UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

EXECUTIVE TRIM CONSTRUCTION, INC., ***doing business as*** **Executive Group,**

Plaintiff,

vs. **1:20-cv-544 (MAD/DJS)**

CHRISTOPHER GROSS; SUDDATH VAN LINES, INC., ***a Florida Corporation*****; and SUDDATH VAN LINES, INC.,** ***doing business as*** **Suddath Workplace Solutions,**

Defendants.

APPEARANCES: **OF COUNSEL:**

ROEMER WALLENS GOLD & MINEAUX, LLP **MATTHEW J. KELLY, ESQ.**
13 Columbia Circle
Albany, New York 12203
Attorneys for Plaintiff

SCOLARO, FETTER LAW FIRM **CHAIM JAFFE, ESQ.**
507 Plum Street
Suite 300
Syracuse, New York 13204
Attorneys for Defendant Christopher Gross

GEORGE W. WRIGHT & ASSOCIATES, LLC **GEORGE W. WRIGHT, ESQ.**
505 Main Street
Suite 106
Hackensack, New Jersey 07601
Attorneys for Defendant Suddath Van Lines, Inc.

Mae A. D'Agostino, U.S. District Judge:

MEMORANDUM-DECISION AND ORDER

I. INTRODUCTION

Plaintiff Executive Trim Construction, Inc. ("Executive") commenced this action on May 14, 2020, and filed a motion for temporary restraining order and preliminary injunction that same

day. *See* Dkt. Nos. 1 & 2. On May 15, 2020, the Court granted Plaintiff's motion for a temporary restraining order and directing expedited briefing on the pending motion for preliminary injunctive relief. *See* Dkt. No. 8. After granting several requests by the parties for extensions of time, the Court held a hearing on the request for injunctive relief on August 11, 2020.

Currently before the Court are the following motions: (1) Plaintiff's motion for a preliminary injunction; (2) Defendant Gross' motion asking the Court to reject the affidavit of Philip Beckett; and (3) Defendant Gross' motion to preclude Plaintiff's use of certain evidence. *See* Dkt. Nos. 2, 42, 43.

II. BACKGROUND

Plaintiff is a domestic corporation duly licensed to do business in the State of New York, with its principal place of business in Gloversville, New York. *See* Dkt. No. 1 at ¶ 2. Defendant Christopher Gross was a resident of Wilton, Connecticut and formerly employed by Plaintiff. *See id.* at ¶ 4. Defendant Suddath Van Lines, Inc. ("Suddath") is a foreign corporation doing business within the State of New York, with a principal place of business in Jacksonville, Florida. *See id.* at ¶ 5.

Defendant Gross was hired by Plaintiff in April 2018 and was hired to provide sales work within the greater New York area. *See id.* at ¶ 7. Plaintiff is engaged in the business of selling, warehousing, freight, and installation services of furniture, fixtures and equipment to the hospitality industry and others in the eastern United States. *See id.* at ¶ 9. The business is regularly conducted by a bid process which requires consideration and evaluation of specific requests in a bid proposal. *See id.* Plaintiff claims that "[c]alculation of a bid in response requires an understanding of the specific worksite and the available labor force to complete the project. These calculations have been developed by Executive Group after years of first-hand experience

and constitute trade secrets." *Id.* Further, Plaintiff claims that "[t]his information would not be known to people outside the business and is limited to specific individuals who calculate the bid amounts. It is guarded against disclosure to anyone else. The information is the coin of the realm in the business and has been developed over years of first-hand experience." *Id.*

On April 30, 2020, Defendant Gross left his employment with Plaintiff. *See id.* at ¶ 10. In the complaint, Plaintiff contends that, unbeknownst to it, Defendant Gross "engaged in a scheme to defraud, and did engage in unfair competition and breach his duty of loyalty to plaintiff, all meant to harm the business of the plaintiff hereto and enhance [his] position as a future employee of the defendant, Suddath Van Lines, Inc. d/b/a Suddath Workplace Solutions, by transmitting and delivering bid calculations and amounts on several current matters to Suddath's employee." *Id.* at ¶ 11. Further, Plaintiff claims that Defendant Gross engaged in slander *per se* both during and subsequent to his employment with Plaintiff, "by contending that the plaintiff's business operations were not stable and inferred plaintiff was not likely to remain as an ongoing entity." *Id.* at ¶ 12. Plaintiff alleges that Defendant Gross "did tell other people, both within and without the industry that plaintiff's business was failing and that it was unlikely to be able to continue in business." *Id.* at ¶ 13. Plaintiff claims that Defendant Gross's conduct harmed its reputation and damaged its business. *See id.* at ¶ 14.

In its complaint dated May 14, 2020, Plaintiff asserts the following causes of action:

> (1) First Cause of Action against Defendant Christopher Gross for breach of duty of loyalty to Plaintiff;
>
> (2) Second Cause of Action against Defendants Gross and Suddath Van Lines, Inc. for diversion of corporate opportunities;
>
> (3) Third Cause of Action against Defendant Gross for slander *per se*;

> (4) Fourth Cause of Action against Defendants Gross and Suddath for tortious interference with Plaintiff's prospective business relationships with its customers;
>
> (5) Fifth Cause of Action against Defendant Gross for breach of fiduciary duty to Plaintiff;
>
> (6) Sixth Cause of Action against Defendants Gross and Suddath for unfair competition;
>
> (7) Seventh Cause of Action against Defendants Gross and Suddath for "hacking" of Plaintiff's computers pursuant to 18 U.S.C. § 1030; and
>
> (8) Eighth Cause of Action against Defendants Gross and Suddath for misappropriation of trade secrets pursuant to 18 U.S.C. §§ 1832-1836.

Dkt. No. 1. That same day, Plaintiff filed a motion for a temporary restraining order, which the Court granted on May 15, 2020. *See* Dkt. No. 8.

III. DISCUSSION

A. Preclusion of Personal Emails

In a letter motion dated July 20, 2020, Defendant Gross argues that the Court preclude Plaintiff from relying on emails it obtained from Defendant Gross' personal email account. *See* Dkt. No. 43 at 1. Defendant Gross contends that these emails were obtained unlawfully in violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* *See id.* In these emails, Defendant Gross sent to Suddath bids that he had prepared on behalf of Executive Group for various jobs, which included the total price for all services to be performed. In response, Plaintiff contends that the case relied upon by Defendant Gross is distinguishable because it had a clear policy in place that it was permitted to access both business and personal email accounts, when the personal email account is accessed through a company computer. *See* Dkt. No. 46 at 2-3.

Plaintiff's Employee Handbook provides as follows:

> All content maintained in Company IT resources and communications systems are the property of the Company. Therefore, employees should have no expectation of privacy in any message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on Company electronic information and communications systems.
>
> The Company reserves the right to monitor, intercept, and/or review all data transmitted, received, or downloaded over Company IT resources and communications systems in accordance with applicable law. Any individual who is given access to the system is hereby given notice that the Company will exercise this right periodically, without prior notice and without prior consent.
>
> The interests of the Company in monitoring and intercepting data include, but are not limited to: protection of Company trade secrets, proprietary information, and similar confidential commercially-sensitive information (i.e. financial or sales records/reports, marketing or business strategies/plans, product development, customer lists, patents, trademarks, etc.); managing the use of the computer system; and/or assisting employees in the management of electronic data during periods of absence.
>
> You should not interpret the use of password protection as creating a right or expectation of privacy, nor should you have a right or expectation of privacy regarding the receipt, transmission, or storage of data on Company IT resources and communications systems.
>
> Do not use Company IT resources and communications systems for any matter that you would like to be kept private or confidential.

Dkt. No. 30-3 at 29-30. Additionally, under the section entitled "Workplace Privacy and Right to Inspect," the Employee Handbook provides as follows:

> Executive Group property, including but not limited to lockers, phones, computers, tablets, desks, work place areas, vehicles, or machinery, remains under the control of the Company and is subject to inspection at any time, without notice to any employees, and without their presence.

> You should have no expectation of privacy in any of these areas. We assume no responsibility for the loss of, or damage to, your property maintained on Company premises including that kept in lockers and desks.

Id. at 31.

In support of his motion to preclude, Defendant Gross relies on *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008). That case involved an action by the plaintiff against two former employees for (1) stealing the plaintiff's business model, customers and internal documents, (2) breaching fiduciary duties, and (3) infringing on the plaintiff's trademarks, trade dress and copyrights. After defendant Alexander Fell was fired from the plaintiff's employ, the plaintiff accessed three of the defendant's personal e-mail accounts and printed e-mails from them. The plaintiff admitted that it was able to access the Hotmail account because the defendant left his username and password information stored on the plaintiff's computer such that when the Hotmail account was accessed, the username and password fields were automatically populated. Also, the defendant had given another employee his user name and password at one point so that she could check on an Ebay sale he was conducting. The plaintiff was able to access the defendant's Gmail account because the username and password were sent to the Hotmail account and was able to access the third account based on a lucky guess that the username and password were the same as the Hotmail account.

In *Pure Power Boot Camp*, while there was a company policy against using the company's equipment for accessing personal e-mail, which provided that no privacy could be expected in such access, there was no evidence that all of the e-mails the plaintiff downloaded were e-mails that were created or reviewed through the use of the plaintiff's system because the plaintiff did not use its computer's memory to determine what the defendant had accessed at work. Thus, because

the plaintiff "accessed three separate electronic communication services, and ... obtained [the defendant's] e-mails while they were in storage on those service providers' systems ... [e]ither of those actions, if done without authorization, would be a violation of the [Stored Communications Act]." *Id.* at 556.

The court found that the defendant had a reasonable expectation of privacy in the e-mail accounts since the policy at issue only addressed the lack of privacy in e-mails the employee created or accessed through the company's computer system. *See id.* at 561-62. Further, the court found that the plaintiff could only be authorized to access those e-mail accounts if the defendant had given his consent and that the defendant, by merely leaving his login information stored on the company's computers where it could be discovered, did not give his implied consent. Instead, the court found "at most, one could argue that [the defendant] ... consented to [the plaintiff] viewing his password. But he did not consent to [the plaintiff] ... using it." *Id.* at 562. The court decided to suppress all e-mails, regardless of whether or not they were otherwise discoverable (*i.e.*, not privileged), but would allow their use for impeachment purposes should the defendant open the door, because the integrity of the judicial process was "threatened by admitting evidence wrongfully, if not unlawfully, secured." *Id.* at 571.

While the Court finds that the decision in *Pure Power Boot Camp* is instructive, it is also distinguishable from the present matter, mainly in that the facts at issue were largely not in dispute. As Mr. Wright indicated at the hearing, there is a factual dispute over how Plaintiff obtained both the emails and the documents attached to them and that this may only be definitively determined after the computer is forensically examined and tested to determine how Defendant Gross' personal email account was accessed. *See* Tr. at 18-19. Specifically, at the hearing, Mr. Mann testified that, once Defendant Gross returned his work computer to Plaintiff,

Mr. Mann accessed the computer by using a password that Defendant Gross had previously provided to Maria Zubieta, who is Plaintiff's "controller/IT" supervisor. *See id.* at 22-23, 25-26. Mr. Mann claimed that, upon gaining access to the computer, he opened the Microsoft Outlook program, which again prompted for a password. *See id.* at 25-27. Mr. Mann then used the same password that was used to access the computer, which granted him access to Outlook. *See id.* Upon gaining access to Outlook, Mr. Mann claims that two different email accounts were displayed side-by-side on the upper left-hand corner of the screen: Defendant Gross' work email (ChrisGross@ExecutiveGroupInc.com) and his personal email account (cpg0914@outlook.com).

According to Defendant Gross, however, he only ever accessed his personal email account through the Google website. *See* Tr. at 113-15. Defendant Gross claims that he never linked his Outlook account with his work email address and, therefore, his personal email account was not displayed along with his work account in Outlook. *See id.* Further, Defendant Gross claims that, prior to returning his work computer to Plaintiff, he "went onto the Google and clear history and did practice runs to make sure that my personal stuff was not accessible." *Id.* at 114. Although Defendant Gross admits to sending the emails at issue, there was no testimony establishing that he sent the emails using his work computer, rather than from a personal device.

Regardless of whether Plaintiff will eventually be permitted to use some of the emails at issue as this case proceeds, the Court has significant doubts regarding the emails that were sent after Defendant Gross left his employment with Plaintiff. For example, Plaintiff provided an email that Defendant Gross sent to Brad Jones on May 5, 2020, five days after his April 30, 2020 resignation. *See* Dkt. No. 50-7 at 3. Assuming that the Employee Handbook provided Plaintiff with the authority to review the emails that were sent while Defendant Gross was still an employee, it clearly does not apply to emails that were sent after he resigned. According to Mr.

Mann, Defendant Gross returned the computer to another employee's house, and Mr. Mann retrieved the computer on May 4, 2020. *See* Tr. at 24-25. Therefore, it is clear that at least some of the emails at issue were not "transmitted, received, or downloaded over Company IT resources and communications systems."

Although the Employee Handbook provides Plaintiff "the right to monitor, intercept, and/or review all data transmitted, received, or downloaded over Company IT resources and communications systems," it is unclear at this point whether the emails at issue were actually "transmitted, received, or downloaded over Company IT resources." Since the precise manner in which the emails at issue were obtained by Plaintiff and whether they were even transmitted using Plaintiff's computer, the Court finds that it is premature at this time to preclude the use of these documents in this litigation. *See City of Almaty, Kazakhstan v. Ablyazov*, No. 1:15-cv-5345, 2017 WL 9771809, *5 (S.D.N.Y. July 28, 2017) (noting that courts consistently prohibit parties from using stolen materials to their advantage in litigation, even when it may have otherwise been discoverable, but holding that ordering a protective order would be premature because the plaintiffs have not yet proven that the defendant was responsible for the hacking); *Hoofnagle v. Smyth-Wythe Airport Comm'n*, No. 1:15-cv-8, 2016 WL 3014702, *10-11 (W.D. Va. May 24, 2016).

Accordingly, Defendant Gross' motion to preclude evidence is denied without prejudice.

E. Evidence Pursuant to Rule 807

On June 8, 2020, Plaintiff filed a notice pursuant to Rule 807 of the Federal Rules of Evidence, stating its intent to offer into evidence certain hearsay statements relating to bids that were awarded to its competitors and the fact that it would be required to submit its current financials to show that it was financially stable in order to compete for a project. *See* Dkt. No. 27.

Defendants seek to preclude Plaintiff from relying on this hearsay testimony in support of the requested injunctive relief. *See* Dkt. No. 37. Defendants contend that the testimony is irrelevant because the "TRO recites that any preliminary injunction shall be limited to the 'retention and utilization of certain proprietary information belonging to Plaintiff in the possession of Defendants[.]'" *Id.* at 8.

Pursuant to Rule 807, under the following conditions, a hearsay statement is not excluded by the rule against hearsay even if the statement is not admissible under a hearsay exception in Rule 803 or 804:

> (1) the statement is supported by sufficient guarantees of trustworthiness – after considering the totality of circumstances under which it was made and evidence, if any, corroborating the statement; and
>
> (2) it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts.

Fed. R. Evid. 807(a). "'To be admissible pursuant to the residual exception, the evidence must fulfill five requirements: trustworthiness, materiality, probative importance, the interests of justice[,] and notice.'" *United States v. Griffin*, 811 Fed. Appx. 683, 686 (2d Cir. 2020) (quoting *Parsons v. Honeywell, Inc.*, 929 F.2d 901, 907 (2d Cir. 1991)). "'Congress intended that the residual hearsay exceptions will be used very rarely, and only in exceptional circumstances.'" *Id.* (quotation omitted).

The statements identified in Plaintiff's Rule 807 notice are relevant solely to Plaintiff's defamation claim. "Constitutional concerns and long tradition make courts often wary of enjoining defamation." *Ferri v. Berkowitz*, 561 Fed. Appx. 64, 65 (2d Cir. 2014) (citations omitted). Given this concern (and the fact that Plaintiff is not seeking injunctive relief as to its

defamation claim), the Court finds that the Rule 807 testimony is irrelevant and will not be considered by the Court.

C. Standard of Review

"A party seeking preliminary injunctive relief must establish: (1) either (a) a likelihood of success on the merits of its case or (b) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in its favor, and (2) a likelihood of irreparable harm if the requested relief is denied." *Time Warner Cable, Inc. v. DIRECTV, Inc.*, 497 F.3d 144, 152-53 (2d Cir. 2007); *accord North American Soccer League, LLC v. United States Soccer Fed'n, Inc. ("NASL")*, 883 F.3d 32, 37 (2d Cir. 2018). In addition, the movant must show that "a preliminary injunction is in the public interest[,]" *NASL*, 883 F.3d at 37; *accord Friends of the E. Hampton Airport, Inc. v. Town of E. Hampton*, 841 F.3d 133, 143 (2d Cir. 2016); and "that the balance of equities tips in his favor." *Benisek v. Lamone*, ___U.S. ___, 138 S. Ct. 1942, 1944 (2018); *see also American Civil Liberties Union v. Clapper*, 804 F.3d 617, 622 (2d Cir. 2015) ("A preliminary injunction is an equitable remedy and an act of discretion by the court. A party seeking a preliminary injunction must generally show a likelihood of success on the merits, a likelihood of irreparable harm in the absence of preliminary relief, that the balance of equities tips in the party's favor, and that an injunction is in the public interest"). "[A] preliminary injunction is 'an extraordinary remedy never awarded as of right[,]'" *Benisek*, 138 S. Ct. at 1943 (quoting *Winter v. Natural Res. Defense Council, Inc.*, 555 U.S. 7, 24, 129 S. Ct. 365, 172 L. Ed. 2d 249 (2008)), and "should not be granted unless the movant, by a clear showing, carries the burden of persuasion." *Sussman v. Crawford*, 488 F.3d 136, 139-40 (2d Cir. 2007) (quoting *Mazurek v. Armstrong*, 520 U.S. 968, 972, 117 S. Ct. 1865, 138 L. Ed. 2d 162 (1997)

(emphasis in original)); *accord Capstone Logistics Holdings, Inc. v. Navarrete*, 736 Fed. Appx. 25, 26 (2d Cir. 2018).

D. Irreparable Harm

Since "[i]rreparable harm is the single most important prerequisite for the issuance of a preliminary injunction[,] ... the moving party must first demonstrate that such injury is likely before the other requirements for the issuance of an injunction will be considered." *Rodriguez ex rel. Rodriguez v. DeBuono*, 175 F.3d 227, 234 (2d Cir. 1999) (quotations and citations omitted); *see also JBR, Inc. v. Keurig Green Mountain, Inc.*, 618 Fed. Appx. 31, 33 (2d Cir. 2015) (holding that since irreparable harm "is the *sine qua non* for preliminary injunctive relief[,] ... the moving party must first demonstrate that irreparable harm would be 'likely' in the absence of a preliminary injunction before the other requirements for the issuance of a preliminary injunction will be considered") (quotations and citations omitted); *Coscarelli v. ESquared Hosp. LLC*, 364 F. Supp. 3d 207, 221 (S.D.N.Y. 2019) ("[I]f a party fails to show irreparable harm, a court need not even address the remaining elements" of the preliminary injunction standard).

"Irreparable harm is defined as certain and imminent harm for which a monetary award does not adequately compensate[,] ... [and] exists where, but for the grant of equitable relief, there is a substantial chance that upon final resolution of the action the parties cannot be returned to the positions they previously occupied." *Allstate Ins. Co. v. Harvey Family Chiropractic*, 677 Fed. Appx. 716, 718 (2d Cir. 2017) (quotations and citations omitted); *see also WPIX, Inc. v. ivi, Inc.*, 691 F.3d 275, 285 (2d Cir. 2012) (holding that irreparable harm is "harm to the plaintiff's legal interests that could not be remedied after a final adjudication").

"Harm may be irreparable where the loss is difficult to replace or measure, or where plaintiffs should not be expected to suffer the loss." *WPIX*, 691 F.3d at 285; *accord Salinger v.*

Colting, 607 F.3d 68, 81 (2d Cir. 2010). Thus, unless the movant demonstrates "an injury that is neither remote nor speculative, but actual and imminent and that cannot be remedied by an award of monetary damages[,] ... a motion for a preliminary injunction should be denied." *Rodriguez*, 175 F.3d at 234 (quotations and citation omitted); *see also eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006) (holding that before a court may grant injunctive relief, the plaintiff must demonstrate, among other things, "that remedies available at law, such as monetary damages, are inadequate to compensate for [its] injury").

In the trade secret and loss of business context, courts have found that irreparable harm can result where the business relationship would otherwise have produced an indeterminate amount of business in years to come. *See Free Country Ltd. v. Drennen*, 235 F. Supp. 3d 559, 568 (S.D.N.Y. 2016) (citing cases). Where there is no allegation concerning an ongoing/indeterminate loss, however, courts regularly find that money damages are sufficient and decline to award injunctive relief. *See id.*; *Liberty Power Corp., LLC v. Katz*, No. 10-CV-1938, 2011 WL 256216, *7 (E.D.N.Y. Jan. 26, 2011) (finding that harm was not irreparable where the plaintiff alleged that the defendant's misappropriation would result in lost contracts with a "finite-albeit large-number of customers").

In the present matter, the Court finds that Plaintiff has failed to demonstrate that it will suffer irreparable harm in the absence of a preliminary injunction. As to the disclosure of Plaintiff's bids on several projects that Defendant Gross disclosed to Defendant Suddath, several facts undercut the claimed irreparable harm. First, in his opposing declaration, Mark A. Scullion, President of Defendant Suddath, attests that Defendant Suddath is not bidding and will not bid on any of the projects where Defendant Gross disclosed confidential information to Defendant Suddath regarding Plaintiff's bid for that project. *See* Dkt. No. 22 at ¶¶ 12-15. Further, Defendant

Suddath has indicated that it will not use or disclose this confidential information, and that it will return these documents to Plaintiff, and destroy all paper and electronic copies in its possession. *See id.* at ¶¶ 15-16.

Second, even assuming that Defendant Suddath received a contract award by underbidding Plaintiff, which Defendant Suddath adamantly denies that it will try to do, Plaintiff can be made whole by an award of money damages. *See Liberty Power Corp., LLC*, 2011 WL 256216, at *7 ("The harm Plaintiff has alleged in this case is the possibility that Defendants will use its trade secrets to undercut its contracts with a defined subset of its current and former customers and move them to competing electricity suppliers. Even if the court finds that Plaintiff has shown that there is an actual and imminent risk that Defendants will use Plaintiff's trade secrets to do this, the harm that would result is measureable [sic] and compensable through an award of damages after trial"). In his affidavit in support of the motion, Lance Orcutt even claims that "[t]he disclosure of the bids of Executive Group on several competitive projects has resulted in ***money damages*** to us[.]" Dkt. No. 2-1 at ¶ 18.

Third, at the hearing, Mr. Mann testified that earlier this year the company was in the process of updating its cost data, which is used in generating bids. *See* Tr. at 23. This cost data included "updated overhead numbers, hourly rates, various cost data for different markets." *Id.* at 23-24. In April, while he was still out on furlough, Defendant Gross requested the updated information on cost data. *See id.* However, because Plaintiff had not yet finished updating the cost data, Defendant Gross was not provided with this new information. *See id.* at 24. Given that Plaintiff's bids are now generated based on new cost data that Defendant Gross was never privy to, it is unclear how his potential use of outdated pricing models could possibly be used by Defendant Suddath to underbid Plaintiff for potential jobs.

Further demonstrating the speculative nature of the alleged harm that Plaintiff has suffered, according to Mr. Mann, four of the five bids that were prepared by Defendant Gross prior to his departure were still outstanding at the time of the hearing. *See* Tr. at 96. As to the bid for the Margaritaville Hotel project, while it is true that Plaintiff was not awarded that bid, nothing before the Court demonstrates that their failure to receive that project had anything to do with Defendants' actions. Moreover, Mr. Mann even admitted that those four remaining bids may eventually be awarded to Plaintiff. *See id.* Further, Mr. Orcutt admitted that, as far as he knows, Defendants' actions have not directly led to Plaintiff losing out on a bid. *See id.* at 168-69.

In sum, the record before the Court clearly demonstrates that any harm Plaintiff suffers as a result of Defendants' actions can be adequately compensated through money damages. As such, Plaintiff has failed to demonstrate that irreparable harm will likely result in the absence of injunctive relief.

E. Likelihood of Success on the Merits[1]

1. Trade Secrets

Under New York law, "[a] plaintiff claiming misappropriation of a trade secret must prove that (1) it possessed a trade secret, and (2) the trade secret was used by defendant in breach of an agreement, confidence, or duty, or as a result of discovery by improper means." *Universal Instruments Corp. v. Micro Sys. Eng'g, Inc.*, 924 F.3d 32, 49 (2d Cir. 2019); *accord E.J. Brooks Co. v. Cambridge Sec. Seals*, 31 N.Y.3d 441, 452 (2018). "A trade secret is any formula, pattern, device or compilation of information which is used in one's business, and which gives one an opportunity to obtain an advantage over competitors who do not know or use it." *E.J. Brooks*, 31

[1] In its motion, Plaintiff only raises arguments regarding its trade secrets cause of action and its "hacking" cause of action. *See* Dkt. No. 2-2. As such, the Court will limit its discussion to these two causes of action.

N.Y.3d at 452; *accord Faiveley Transport Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 117 (2d Cir. 2009).

In determining whether information constitutes a trade secret, New York courts have considered:

> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; [and] (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Faiveley, 559 F.3d at 117; *accord Haber*, 188 F.3d at 44.

"Data relating to pricing can constitute a trade secret under some circumstances." *Free Country Ltd v. Drennen*, 235 F. Supp. 3d 559, 566-67 (S.D.N.Y. 2016) (citing *In re Dana Corp.*, 574 F.3d 129, 152 (2d Cir. 2009)). "However, this is generally where a company uses some type of proprietary formula that gives it a unique advantage, such as a complex pricing or trading algorithm in a financial business." *Id.* at 567 (citing *Saks Inc. v. Attachmate Corp.*, No. 14 CIV. 4902, 2015 WL 1841136, *18 (S.D.N.Y. Apr. 17, 2015); *Johnson Controls, Inc. v. A.P.T. Critical Sys., Inc.*, 323 F. Supp. 2d 525, 537-38 (S.D.N.Y. 2004)). On the other hand, information relating to a business' underlying mechanics, such as the prices of materials and costs of manufacturing, are not trade secrets because "any seller's publicly-available prices signal to competitors some information about the underlying mechanics of the seller's pricing structure." *Id.* (citing *Silipos, Inc. v. Bickel*, No. 1:06–CV–02205, 2006 WL 2265055, *4-5 (S.D.N.Y. Aug. 8, 2006); *Prod. Res. Grp., L.L.C. v. Oberman*, No. 03 CIV. 5366, 2003 WL 22350939, *14 (S.D.N.Y. Aug. 27, 2003)).

In the present matter, based on the testimony at the hearing, it is clear that the confidential cost information that Defendant Gross provided to Defendant Suddath is not as "unique" as Plaintiff would like the Court to believe. Rather, all businesses in this field necessarily rely on the same types of information to generate bids for projects. According to Mr. Mann, Plaintiff's final bids are generated by combining labor rates, overhead, warehouse storage, handling, driver costs, trucking costs, etc. While Plaintiff may have lower warehouse storage costs because its warehouse is in Amsterdam, New York, compared to its competitors located in and around New York City, it necessarily incurs higher trucking costs to transport the furniture and fixtures to the site of the project. These basic underlying costs, which are combined to determine the final bid price, are not the type of information that is generally afforded trade secret protection. *See Free Country Ltd*, 235 F. Supp. 3d at 566-67.

Even assuming that the information at issue did constitute a trade secret, Plaintiff has failed to establish the second element of this claim, *i.e.*, that Defendants used the information. Rather, as discussed above, Defendants have sworn under oath that they will not use the information at issue and that, to the extent that any physical copies of the documents will be either returned to Plaintiff or destroyed.

Accordingly, the Court finds that Plaintiff has not established that it is likely to succeed on its trade secret claim.

2. Computer Fraud and Abuse Act

In its seventh cause of action, Plaintiff alleges that Defendants jointly and severally violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, "by engaging in the utilization of computers owned by [Plaintiff] and by misappropriating trade secrets and confidential proprietary

information from said computers in excess of any authorization and utilizing them to improperly and illegally obtain and use proprietary information." Dkt. No. 1 at ¶ 39.

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

Because Defendant Gross was permitted to access Plaintiff's computer system, whether Defendant Gross violated the CFAA turns on the question of whether he "exceed[ed] authorized access" within the meaning of the CFAA.

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

follows: "While 'authorization' could refer, as the Government contends, to the purposes for which one is authorized to access a computer, it could alternatively refer to the particular files or databases in the computer to which one's authorization extends." *Id.*

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

Following *Valle*'s reasoning, it has been held that the CFAA "does not apply to a 'so-called faithless or disloyal employee' — that is, an employee who has been granted access to an employer's computer and misuses that access, either by violating the terms of use or by breaching a duty of loyalty to the employer." *Chefs Diet Acquisition Corp. v. Lean Chefs, LLC*, No. 14-cv-8467, 2016 WL 5416498, *6 (S.D.N.Y. Sept. 28, 2016); *accord Apple Mortg. Corp. v. Barenblatt*, 162 F. Supp. 3d 270, 286 (S.D.N.Y. 2016) ("If an employer has given an employee access to the computer and to the relevant files, the employee's subsequent misuse of the information or misappropriation with the intent to compete with his employer is not sufficient to violate the CFAA"). In other words, "to prevail on its claim under the CFAA, [a plaintiff] must show that [d]efendants accessed its computer system without approval; it is not enough to prove access to information beyond the scope of approval." *Chefs Diet*, 2016 WL 5416498, at *6.

In *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 206-07 (4th Cir. 2012), the Fourth Circuit held, under highly analogous facts, that an employee who accessed his former employer's computers and transmitted information to his new employer was not liable under the CFAA, nor was the new employer liable regardless of whether it encouraged the defendant. The court held that it was "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *Id.* at 207.

In the present matter, it is undisputed that Defendant Gross was granted access by Plaintiff to the confidential information he sent to Defendant Suddath. The fact that Defendant Gross may have misused that access is irrelevant, since he accessed the information while still employed by Plaintiff. While it is true that Defendant Gross did send additional information on May 5, 2020, after his resignation, as discussed above, Defendant Gross had returned his work computer no later than May 4, 2020. As such, it is likely that he accessed this information while still employed by Plaintiff, but only sent it to Defendant Suddath after his resignation.

Accordingly, the Court finds that Plaintiff is unlikely to succeed on the merits of its CFAA claim.

IV. CONCLUSION

After carefully reviewing the entire record in this matter, the parties' submissions and the applicable law, and for the reasons set forth herein, the Court hereby

ORDERS that Plaintiff's motion for preliminary injunctive relief (Dkt. No. 2) is **DENIED**; and the Court further

ORDERS that the May 15, 2020 temporary restraining order (Dkt. No. 8) is **DISSOLVED and VACATED**; and the Court further

ORDERS that Defendants' joint motion to preclude the use of Rule 807 evidence (Dkt. No. 37) is **GRANTED**; and the Court further

ORDERS that Defendant Gross' motion asking the Court to reject the affidavit of Philip Becket (Dkt. No. 42) is **DENIED as moot**; and the Court further

ORDERS that Defendant Suddath's letter motion requesting that the Court deny Plaintiff's request to compel Suddath witnesses (Dkt. No. 44) is **DENIED as moot**; and the Court further

ORDERS that the Clerk of the Court shall serve a copy of this Memorandum-Decision and Order on the parties in accordance with the Local Rules.

IT IS SO ORDERED.

Dated: September 2, 2020
Albany, New York

Mae A. D'Agostino
U.S. District Judge