," *S.E.C. v. HGI Inc.*, No. 99-CV-3866 (DLC), 1999 WL 1021087, at *1 (S.D.N.Y. Nov. 8, 1999) (citing *Tome*, 833 F.2d at 1093).

The Court finds that Plaintiffs' efforts to serve Defendants via email and publication were adequately designed to inform Defendants of the action against them. (*See* Saber Decl.) The Declarations of Christopher Coy, Jonathan Gross, Rodel Fiñones, Robert Erdman, and Jason Lyons outline the extensive efforts Plaintiffs undertook to identify Defendants, and they were only able to identify the email addresses associated with the domains where Defendants hosted their illicit scheme. (*See* Coy Decl.; Gross Decl.; Fiñones Decl; Decl. of Robert G. Erdman II ("Erdman Decl."), ECF No. 2-1; Lyons Decl.; Compl. App. A.) Despite emailing Defendants the documents in this case and publishing them online, Defendants ignored this lawsuit. Indeed, Defendants appear to have intentionally ignored this lawsuit based on Plaintiffs' ability to track the receipt of their service through ReadNotify. (Saber Decl. ¶¶ 5-7.) Accordingly, the Court concludes that service was properly effectuated by email and publication.

B. Liability

1. Default Judgment Standard

Under Rule 55 of the Federal Rules of Civil Procedure, there are two steps to entering a default judgment. *See Enron Oil Corp. v. Diakuhara*, 10 F.3d 90, 95-96 (2d Cir. 1993). First, the Clerk of Court enters the default pursuant to Rule 55(a) by notation of the party's default on the Clerk's record of the case. Fed R. Civ. P. 55(a) (providing that "[w]hen 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."). This first step is nondiscretionary. *See United States v. Conolly*, 694 F. App'x 10, 12 (2d Cir. 2017). Second, after the Clerk of the Court enters a defendant's default, the court may enter a default judgment. *See* Fed R. Civ. P. 55(b).

Here, on August 22, 2024, the Clerk of the Court entered default against Defendants after Defendants failed to respond to the Complaint or otherwise appear in this action. (ECF No. 47.) To date, Defendants have not appeared or moved to vacate the entry of default.

Whether or not a default judgment is issued is within the discretion of the court. When evaluating a plaintiff's application for a default judgment, "a court is required to accept all [ ] factual allegations as true and draw all reasonable inferences in [plaintiff's] favor." *Finkel v. Romanowicz*, 577 F.3d 79, 84 (2d Cir. 2009). "Nevertheless, it remains for the court to consider whether the unchallenged facts constitute a legitimate cause of action, since a party in default does not admit conclusions of law." *Labarbera v. ASTC Labs., Inc.*, 752 F. Supp. 2d 263, 270 (E.D.N.Y. 2010) (internal quotations and citations omitted); *see also TAGC Mgmt., LLC v. Lehman, Lee & Xu Ltd.*, 536 F. App'x 45, 46 (2d Cir. 2013) ("[P]rior to entering default judgment, a district court

is required to determine whether the plaintiff's allegations establish the defendant's liability as a matter of law.") (internal quotations and citations omitted).

"Default judgments are generally disfavored and are reserved for rare occasions." *City of New York v. Mickalis Pawn Shop, LLC*, 645 F.3d 114, 129 (2d Cir. 2011) (quoting *Enron Oil Corp.*, 10 F.3d at 96) (internal quotation marks omitted). While the Second Circuit has recognized the "push on a trial court to dispose of cases that, in disregard of the rules, are not processed expeditiously [and] ... delay and clog its calendar," it has held that a district court must balance that interest with its responsibility to "afford litigants a reasonable chance to be heard." *Enron Oil Corp.*, 10 F.3d at 95-96. Thus, considering the "oft-stated preference for resolving disputes on the merits," doubts should be resolved in favor of the defaulting party. *See id.* Accordingly, a plaintiff is not entitled to a default judgment as a matter of right simply because defendants are in default. *See Erwin DeMarino Trucking Co. v. Jackson*, 838 F. Supp. 160, 162 (S.D.N.Y. 1993) (noting that courts must "supervise default judgments with extreme care to avoid miscarriages of justice").

Once the Clerk of the Court enters a certificate of default, a defendant is deemed to have admitted the well-pled allegations in the complaint pertaining to liability. *See Greyhound Exhibitgroup, Inc. v. E.L.U.L. Realty Corp.*, 973 F.2d 155, 158 (2d Cir. 1992); *Montcalm Publ'g. Corp. v. Ryan*, 807 F. Supp. 975, 977 (S.D.N.Y. 1992) (citations omitted). A fact is not considered well-pled, however, "if it is inconsistent with [the] other allegations of the complaint or with facts of which the court can take judicial notice, or is contrary to uncontroverted material in the file of the case." *Hop Hing Produces Inc. v. Lin Zhang Trading Co., Inc.*, No. 11-CV-3259 (NGG) (RLM), 2013 WL 3990761, at *3 (E.D.N.Y. Aug. 5, 2013) (citations and internal quotation marks omitted). Ultimately, whether to grant a motion for default judgment is "left to the [court's] sound discretion." *Shah v. New York State Dep't of Civ. Serv.*, 168 F.3d 610, 615 (2d Cir. 1999) (quoting

Enron Oil Corp., 10 F.3d at 95); *Div. 1181 Amalgamated Transit Union-New York Emps. Pension Fund v. D & A Bus Co.*, 270 F. Supp. 3d 593, 606 (E.D.N.Y. 2017).

"In determining whether to enter a default judgment, the Court is guided by the same factors that apply to a motion to set aside entry of a default." *Double Green Produce, Inc. v. Forum Supermarket Inc.*, No. 18-CV-2660 (MKB) (SJB), 2019 WL 1387538, at *2 (E.D.N.Y. Jan. 29, 2019) (citing *Enron Oil Corp.*, 10 F.3d at 96; *Pecarsky v. Galaxiworld.com Ltd.*, 249 F.3d 167, 170-71 (2d Cir. 2001)). "These factors are 1) whether the defendant's default was willful; 2) whether the defendant has a meritorious defense to plaintiff's claims; and 3) the level of prejudice the non-defaulting party would suffer as a result of the denial of the motion for default judgment." *Double Green Produce*, 2019 WL 1387538, at *2 (quoting *Mason Tenders Dist. Council v. Duce Constr. Corp.*, No. 02-CV-9044 (LTS) (GWG), 2003 WL 1960584, at *2 (S.D.N.Y. Apr. 25, 2003)) (internal quotation marks omitted).

As to the first factor, "a defendant's nonappearance and failure to respond sufficiently demonstrates willfulness." *Luna v. Gon Way Constr., Inc.*, No. 16-CV-1411 (ARR) (VMS), 2017 WL 835321, at *4 (E.D.N.Y. Feb. 14, 2017), *report and recommendation adopted*, 2017 WL 835174 (E.D.N.Y. Mar. 2, 2017) (collecting cases). Here, Defendants did not respond to the Complaint, TRO, or multiple versions of the PI, despite proper service of each. Accordingly, Defendants' failure to respond to the Complaint or the instant motion demonstrates that Defendants' default is willful.

As to the second factor, Defendants' failure to appear in this action has left the Court unable to assess whether they have a meritorious defense. "Where a defendant fails to answer the complaint, courts are unable to make a determination whether the defendant has a meritorious

defense to the plaintiff's allegations[.]" *See Joseph v. HDMJ Rest., Inc.*, 970 F. Supp. 2d 131, 143 (E.D.N.Y. 2013). Therefore, this factor weighs in favor of granting a default judgment.

With respect to the third factor, Plaintiffs will be prejudiced if the motion for default judgment is denied because they have "no alternative legal redress." *United States v. Myers*, 236 F. Supp. 3d 702, 709 (E.D.N.Y. 2017). Accordingly, the Court recommends finding that Defendants' failure to answer or otherwise respond to the Complaint constitutes an admission of the factual allegations therein.

2. Lanham Act Claims

Plaintiffs bring claims under the Lanham Act for both Trademark Infringement for Defendants' creation of unauthorized copies of Plaintiffs' trademarks and False Designation of Origin for Defendants' unauthorized use of Plaintiffs' trademarks which was likely to cause confusion, mistake, or deception. (Compl. ¶¶ 1, 113, 119.) "Claims for false designation of origin and trademark infringement 'are both governed by the same legal standard.'" *Juul Labs, Inc. v. EZ Deli Grocery Corp I*, No. 21-CV-2615 (MKB) (VMS), 2022 WL 1085406, at *5 (E.D.N.Y. Feb. 10, 2022), *report and recommendation adopted*, No. 21-CV-2615 (MKB) (VMS), 2022 WL 819152 (E.D.N.Y. Mar. 18, 2022) (quoting *Am. Auto. Ass'n, Inc. v. Limage*, No. 15-CV-7386 (NGG) (MDG), 2016 WL 4508337, at *2 (E.D.N.Y. Aug. 26, 2016)). "To state a claim for either cause of action, Plaintiffs 'need only show that they own a valid trademark and that the defendants' use of the trademark is likely to cause confusion regarding the source of the product.'" *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *5 (quoting *Microsoft Corp. v. Atek 3000 Computer Inc.*, No. 06-CV-6403 (SLT) (SMG), 2008 WL 2884761, at *2 (E.D.N.Y. July 23, 2008)). To determine whether a defendant's use of a trademark will likely cause confusion, the Second Circuit has established an eight-factor balancing test:

> (1) strength of the trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user[2] may "bridge the gap" by developing a product for sale in the market of the alleged infringer's product; (5) evidence of actual consumer confusion; (6) evidence that the imitative mark was adopted in bad faith; (7) respective quality of the products; and (8) sophistication of consumers in the relevant market.

Starbucks Corp. v. Wolfe's Borough Coffee, Inc., 588 F.3d 97, 115 (2d Cir. 2009) (citing *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492 (2d Cir. 1961)). No factor is dispositive, and courts evaluate the totality of the circumstances. *Limage*, 2016 WL 4508337, at *3. "However, in cases involving the use of counterfeit marks, 'the Court need not undertake a factor-by-factor analysis under *Polaroid* because counterfeits, by their very nature, cause confusion.'" *Mitchell Grp. USA LLC v. Udeh*, No. 14-CV-5745 (AMD) (JO), 2017 WL 9487193, at *3 (E.D.N.Y. Mar. 8, 2017), *report and recommendation adopted*, No. 14-CV-5745 (AMD) (JO), 2017 WL 3208532 (E.D.N.Y. July 28, 2017) (quoting *Phillip Morris USA Inc. v. Marlboro Express*, No. 03-CV-1161 (CPS), 2005 WL 2076921, at *4 (E.D.N.Y. Aug. 26, 2005)).

Microsoft has registered trademarks for Microsoft and Windows, and it attached copies of the federal registrations to the Complaint. (Compl. ¶ 28, App. B ("Microsoft Trademarks").) Plaintiff Fortra has registered a trademark for Cobalt Strike, and it attached a copy of the federal registration to the Complaint. (Compl. ¶ 33, App. E ("Cobalt Strike Trademark").) This sufficiently establishes Microsoft's and Fortra's valid ownership of the subject trademarks. *See Atek 3000*

[2] "Cases analyzing Lanham Act claims refer to 'senior' and 'junior' users of a subject mark." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *5 n.3. Here, the senior user refers to Microsoft's use of the Microsoft and/or Windows marks with devices operating on unadulterated Windows operating systems. The junior users refer to Defendants' use of computer devices running on a corrupted operating system due to being infected by a cracked version of Cobalt Strike, but the devices still bear the Microsoft and/or Windows marks. *See id.* The same definitions of senior and junior users apply to Plaintiff Fortra with its use of Cobalt Strike (senior user) and Defendants' use of cracked versions of Cobalt Strike (junior users).

Computer Inc., 2008 WL 2884761, at *2 n.2 (citing *Island Software & Comput. Serv., Inc. v. Microsoft Corp.*, 413 F.3d 257, 260 (2d Cir. 2005)).

As to whether Defendants' use of subject marks is likely to cause confusion, each factor weighs in favor of Plaintiffs. The Court will briefly address each factor.

First, the marks "are presumed to be strong by virtue of being registered." *Juul Labs, Inc.*, 2022 WL 1085406, at *5 (citing *Doctor's Assocs. LLC v. Hai*, No. 19-CV-1968 (NGG) (RER), 2019 WL 3330242, at *4 (E.D.N.Y. May 13, 2019), *report and recommendation adopted as modified*, No. 19-CV-1968 (NGG) (RER), 2019 WL 2385597 (E.D.N.Y. June 6, 2019)). As discussed *supra*, Microsoft has registered trademarks for Microsoft and Windows (Compl. ¶ 28, Microsoft Trademarks), and Fortra has registered a trademark for Cobalt Strike. (Compl. ¶ 33, Cobalt Strike Trademark.) "Microsoft is one of the world's leading technology companies" and it provides "the Windows operating system [and] Microsoft Word." (Compl. ¶ 28.) It "has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols…" (*Id.*; Coy Decl. ¶ 60.) Fortra "is a well-known cybersecurity software development company that is trusted by government, industry and the security community at large." (Erdman Decl. ¶ 5.) "The Cobalt Strike software contains technical protections that require a valid, time limited license and a valid authorization ID or 'watermark", [and] [a]ll downloads and updates of the Cobalt Strike product code are validated against the licensing and watermark requirements before access can proceed." (*Id.* ¶ 6.) Therefore, Plaintiffs have demonstrated the strength of their marks. *See Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *5.

Second, "the conduct [Plaintiffs] allege[] involves marks that are not only similar, but identical." (*Id.*) The entire premise of Defendants' scheme is to create cracked versions of Cobalt

Strike and infect Windows operating systems in an undetectable way so that they can be exploited. (*See* Coy Decl. ¶¶ 24, 47 ("The compromised Windows operating system does not appear any different to the user of the infected computer."); Compl. ¶¶ 26, 113, 119, 156.)

Third, the cracked versions of Cobalt Strike and corrupted Windows operating systems not only compete with each other, but the corrupted versions are meant to hide in the victim's computer without the victim's knowledge. (Compl. ¶ 72 ("Defendants can use the victim's computer to send commands and … control it surreptitiously…); *see also* Gross Decl. ¶ 14 ("[T]he only difference between sanctioned use of legitimate Cobalt Strike and malicious use of cracked Cobalt Strike is the authority or permission granted to the operator by the client. They otherwise function exactly the same way.").) The Fourth factor, whether Plaintiffs can "bridge the gap," meaning "enter a market related to that in which the defendant[s] sell[] [their] products" (*Juul Labs, Inc.*, 2022 WL 1085406, at *5), is irrelevant here given that Defendants have created counterfeit versions of Plaintiffs' marks and consumers are not purchasing them in any marketplace.

Fifth, although Plaintiffs have not presented evidence of actual confusion, they have asserted that millions of computers have been infected with counterfeit versions of Plaintiffs' marks due to Defendants' activities. (Compl. ¶ 69); *see also Guthrie Healthcare Sys. v. ContextMedia, Inc*., 826 F.3d 27, 45 (2d Cir. 2016) ("[I]t is black letter law that actual confusion need not be shown to prevail under the Lanham Act, since actual confusion is very difficult to prove and the Act requires only a likelihood of confusion as to source.") (internal quotation omitted). Plaintiffs assert that "misuse of cracked versions [of Cobalt Strike] causes irreparable harm, where customers and potential customers mistakenly believe that it is Fortra's legitimate product offering that is responsible for these ransomware and malware attacks." (Erdman Decl. ¶ 38.) They further assert that "Cobalt Strike being referred to repeatedly [in news articles] as a

favorite tool amongst cybercriminals does not engender trust of Cobalt Strike and the Cobalt Strike brand because individuals may not be able to distinguish between nefarious use of cracked Cobalt Strike by criminals and legitimate uses." (*Id.*; Erdman Decl. Exs. 2-9 ("Articles").) Moreover, cracked versions of Cobalt Strike compromise the Window's operating system "to ensure that the malware is launched automatically every time the computing device is started." (Coy Decl. ¶ 46.) In effect, the "compromised Windows operating system does not appear any different to the user of the infected computer…thus, [the user] thinks the compromised operating system is developed and distributed by Microsoft, despite the fact that it is the operators of the malware that are compromising the operating system." (*Id.* ¶ 47.) These allegations are more than sufficient to establish legitimate concerns about confusion.

Sixth, there is no question Defendants' imitative mark was adopted in bad faith. *See Star Indus., Inc. v. Bacardi & Co.*, 412 F.3d 373, 388 (2d Cir. 2005) ("Bad faith generally refers to an attempt by a junior user of a mark to exploit the good will and reputation of a senior user by adopting the mark with the intent to sow confusion between the two companies' products.") As discussed *supra*, the premise of Defendants' scheme is to create cracked versions of Cobalt Strike and infect Windows operating systems in an undetectable way so that they can be exploited. (*See* Coy Decl. ¶¶ 24, 47 ("The compromised Windows operating system does not appear any different to the user of the infected computer."); Compl. ¶¶ 26, 113, 119, 156.) "Seventh, and similarly, the respective quality of the products could not be more different." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *6.

Finally, it is beyond dispute that the general public regularly interacts with Microsoft and Windows operating systems. (*Id.*) The Complaint alleges that the cracked versions of Cobalt Strike are used by Defendants "to compromise countless end user computers of the type commonly found

in businesses, living rooms, schools, libraries, and Internet cafes." (Compl. ¶ 45.) At least 1.5 million computers were infected with the cracked versions of Cobalt Strike. (Coy. Decl. ¶¶ 28, 53 ("The cracked versions of Cobalt Strike are used by Defendants to infect and run on computer devices equipped with the Windows operating system.").) Given that victims don't know that their computers are infected and so many computers have been effected, this factor weighs in favor of Plaintiffs.

Accordingly, Plaintiffs have established Defendants' liability for trademark infringement and false designation of origin under the Lanham Act.

3. Computer Fraud and Abuse Act Claim

"The CFAA imposes liability on anyone who 'intentionally accesses a computer without authorization ... and thereby obtains information from any protected computer.'" *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (quoting 18 U.S.C. § 1030(a)(2)(C)). A protected computer is any computer with Internet access. *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). "Plaintiff[s] must show that Defendants (1) accessed a computer; (2) did so without authorization; (3) obtained information from a protected computer; and (4) caused an aggregate loss of at least $5,000 during any one-year period." *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017); *see also JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 520-21 (S.D.N.Y. 2013).

Plaintiffs have sufficiently stated a valid claim under the CFAA. The first three elements are plainly satisfied. Defendants infected "protected computers" with cracked versions of Cobalt Strike via the Internet because they used malicious spam email and phishing to infect the computers. (Compl. ¶¶ 45, 54; Lyons Decl., Fig. 8.) Second, Defendants' access was unauthorized because it was designed to infect computers without the users' knowledge or consent. (Compl. ¶

77); *see also Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811 (LO) (IDD), 2015 U.S. Dist. LEXIS 110145, at *19 (E.D. Va. July 20, 2015) (collecting cases), *report and recommendation adopted* by 2015 U.S. Dist. LEXIS 109729 (Aug. 17, 2015) ("The CFAA was designed to prohibit the type of unauthorized access and fraudulent conduct facilitated by malware and botnet activity.")

Finally, Plaintiffs have alleged a loss well in excess of $5,000 due to Defendants' CFAA violations. Plaintiff Fortra alleges it "has expended over a million…dollars on" combatting the cracked versions of Cobalt Strike. (Erdman Decl. ¶ 40.) Plaintiffs Microsoft and H-ISAC also allege Defendants' conduct has caused a loss to each of them of at least $5,000. (Compl. ¶¶ 100-01.) Plaintiffs describe in detail the significant resources expended in conducting thorough investigations to identify cracked versions of Cobalt Strike and the IP addresses and domains used by Defendants. (*See* Gross Decl.; Fiñones Decl.; Lyons Decl.; Compl. ¶ 41, App. A.) Accordingly, Plaintiffs have demonstrated a claim against Defendants under the CFAA. *See Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (granting Microsoft's motion for default judgment and permanent injunction under only the CFAA in substantially similar case); *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *7-8 (granting Microsoft's motion for default judgment and permanent injunction pursuant to the CFAA, Lanham Act, and ECPA in substantially similar case).

4. Electronic Communications Privacy Act

The ECPA is violated when a defendant "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility and thereby obtains access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The ECPA

provides a civil cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter." *Id.* at § 2707(a). Microsoft alleges that "Defendants … intentionally accessed the Windows operating system and Health-ISAC's members' healthcare network infrastructure… without authorization…[and] intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users and Health-ISAC's members and their users." (Mem. in Supp. at 15.) "This is precisely the behavior that the ECPA aims to prevent." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *8 (collecting cases). Accordingly, Plaintiffs have established a claim against Defendants under the ECPA.

5. Remaining Claims

Plaintiffs additionally bring claims for (1) Circumvention of Copyright Protection Systems under the Digital Millennium Copyright Act, 17 U.S.C. § 1201; (2) Copyright Infringement, 17 U.S.C. §§ 101 et seq.; (3) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (4) Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962, (5) Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d); (6) Trespass to Chattels; (7) Conversion; and (8) Unjust Enrichment. (Compl. ¶ 1.) Because the Court recommends granting Plaintiffs' motion for default judgment as to the claims discussed *supra*, it is unnecessary to reach the remaining claims as "[t]he scope of appropriate injunctive relief would not vary based on the merits of Plaintiff's remaining federal and state-law claims." *Limage*, 2016 WL 4508337, at *2 (citing *Pretty Girl, Inc. v. Pretty Girl Fashions, Inc.*, 778 F. Supp. 2d 261, 269 (E.D.N.Y. 2011)). The Court therefore recommends dismissing Plaintiffs' remaining claims

without prejudice as moot. *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *8.

C. Injunctive Relief

Plaintiffs seek a permanent injunction "(1) prohibiting…Defendants from operating or propagating the Cracked Cobalt Strike botnet, (2) preventing registration of malicious domains identified in the Court's preliminary injunction order and subsequent supplemental preliminary injunction orders, and (3) preventing the malicious use of other Internet infrastructure, such as IP addresses identified in the Court's preliminary injunction order and subsequent supplemental preliminary injunction orders." (Mem. in Supp. at 1.) "A plaintiff seeking a permanent injunction on a motion for a default judgment must show that they are entitled to injunctive relief under the applicable statutes and that they meet the prerequisites for issuance of an injunction." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *9 (citing *Brydge Techs. LLC v. Ogadget LLC*, No. 19-CV-5692 (EK) (CLP), 2021 WL 1200316, at *5 (E.D.N.Y. Mar. 4, 2021)). A Plaintiff seeking a permanent injunction must demonstrate:

> (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

Each of the federal statutes discussed *supra*—the Lanham Act, CFAA, and ECPA—provides for injunctive relief. *See Streamlight, Inc. v. Gindi*, No. 18-CV-987 (NG) (RLM), 2019 WL 6733022, at *8 (E.D.N.Y. Oct. 1, 2019), *report and recommendation adopted*, No. 18-CV-987 (NG) (RLM), 2019 WL 6726152 (E.D.N.Y. Dec. 11, 2019) (citing 15 U.S.C. § 1116(a)) (Under the Lanham Act, "courts enjoy broad discretion in determining whether to grant a

permanent injunction or similar equitable relief for trademark infringement."); 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."); 18 U.S.C. § 2702(b) ("In a civil action under this section, appropriate relief includes . . . such preliminary and other equitable or declaratory relief as may be appropriate. . ."). Accordingly, the Court respectfully recommends converting the terms of the preliminary injunction into a permanent injunction, as outlined in Plaintiffs' proposed order.

1. Irreparable Harm

"In trademark infringement cases under the Lanham Act, a party may show irreparable injury by demonstrating a likelihood of confusion." *Streamlight, Inc.*, 2019 WL 6733022, at *8. "In counterfeit cases, such as this one, counterfeit products, 'by their very nature, cause confusion.'" *Id.* (quoting *Gucci Am., Inc. v. Duty Free Apparel, Ltd.*, 286 F. Supp. 2d 284, 287 (S.D.N.Y. 2003)). As discussed *supra*, the cracked versions of Cobalt Strike that infect Windows systems without the users' knowledge or consent inherently cause a likelihood of confusion. (*See* Erdman Decl. ¶ 38 ("…misuse of cracked versions [of Cobalt Strike] causes irreparable harm, where customers and potential customers mistakenly believe that it is Fortra's legitimate product offering that is responsible for these ransomware and malware attacks."); Coy Decl. ¶ 53 ("Defendants' activities using the cracked versions of Cobalt Strike harm Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems.").) Microsoft further alleges that "Defendants irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill…[by] physically alter[ing] and corrupt[ing] Microsoft products." (Coy Decl. ¶ 58.) Further, H-ISAC argues that "[c]racked versions of Cobalt Strike harm the brand

reputation of Health-ISAC's member organizations" because "Defendants… utilize…ransomware to intrude and arrest the operational status of Health-ISAC member organizations' computers and networks." (Decl. of Errol Weiss ("Weiss Decl."), ECF No. 2-6 ¶ 10.) These intrusions thus cause "injury to their brands, by calling into question the safety and security of patient data and the healthcare network system as a whole." (*Id.*)

Without a permanent injunction, Defendants would regain access to the IP addresses and domains that they have used to infect over a million computers already and continue to harm Plaintiffs and their customers. *See Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518 at *9.

2. Inadequacy of Remedies at Law

"Where, as here, there are no assurances 'against a defendant's continued infringing activity, a remedy at law may be deemed insufficient to compensate a plaintiff for [its] injuries.'" *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (quoting *Stark Carpet Corp. v. Stark Carpet & Flooring Installations, Corp.*, 954 F. Supp. 2d 145, 158 (E.D.N.Y. 2013) (collecting cases)). "Because the losses of reputation and goodwill and resulting loss of customers are not precisely quantifiable, remedies at law cannot adequately compensate Plaintiff for its injuries." *U.S. Polo Ass'n, Inc. v. PRL USA Holdings, Inc.*, 800 F. Supp. 2d 515, 541 (S.D.N.Y. 2011), *aff'd*, 511 F. App'x 81 (2d Cir. 2013). Moreover, Defendants have shown that they would not be easily deterred from continuing their activities. Defendants attempted to rebuild their technical infrastructure after the Court issued the first preliminary injunction in this case by using new IP addresses and domains to host the command and control infrastructure, requiring Plaintiffs to file supplemental requests for preliminary injunctions to transfer the new additional website domains to Microsoft. (First Mot. to Suppl. Prelim. Inj., ECF

No. 23; Second Mot. to Suppl. Prelim. Inj., ECF No. 30; Third Mot. to Suppl. Prelim. Inj., ECF No. 39.) Given that Defendants attempted to circumvent the first preliminary injunction, causing the Court to supplement it multiple times, this factor weighs in favor of granting a permanent injunction.

3. Balance of Hardships

The balance of hardships weighs in favor of granting an injunction. Plaintiffs provide services that are widely used and depended upon by millions of people, while Defendants engage in nefarious acts to exploit victims. Defendants' activities directly harm Plaintiffs and the general public. The only hardship to Defendants is that they will not be able to further perpetuate their activities through the IP addresses and domains identified by Plaintiffs. *N. Atl. Operating Co., Inc. v. Evergreen Distribs. LLC*, No. 13-CV-4974 (ERK) (VMS), 2013 WL 5603810, at *5 (E.D.N.Y. Sept. 30, 2013) ("Where the only hardship to Defendant from an injunction would be to prevent him from engaging in further illegal activity, the balance clearly weighs in Plaintiffs' favor.") (internal citation and quotations omitted).

4. Public Interest

"The consuming public has a protectable interest in being free from confusion, deception and mistake." *Polo*, 800 F. Supp. at 541 (citing *NYC Triathlon, LLC v. NYC Triathlon Club, Inc.*, 704 F. Supp. 2d 305, 344 (S.D.N.Y. 2010)). Cracked versions of Cobalt Strike are used to infect Windows systems "in businesses, living rooms, schools, libraries, and Internet cafes" (Compl. ¶ 45), and exploit those machines to steal money and personal information from their users. The public interest would be served by a permanent injunction.

5. Third Parties

"The statutes at issue do not expressly authorize the Court to order a third-party to transfer domain ownership." *Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *11 (citing *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017)). The All Writs Act ("AWA"), however, provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). "That includes the power to 'issue such commands . . . as may be necessary or appropriate to effectuate and to prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'" *In re Stabile*, 436 F. Supp. 2d 406, 413 (E.D.N.Y. 2006) (quoting *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 40 (1985)). "'The Act's grant of authority is plainly broad and, on its face, makes no distinctions between parties and nonparties.'" *Id.* at 414 (quoting *United States v. Int'l Bhd. of Teamsters*, 266 F.3d 45, 49–50 (2d Cir. 2001)).

Plaintiffs argue that "[t]o execute the requested relief, cooperation from third parties may be required" because Plaintiffs need the third-party hosting providers where Defendants' IP addresses are hosted and the third-party domain registries to cooperate in effectuating the proposed permanent injunction order. (Mem. in Supp. at 27.) Plaintiffs want the IP addresses and domain listed in Appendix A to the Proposed Order "be disabled and/or transferred to Plaintiffs' control, in order to mitigate the risk and injury caused by Defendants," and the third parties are "the only entities that can effectively disable Defendants' malicious software at the IP addresses [and] disable Defendants' domains and preserve the evidence." (*Id.*; Proposed Order Granting Permanent Injunction ("Proposed Order"), ECF No. 50-2, App. A.) Plaintiffs' requested relief amounts to leaving in place the current preliminary injunction and is limited to the domain registries identified in the PI and supplemental preliminary injunction orders. (Mem. in Supp. at

1; Prelim. Inj.; Suppl. Prelim. Inj. Orders; Proposed Order.) Courts in this district have entered substantially similar permanent injunctions to the one Plaintiffs are requesting. *See Microsoft Corp. v. Does 1-2*, No. 20-CV-1217 (LDH) (RER), 2021 WL 4755518, at *11 (ordering injunctive relief involving domain registries pursuant to the AWA); *Microsoft Corp. v. John Does 1–39*, No. 12-CV-1335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012) (same). Accordingly, the Court respectfully recommends granting Plaintiffs' request relief as to the identified third parties.

III. CONCLUSION

For the foregoing reasons, the Court respectfully recommends (1) granting Plaintiffs' motion for default judgment, and (2) converting the terms of the preliminary injunction and supplemental preliminary injunctions into a permanent injunction—as outlined in Plaintiffs' proposed order—thereby enjoining Defendants, their representatives and persons who are in active concert or participation with them, from engaging in any of the activity complained of in this action, or causing any of the injuries complained of in this action.

Plaintiffs' counsel is hereby directed to serve copies of this Report and Recommendation upon Defendants by email and publication and to file proof of service with the Clerk of the Court by August 12, 2025. Any objections to this Report and Recommendation must be filed with the Clerk of the Court and the Honorable Ramón E. Reyes, Jr. within 14 days of service. 28 U.S.C. § 636(b)(1)(C); Fed. R. Civ. P. 72(b). Any requests for an extension of time to file objections shall be directed to Judge Reyes. If a party fails to object timely to this Report and Recommendation, it

waives any right to further judicial review of this decision. *See Miller v. Brightstar Asia, Ltd.*, 43 F.4th 112, 120 (2d Cir. 2022).

SO ORDERED.

Dated: Brooklyn, New York
August 6, 2025

Lara K. Eshkenazi
LARA K. ESHKENAZI
United States Magistrate Judge