DAVID W. HANSEN (Bar No. 196958)
JACK P. DICANIO (Bar No. 138782)
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
525 University Avenue, Suite 1400
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
DAVID.HANSEN@SKADDEN.COM
JACK.DICANIO@SKADDEN.COM

Attorneys for Plaintiff,
DOTLOOP, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DOTLOOP, INC.,

Plaintiff,

v.

JOHN DOE (d/b/a "Ian Dawtnapstur"),

Defendant.

CASE NO.: 3:13-cv-02654-RS

PLAINTIFF'S NOTICE OF MOTION AND MOTION FOR LEAVE TO CONDUCT THIRD PARTY DISCOVERY AND SUPPORTING MEMORANDUM OF POINTS AND AUTHORITIES

Date: August 29, 2013
Time: 1:30 PM
Judge: Honorable Richard Seeborg

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR COUNSEL:

PLEASE TAKE NOTICE that Plaintiff, dotloop, Inc., hereby moves this Court for an order granting leave to conduct third-party discovery sufficient to identify, name and serve the John Doe Defendant in this action. Pursuant to the Motion to Shorten Time filed herewith, Plaintiff respectfully requests that the instant motion be heard on August 29, 2013, or as soon thereafter as possible, so that Plaintiff can quickly learn Defendant's true identity and location, and name and serve him with the Complaint in this lawsuit.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

As detailed in Plaintiff's Complaint and below, Defendant is an experienced and skilled computer hacker. Defendant fraudulently posed as an Administrator of one of Plaintiff's largest clients in order to unlawfully access Plaintiff's protected computer system, without authorization, and misappropriate and wrongfully disseminate a large volume of information stored on Plaintiff's system. Defendant also unlawfully provided third parties with the means to improperly access and use Plaintiff's computer system and information contained on that system.

Plaintiff filed this action alleging violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, California Penal Code § 502(c), and other state law claims. Through this action, Plaintiff seeks damages, an injunction, and other appropriate relief against Defendant.

Defendant has gone to great lengths to conceal his true identity and escape liability for his wrongdoing. Since learning of Defendant's unauthorized access to its computers and his disclosure of documents contained therein, Plaintiff has undertaken an extensive investigation to identify Defendant's true identity. These efforts are detailed herein and include public record searches, direct contact with Defendant concerning this lawsuit, and requests for assistance from third parties Plaintiff believes to have information concerning Defendant's true identity. Plaintiff's efforts have proved unsuccessful.

Having exhausted all reasonable efforts, Plaintiff is unable to determine Defendant's

identity. The information that may definitively identify Defendant appears to reside with third parties, including Internet Service Provider Google, Inc. ("Google"), which maintains the records regarding the Gmail and Google+ accounts used by Defendant in connection with his unlawful activities, and others discussed below that Plaintiff believes have information that will allow Plaintiff to learn Defendant's identity.

Plaintiff therefore respectfully requests that the Court allow Plaintiff to conduct the limited discovery necessary to identify and locate Defendant so that he can be named in this lawsuit and held accountable for his misconduct.

II. FACTS

A. Plaintiff's Secure Computer System

Founded in 2009, Plaintiff is a leading provider of computer systems that allow residential real estate buyers, sellers, and their agents to interact and collaborate online. *See* Declaration of Matt Vorst ("Vorst Decl."), submitted herewith, ¶ 3. Plaintiff's service provides a secure on-line "virtual workspace" for agents to work and share information. *Id.* Once a potential transaction is identified, the parties and their agents can collaborate through Plaintiff's service to complete paperwork and collect the signatures needed to execute a real estate transaction electronically in real-time. *Id.*

Keller Williams Realty, the largest real estate brand in the United States by agent count, integrated Plaintiff's system into its "eEdge" all-in-one software system for agents in late 2011. *Id.* ¶ 4. Keller Williams' eEdge platform uses Plaintiff's system for document storage, compliance management, electronic signatures and filling out residential real estate forms. *Id.*

Keller Williams is organized into geographic "Market Centers" distributed throughout the country. *Id.* ¶ 5. Plaintiff's portion of the eEdge system includes "Form Spot," a secure repository of forms used by Keller Williams' agents and Administrators in the various Market Centers. *Id.* Only an authorized Keller Williams Administrator has lawful authority to upload and manage the forms included in Form Spot for each Market Center. *Id.*

The Form Spot Market Center activation page contains a number of "Required Fields" to be entered by the Administrator, including the Administrator's name, email address, Market Center

number, and the state(s) and Association(s) where they do business. *Id.* ¶ 6. The Administrator is also required to agree to the Form Spot Terms and Conditions. *Id.*

B. Defendant's Unlawful Conduct

On or about March 16, 2013, Defendant unlawfully created an account on Form Spot using the name "Ian Dawtnapster" and the email address ian.dawtnapstur@gmail.com. *See* Vorst Decl. ¶ 7. In creating this account, Defendant fraudulently posed as an authorized Administrator of Keller Williams Market Center No. 539, which covers L.A. Harbor, California. *Id.*

Prior to succeeding in this fraudulent and unauthorized access to Form Spot, Defendant had unsuccessfully attempted to hack into the Form Spot system under two other California Market Center numbers. *Id.* ¶ 8.

Once fraudulently logged in to Form Spot, Defendant proceeded to unlawfully upload and download forms. *Id.* ¶ 9. Defendant also unlawfully recorded and posted his unlawful activities on the Google+ service and on a variety of other, hacker-affiliated websites. *Id.* Defendant further unlawfully provided third parties with the means to improperly access and use dotloop's protected computer system and information contained on that system. *See id.* ¶ 14-17.

The Form Spot system keeps a log of the Internet Protocol ("IP") addresses that visit the system. *Id.* ¶ 11. An IP address provides information concerning where the visitor is located and, in many instances, the identity of the visitor. *Id.*

To hide his location and identity and cover his tracks in connection with his unlawful activities, Defendant "spoofed" the IP address of his computer by accessing Form Spot through various "proxy" servers with Auckland, New Zealand IP addresses. *Id.* ¶ 12-13.

Defendant's conduct has caused Plaintiff to suffer damages (including impairment of its systems) and to incur losses (including costs associated with investigating Defendant's unauthorized access and disclosure, taking mitigation measures, and implementing additional safety measures to prevent further unauthorized access or disclosure). *Id.* ¶ 14.

C. Plaintiff Has Exhausted All Reasonable Efforts To Identify And Locate Defendant

Immediately upon learning of Defendant's unauthorized access to its computers and unlawful dissemination of information contained thereon, Plaintiff undertook an extensive investigation to determine Defendant's true identity. Defendant has gone to great lengths to conceal his true identity and hide from liability for his wrongdoing. Despite exhaustive efforts, Plaintiff has so far been unable to learn Defendant's true identity. Those efforts include the following:

1. Investigation of the IP addresses associated with Defendant

Plaintiff analyzed the IP addresses associated with Defendant's access to Plaintiff's computer system in an attempt to learn Defendant's identity. Plaintiff's efforts in this regard were futile.

As noted, to hide his location and identity and cover his tracks in connection with his unlawful activities, Defendant apparently "spoofed" the IP address of his computer by accessing Plaintiff's secure computer system through various "proxy" servers with Auckland, New Zealand IP addresses. *See* Vorst Decl. ¶ 13. These IP addresses thus provided no useful information as to Defendant's identity. *Id.*

2. Investigation of "Ian Dawtnapstur"

Although the name used by Defendant, "Ian Dawtnapstur," is obviously fictitious, Plaintiff searched available online sources to determine whether an individual of this name could be located. *See* Declaration of David W. Hansen ("Hansen Decl.), submitted herewith, ¶ 5. Not surprisingly, Plaintiff's investigation indicates that there is no real individual named "Ian Dawtnapster." *Id.*

Plaintiff also reviewed publicly available information concerning the Gmail (ian.dawtnapstur@gmail.com) and Google+ (https://plus.google.com/111710388906785189336/posts#111710388906785189336/posts) accounts used by Defendant. *Id.* ¶ 6. These efforts also provided no information as to Defendant's identity. *Id.*

3. Communication with Defendant concerning this lawsuit

After filing this lawsuit, Plaintiff's counsel sent a letter to Defendant *via* the Gmail address

he used to hack Plaintiff's system and provided him with a copy of the Complaint and related materials. *See id.* ¶ 7. Plaintiff's counsel asked Defendant to contact him immediately to discuss this matter. *Id.* He also informed Defendant that Plaintiff would "otherwise have no choice but to petition the Court for expedited discovery directed to Google, Inc. and possibly others to learn your true identity." *Id.*

Defendant did not respond. *Id.* ¶ 8.

4. Communications with third parties concerning Defendant

Plaintiff's counsel also contacted certain third parties that Plaintiff believes have information concerning Defendant's identity.

(a) California Association of Realtors

On July 18, 2013, Plaintiff's counsel sent a letter to Brian A. Manson, Esq., Managing Counsel of the California Association of Realtors ("CAR"), requesting CAR's help in identifying Defendant. *See* Hansen Decl. ¶ 10.

Mr. Manson told Plaintiff's counsel during an earlier call that CAR had accessed Plaintiff's computer system. *Id.* ¶ 11. Counsel informed Mr. Manson that Plaintiff's "investigation of this matter indicates that CAR obtained the URL it used to access the dotloop system from the Defendant, who only learned this Internet address as a result of his unlawful activities."

> "For example, a computer with an IP address registered to CAR (12.201.80.66) first accessed the dotloop system *via* this URL on March 21, 2013, less than four minutes after the Defendant used this same URL to access the system. It would have been virtually impossible for CAR to have learned this URL unless it was provided by the Defendant, and the timing of CAR's access strongly indicates that the address was in fact provided to CAR by the Defendant."

See id.; *see also* Vorst Decl. ¶ 16-18.

Mr. Manson responded on July 19, 2013. *See* Hansen Decl. ¶ 12. Although Mr. Manson did not deny that CAR accessed Plaintiff's computer system, he did not explain how CAR obtained the complex URL it used, he did not deny that CAR obtained the URL from Defendant, and he did not provide any information that would help Plaintiff learn Defendant's identity. *Id.* ¶ 13. Instead, Mr. Monson simply claimed ignorance and washed his hands of the whole affair:

> "Thank you for your letter of July 18, 2013. Protecting one's intellectual property is a high priority for us as well. We were unaware of the actions described in your complaint prior to reading it. We haven't found anything that identifies the user referred to as ian.dawtnapstur@gmail.com. We're sorry we couldn't help you in this regard."

Id.

Contrary to Mr. Manson's statement, CAR was well-aware of the third party access to Plaintiff's computer system referenced in the Complaint. As noted, Mr. Manson previously admitted that CAR had accessed Plaintiff's computer system. *Id.* ¶ 14. In addition, during a July 10, 2013 discussion at "Real Estate Connect," CAR's CEO, Joel Singer, publicly criticized the security of Plaintiff's system based on CAR's access to the system. *Id.* ¶ 15.

But CAR was only able to access the Plaintiff's computer system by using the complex URL that Defendant only discovery as a result of his unlawful hack of Plaintiff's system. *See* Vorst Decl. ¶¶ 15-16. Plaintiff estimates that the odds are less than one in one trillion that CAR independently learned the details of this complex URL. *Id.* ¶ 17. Moreover, CAR first used this complex URL to access Plaintiff's system less than four minutes after Defendant used this same URL to access the system. *Id.* ¶ 16.

CAR was obviously less than forthcoming in its response to Plaintiff's counsel. It is most likely that CAR obtained the complex URL it used to access Plaintiff's computer system from Defendant or someone associated with Defendant. Plaintiff therefore believes that discovery directed to CAR would assist in determining Defendant's true identity.

(b) Northwest Multiple Listing Service

On July 18, 2013, Plaintiff's counsel sent a letter to Justin D. Haag, the Director of Policies and Forms for Northwest Multiple Listing Service ("NWMLS"), requesting NWMLS's help in identifying Defendant. Hansen Decl. ¶ 17. NWMLS's outside counsel Chris Osborn, Esq., of Foster Pepper, PLLC, also was provided a copy of this letter. *Id.*

Mr. Haag previously sent an email to Plaintiff's CEO, Austin Allison, on April 19, 2013, which attached "a copy of a PDF that shows hundreds of NWMLS forms being hosted by Dotloop." *Id.* ¶ 18. Mr. Haag told Mr. Allison that NWMLS had "downloaded over 200 NWMLS forms from this site." *Id.*

In his July 18 letter, Plaintiff's counsel included a copy of the PDF that Mr. Haag had provided to Mr. Allison. *Id.* ¶ 19. This PDF "shows access to the secure dotloop Form Spot system on April 3, 2013 *via* the same Keller Williams Market Center that was unlawfully hacked by the Defendant, which was only possible using the log-in and password information created by the Defendant/hacker in connection with his unlawful activities." *Id.* Plaintiff's counsel told Mr. Haag:

> This indicates that the Defendant/hacker is someone working for NWMLS or that this information was provided to NWMLS by the Defendant/hacker. At the very least it is clear that NWMLS knows the identity of the Defendant/hacker.

Id.

NWMLS's counsel, Mr. Osborn, called Plaintiff's counsel and they spoke on August 2, 2013. *Id.* ¶ 20. Mr. Osborn stated that Tom Hurdelbrink, the President & CEO of NWMLS, received a call from "someone" at Instanet Solutions, one of NWMLS's vendors, with the log-in and password information that NWMLS used to access Plaintiff's computer system through the Keller Williams Market Center. *Id.* Mr. Osborn stated that although NWMLS only dealt with a few people at Instanet Solutions, Mr. Hurdlebrink claimed not to recall the name of the person from Instanet Solutions who provided the log-in and password information. *Id.*

Plaintiff believes that NWMLS also was less than forthcoming in its response and that it most likely has more information concerning Defendant's hack that would assist in determining Defendant's true identity.

(c) Instanet Solutions

On August 8, 2013, Plaintiff's counsel sent a letter to Martin Scrocchi, the CEO and President of Instanet Solutions, requesting his help in identifying Defendant. *Id.* ¶ 21. Plaintiff's counsel told Mr. Scrocchi what NWMLS had passed along concerning its unauthorized access to Plaintiff's computer system, and that this indicated that Defendant works for Instanet Solutions or that Instanet Solutions at least knows Defendant's identity:

> NWMLS has informed us that the Defendant/hacker's log-in and password were provided to Mr. Tom Hurdelbrink, CEO and President of NWMLS, by Instanet Solutions. This indicates that the Defendant/hacker is someone working for Instanet Solutions or that the log-in and password were provided to Instanet

> Solutions by the Defendant/hacker. At the very least it is clear that Instanet Solutions knows the identity of the Defendant/hacker.

Id. Plaintiff's counsel requested "that Instanet Solutions provide us with all information in its possession concerning the identity of the Defendant/hacker and the unlawful access to the dotloop computer system." *Id.*

Mr. Scrocchi did not respond. *Id.* ¶ 23.

Plaintiff believes that discovery directed to Instanet Solutions is appropriate and very likely will assist in determining Defendant's true identity.

III. DISCUSSION

In situations like this one, where a defendant's identity cannot be ascertained prior to the filing of a lawsuit, "'the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds.'" *Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (quoting *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980)). *See also In re Comm'r re Request for Judicial Assistance for the Issuance of Subpoena Pursuant to 28 U.S.C. § 1782*, 2011 U.S. Dist. LEXIS 75471, at *16-17 (N.D. Cal. July 13, 2011); *SolarBridge Techs., Inc. v. John Doe (dba "Mark Tatley")*, 2010 U.S. Dist. LEXIS 97508, at *3 (N.D. Cal. Aug. 27, 2010).

Courts in this district generally consider whether a plaintiff has shown "good cause" for the early discovery. *See, e.g., In re Comm'r re Request for Judicial Assistance*, 2011 U.S. Dist. LEXIS 75471, at *16-18; *IO Group, Inc. v. Does 1-65*, 2010 U.S. Dist. LEXIS 114039, at *2 (N.D. Cal. Oct. 5, 2010); *SolarBridge*, 2010 U.S. Dist. LEXIS 97508, at *4.

> "In evaluating whether a plaintiff establishes good cause to learn the identity of Doe defendants through early discovery, courts examine whether the plaintiff (1) identifies the Doe defendant with sufficient specificity that the court can determine that the defendant is a real person who can be sued in federal court, (2) recounts the steps taken to locate and identify the defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) proves that the discovery is likely to lead to identifying information that will permit service of process."

Zoosk, Inc. v. Doe, 2010 U.S. Dist. LEXIS 134292, *4-5 (N.D. Cal. Dec. 9, 2010) (citations omitted). *See also In re Comm'r re Request for Judicial Assistance*, 2011 U.S. Dist. LEXIS 75471, at*16-17; *SolarBridge*, 2010 U.S. Dist. LEXIS 97508, at *3-4.

Plaintiff has established its entitlement to limited discovery under this standard to determine Defendant's identity.

A. Defendant Is A Real Person

As detailed above, Defendant is an individual who unlawfully hacked into Plaintiff's secure computer system using a Gmail account associated with Mountain View-based Google. Plaintiff also posted fruits of his unlawful activity on his Google+ account. Defendant's misconduct caused Plaintiff to incur damages and losses, including impairment to its computer systems, costs associated with investigating Defendant's unauthorized computer access, as well as the loss to its business stemming from the diminished value of its trade secrets and associated goodwill.

Defendant is a real person who, once identified, will be subject to this lawsuit.

B. Plaintiff Has Taken Substantial Steps To Locate Defendant

As also detailed above, Plaintiff has undertaken a diligent investigation to identify Defendant without the use of third party discovery. Plaintiff's efforts have been substantial and exhaustive but have not led to the identification of Defendant.

The "Ian Dawtnapster" name and Gmail and Google+ accounts, by themselves, only have value insofar as they can be associated with further account information and/or an IP address. This information is only possessed by Google, which typically does not divulge customer information without a subpoena or other legal authorization. *See SolarBridge*, 2010 U.S. Dist. LEXIS 97508, at *5; *see also* http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_does_google_do. Plaintiff therefore seeks to subpoena Google for this otherwise unobtainable information.

In addition, the responses—or lack thereof—from CAR, NWMLS and Instanet Solutions show that subpoenas are necessary to obtain all of the information in their possession concerning Defendant's identity.

Accordingly, Plaintiff requests leave to serve discovery on these third parties. The requested discovery is necessary to identify and serve Defendant.

C. Plaintiff's Action Can Withstand A Motion To Dismiss

The Complaint adequately alleges claims against Defendant for violations of the CFAA and

California Penal Code § 502(c).

To state a claim for relief under the CFAA, Plaintiff must plead facts that show Defendant (1) accessed a "protected computer," (2) without authorization or in excess of authorization, (3) intentionally, and (4) as result of the conduct caused damages. *Multiven, Inc. v. Cisco Systems, Inc.*, 725 F. Supp. 2d 887, 891 (N.D. Cal. 2010) ; *see also Craigslist Inc. v. 3Taps Inc.*, 2013 U.S. Dist. LEXIS 116732, at *7-8 (N.D. Cal. Aug. 16, 2013). Plaintiff meets this requirement because the Complaint pleads facts showing that Defendant has violated Section 1030(a)(2)(C) of the CFAA by intentionally accessing a computer used for interstate commerce or communication, without authorization, and by obtaining information from such protected computer. *See* Complaint (Dkt No. 1) ¶¶ 13-21. The Complaint also pleads facts showing that Defendant has violated Section 1030(a)(4) of the CFAA by knowingly, and with intent to defraud Plaintiff, accessing a protected computer, without authorization, and by means of such conduct furthered the intended fraud and obtained one or more things of value. *See id.* ¶¶ 13-20, 22. The Complaint also alleges that Plaintiff "has suffered damages or loss as the result of Defendant's wrongful conduct as alleged herein in excess of $5,000." *Id*. ¶ 23.

Like the CFAA, Section 502(c) prohibits the unauthorized access of a computer. *See Craigslist*, 2013 U.S. Dist. LEXIS, at *8; *Multiven*, 725 F. Supp. 2d at 895. Plaintiff's claim under Section 502(c) is based on the same operative facts underlying its claim for violation of the CFAA. *See* Complaint (Dkt No. 1) ¶¶ 25-29. The sufficiency of Plaintiff's CFAA claim also shows that Plaintiff has alleged facts sufficient to state a claim under §502(c). *See Craigslist*, 2013 U.S. Dist. LEXIS, at *8; *Multiven*, 725 F. Supp. 2d at 895.[1]

D. Plaintiff's Proposed Discovery Will Likely Lead To Information Identifying Defendant

Finally, there is a reasonable likelihood that its requested discovery will lead to information to identify Defendant and make service on Defendant possible.

---

[1] The Complaint also adequately pleads causes of action for Trespass, *see* Complaint (Dkt No. 1), ¶¶ 30-33, Breach Of Contract, *id.* ¶¶ 34-38, Tortious Interference With Actual And Prospective Economic Advantage, *id.* ¶¶ 39-44.

As described above, Plaintiff proposes a limited course of discovery that likely will result in the identification of Defendant. Plaintiff proposes to serve discovery on Google for all information relating to the individual who registered for and used its services. Plaintiff also proposes serving discovery on CAR, NWMLS and Instanet Solutions for all information relevant to determining Defendant's identity.

Recognizing that these entities may only be the first step in an investigation that ultimately leads to the identification of Defendant, Plaintiff requests authority to issue limited follow-up discovery, if necessary, on leads provided by the subpoenaed parties.

IV. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court grant Plaintiff's Motion for Leave to Conduct Third-Party Discovery.

DATED: August 27, 2013

Respectfully submitted,
SKADDEN, ARPS, SLATE, MEAGHER & FLOM, LLP

By: */s/ David W. Hansen*
DAVID W. HANSEN
Counsel for Plaintiff,
DOTLOOP, INC.