UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

RELIABLE PROPERTY SERVICES, LLC, Plaintiff, v. CAPITAL GROWTH PARTNERS, LLC and CARL T. GEORGE, Defendants.	Case No. 14-CV-0055 (PJS/TNL) ORDER

Peter J. Gleekel and Bradley J. Walz, WINTHROP & WEINSTINE, P.A., for plaintiff.

Carl T. George, pro se.[1]

Plaintiff Reliable Property Services, LLC ("Reliable") provides snow-removal services to retail and commercial establishments, medical facilities, and other customers. Reliable alleges that defendant Carl George recently accessed Reliable's computer system and stole confidential customer information. Reliable brings this action against George and his company, Capital Growth Partners, LLC ("Capital"), alleging violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, the Digital Millenium Copyright Act, 17 U.S.C. § 1201, and the Minnesota Uniform Trade Secrets Act, Minn. Stat. §§ 325C.01 et seq.

[1]Because George is not an attorney, he can represent only himself, and not Capital. *Cf. United States v. Van Stelton*, 988 F.2d 70 (8th Cir. 1993) (per curiam) (corporations cannot appear pro se). No attorney has entered an appearance on behalf of Capital in this matter.

This matter is before the Court on Reliable's motion for a preliminary injunction seeking to enjoin defendants from using the customer information and to require defendants to return it.[2] For the reasons stated below, the motion is granted.

I. BACKGROUND

Reliable uses a software program called "SnowMaster" to facilitate almost all aspects of its business, from coordinating work crews to invoicing. Reliable, George, and Capital are embroiled in a dispute over the rights to the SnowMaster program. In December, Capital filed a lawsuit against Reliable and others in which Capital alleged, among other things, that the defendants had infringed Capital's copyright in the SnowMaster program. *See Capital Growth Partners LLC v. Reliable Property Service LLC*, No. 4:13-CV-2489 (JCH) (E.D. Mo. filed Dec. 13, 2013).

On the same day that Capital filed the Missouri lawsuit, Reliable learned that the SnowMaster program on its computer system had been disabled. There is no dispute that George was responsible for the shutdown. It appears that George accessed Reliable's computer system and installed or activated a piece of software — which Reliable calls a "time bomb" and which George calls a "license management control" — which allows George to disable the system and thus to cripple Reliable's business. George later agreed to re-enable the program, but he threatened to shut it down again unless Reliable met his demands with respect to the copyright dispute.

[2]Although the motion is styled as a motion for a temporary restraining order, defendants have received notice and an opportunity to respond. Accordingly, the Court treats it as a motion for a preliminary injunction.

Reliable filed this lawsuit and sought a temporary restraining order and a preliminary injunction. At the hearing on Reliable's motion for a preliminary injunction, George agreed that he would not access Reliable's computer system nor do anything to disable the SnowMaster program on Reliable's system without the prior permission of a judge. Based on George's promise, the Court denied Reliable's motion for a preliminary injunction as moot.

A few days later, Reliable learned that, when George accessed its system, he not only implanted or activated the "time bomb," but he also obtained Reliable's confidential customer information, including invoices and billing information. *See* Walz Aff. Ex. 1. Reliable learned this in an email from George in which George threatened to publish the customer information that he had obtained unless Reliable met his demands with respect to the copyright dispute. *Id.* George claimed that the customer information showed that Reliable had grossly over-billed its customers for many years. *Id.* George threatened to organize a class-action lawsuit against Reliable to help its customers recover the alleged overcharges. *Id.* About a week later, dissatisfied with Reliable's response to his demands, George created two websites soliciting Reliable customers to join a proposed class action and disseminating the information that George obtained by accessing Reliable's computer system. Walz Aff. Ex. 2.

Reliable now moves for a preliminary injunction to prohibit George and Capital from using or disclosing any of the customer information that George obtained from Reliable, to require George and Capital to return all copies of that information to Reliable, and to order George and Capital to disable the websites through which they have been distributing the information. Capital failed to respond to Reliable's motion, and thus Reliable's motion is granted insofar as it applies to Capital and all of its members, managers, employees, agents,

representatives, and attorneys. *Cf. Van Stelton*, 988 F.2d at 70 (corporations cannot appear pro se). Because George is a member and agent of Capital, the injunction against Capital affords Reliable all of the relief that it seeks. In the interest of thoroughness, however, the Court will separately analyze Reliable's motion as it applies to George individually.

II. ANALYSIS

A. Standard of Review

A court must consider four factors in deciding whether to grant a preliminary injunction: (1) the movant's likelihood of success on the merits; (2) the threat of irreparable harm to the movant if the injunction is not granted; (3) the balance between this harm and the injury that granting the injunction will inflict on the other parties; and (4) the public interest. *Dataphase Sys., Inc. v. C L Sys., Inc.*, 640 F.2d 109, 114 (8th Cir. 1981). Preliminary injunctions are extraordinary remedies, and the party seeking such relief bears the burden of establishing its entitlement to an injunction under the *Dataphase* factors. *Watkins Inc. v. Lewis*, 346 F.3d 841, 844 (8th Cir. 2003).

B. CFAA

Reliable moves for injunctive relief on its CFAA claims. The Court need not address all of Reliable's CFAA claims because it finds that Reliable is likely to succeed on its claim under 18 U.S.C. § 1030(a)(2).[3]

[3]Reliable's § 1030(a)(2) claim appears only in a second amended complaint that Reliable did not seek or receive permission to file. In light of the near certainty that Reliable will receive permission to file that complaint and the exigent circumstances presented by Reliable's motion, the Court will treat the claim as properly before it at this time. Reliable is directed to formally seek leave to file the second amended complaint in compliance with Fed. R. Civ. P. 15 and Local Rules 7.1 and 15.1.

1. Likelihood of Success

Section 1030(a)(2) of title 18 of the United States Code provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" has violated the CFAA. There is no question that Reliable's computer system qualifies as a "protected computer" under the CFAA. *See* § 1030(e)(2)(B) (defining "protected computer" to include a computer "which is used in or affecting interstate or foreign commerce or communication"). Although at one point in his briefing George seems to deny that he obtained any information from Reliable's computer, the evidence that he did so is overwhelming. George has disseminated billing and other information about Reliable's customers, and that information is clearly derived from the billing and other data that he accessed on Reliable's system.

As discussed at the Court's hearing on Reliable's earlier motion for injunctive relief, it is far from clear whether George accessed Reliable's computer "without authorization . . . ." But § 1030(a)(2) prohibits not only accessing a computer "without authorization," but also accessing a computer in a manner that "exceeds authorized access . . . ." George may have been authorized to *access* Reliable's system at the time that he obtained Reliable's customer information, but there is absolutely no evidence that George was authorized to access Reliable's *customer information* for his own purposes (here, to try to force Reliable to give in to his demands with respect to the copyright dispute). At most, the evidence shows that George was authorized to access Reliable's system in order to help maintain the SnowMaster software. When George used his access not to help maintain the SnowMaster software, but instead to analyze and compile

customer data to further his own interests, George almost certainly "exceed[ed] authorized access" for purposes of § 1030(a)(2).

George claims that because his company has a copyright interest in the SnowMaster software on Reliable's computer system, he also has a right to access all of the data stored on that system. But there is a clear distinction between the software on a computer (e.g., Microsoft Word) and data that the user of the software inputs into the computer (e.g., a mother's letter to her daughter). George cites no contract, statute, or other legal authority that gives him the right to access the latter even if his company owns the former. Nor does George get any further with his claim that, because he performed his own analysis of the improperly accessed data and sorted it into various tables and other compilations, he somehow acquired a legal right to that data. George almost certainly had no right to access Reliable's customer information in the first place, and thus he almost certainly has no right to anything that he derived from that information, including any analyses or compilations.

The sole remaining question on the merits, then, is whether § 1030 creates a private right of action for violations of § 1030(a)(2). Section 1030(g) states, in relevant 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).

Under the plain language of this subsection, a plaintiff may bring a claim for a violation "of this section" — meaning § 1030 as a whole — as long as the violation "involves 1 of the factors set

forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." *See Fiber Sys. Int'l, Inc. v. Roehrs*, 470 F.3d 1150, 1157 (5th Cir. 2006).

In an earlier version of the statute, the required "factors" were codified in subsection (a)(5), which led some courts to conclude that the statute only provided a cause of action for violations of (a)(5). *See, e.g.*, *Mclean v. Mtg. One & Fin. Corp.*, No. 04-1158, 2004 WL 898440, at *2 (D. Minn. Apr. 9, 2004). Whether or not that reading of the earlier version of the statute was correct, it no longer remains tenable in light of the revisions that were made to the statute. In the revised version, the required "factors" are set forth in subsection (c)(4)(A). Subsection (c) does not proscribe any conduct, but merely defines the criminal penalties for violations of subsections (a) and (b). Because subsection (c) does not proscribe any conduct, the reference to the factors in subsection (c)(4)(A) obviously cannot be read to limit a private right of action to violations of subsection (c). And, given the reorganization of the statute, there is no longer any textual basis for limiting the private right of action to violations of subsection (a)(5). The Court therefore agrees with Reliable that it may maintain a private right of action under subsection (a)(2), as long as the alleged violation "involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."

Subclause (I) of subsection (c)(4)(A)(i) requires a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value . . . ." George does not dispute that Reliable will suffer at least $5,000 in losses as a result of his actions. Moreover, Reliable has submitted evidence that it retained an audit firm to investigate how George accessed Reliable's computer. Although Reliable has not submitted evidence regarding the cost of the audit, it is almost certain that the audit, in combination with the damage to Reliable's business that would

likely occur in the absence of an injunction, would cause a loss to Reliable of at least $5,000. The Court therefore finds that Reliable is likely to succeed on the merits of its § 1030(a)(2) claim against George.

2. Irreparable Harm

George unlawfully took volumes of detailed data about Reliable's customers and has published it on the Internet. Permitting George to publicize Reliable's customer information is highly likely to damage Reliable's goodwill and its relationships with its customers. The Court therefore finds that Reliable faces a substantial threat of irreparable harm in the absence of an injunction.

3. Balance of Harms and the Public Interest

George used information to which he had no right to attempt to force Reliable to agree to some kind of concession or settlement in connection with the parties' ongoing copyright dispute. Enjoining such conduct would not cause George any harm that can legitimately outweigh the harm that George is causing Reliable. Both the balance of the harms and the public interest clearly favor an injunction.[4]

The Court therefore grants Reliable's motion as to both Capital and George. In light of the circumstances of this case, the Court will not require Reliable to post a bond. Instead, the Court can fully protect George's interests by requiring George to deposit materials containing Reliable's information with the Court, where it will be maintained pending the resolution of this

[4]George argues that issuing the injunction would be contrary to the public interest because the customer information that he acquired provides evidence of criminal behavior on the part of Reliable. But nothing about the Court's injunction would prevent the Court from turning over the information to the United States Attorney's Office, if the Court concludes that the information does indeed provide evidence of a crime.

action. Finally, the Court will defer a decision on whether to transfer this action to the Eastern District of Missouri pending the outcome of the motion to dismiss currently pending in the Missouri action.

ORDER

Based on the foregoing, and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT:

1. Plaintiff's motion for a preliminary injunction [ECF No. 37] is GRANTED.

2. Defendants are hereby enjoined until further order of the Court as follows:

   a. As used in this order, "Information" means:

      i. any information or data that defendants obtained, accessed, or retrieved from plaintiff's computer system, including but not limited to customer lists, invoices, and billing and payment information, and

      ii. any other information, data, data sets, tables, spreadsheets, or any other form of analysis or compilation, that contains, is based on, is derived from, or in any way discloses any of the information or data listed in subparagraph (i).

   b. Defendants are prohibited from using, disclosing, possessing, or transmitting any Information in any format whatsoever including but not limited to paper, electronic, machine-readable, or graphic form.

   c. Defendants are ordered to immediately deposit with the Court any and all materials in any format whatsoever including but not limited to paper,

electronic, machine-readable, or graphic form, that contain, are based on, are derived from, or disclose any Information. To comply with this subparagraph, defendants must make all reasonable efforts to retrieve such materials from any third parties who may be in possession of such materials with the exception of the United States Attorney's Office.

d. Defendants are prohibited from retaining any materials in any format whatsoever including but not limited to paper, electronic, machine-readable, or graphic form that contain, are based on, are derived from, or disclose any Information. If necessary to comply with this paragraph, defendants must, after complying with ¶ 2(c) of this order, permanently destroy, delete, or erase any and all materials that they are prohibited from retaining under this paragraph.

e. Defendants are ordered to disable the websites located at www.snowplowingfraud.com and www.reliablebillingfraud.com and any other websites that contain, store, allow access to, or disclose any Information. Defendants are further ordered not to create any new websites that contain, store, allow access to, or disclose any Information.

3. Defendants are enjoined from accessing or interfering with plaintiff's computer system or servers or any software on plaintiff's computer system or servers by any means whatsoever.

4. This order and injunction also apply to any and all of defendants' members, managers, employees, agents, representatives, or attorneys, and any and all

persons or entities acting in concert or participation with defendants or defendants' members, managers, employees, agents, representatives, or attorneys, with the exception of the United States Attorney's Office.

5. All persons and entities enjoined under the terms of this order — including those listed in ¶ 4 — are warned that any violation of this order may subject them to sanctions or to civil or criminal contempt proceedings.

6. This action is STAYED until further order of the Court, with the exception of:

   a. any proceedings necessary to enforce this order; and

   b. plaintiff's motion for leave to file the second amended complaint, defendants' response to such motion, and the resolution of such motion.

LET JUDGMENT BE ENTERED ACCORDINGLY.

Dated: February 14, 2014

s/Patrick J. Schiltz
Patrick J. Schiltz
United States District Judge