HOLME ROBERTS & OWEN LLP
George M. Haley, #1302
george.haley@hro.com
Blaine J. Benard, #5661
blaine.benard@hro.com
Craig Buschmann, #10696
craig.buschmann@hro.com
299 South Main Street, Suite 1800
Salt Lake City, UT 84111-2263
Telephone: (801) 521-5800
Facsimile: (801) 521-9639

Attorneys for Plaintiff GOOGLE INC.

IN THE UNITED STATES DISTRICT COURT,
DISTRICT OF UTAH, CENTRAL DIVISION

GOOGLE INC., a Delaware corporation, Plaintiff, v. PACIFIC WEBWORKS, INC., a Nevada corporation, and DOES 1-50, Defendants.	Case No. 2:09-cv-1068 **MEMORANDUM OF LAW IN SUPPORT OF *EX PARTE* APPLICATION FOR LEAVE TO TAKE IMMEDIATE DISCOVERY** Judge Bruce S. Jenkins

I. INTRODUCTION

In this case, Plaintiff Google Inc. ("Google") seeks to stop a "work-from-home" Internet scam that utilizes widespread trademark infringement of the famous Google name and marks to defraud the public. The scam involves more than 1,000 websites using a series of electronic templates that generate virtually identical fake news stories, blogs and testimonials to deceive consumers into believing they can make money working at home in a Google-sponsored program. The representations are false – the advertised programs do not exist, and Google does not sponsor these websites. But unwitting consumers, desperate for sources of income in hard times, are being duped into providing their credit or debit card information to pay a nominal fee to sign up, then are charged automatic recurring fees of up to $79.90 a month.

Those involved in the scam use elaborate and sophisticated means to hide their identities and obscure their relationships with each other, making it difficult – if not impossible – without formal discovery to identify all those involved. One defendant that has been identified is Pacific WebWorks, Inc. ("PWW"). Two years ago, PWW settled an action by the Utah Division of Consumer Protection seeking $1.3 million in fines for 174 alleged violations of Utah's Consumer Sales Practices Act – by, *inter alia*, making unauthorized charges – and agreed to refund consumers and comply with the Act. Now PWW is misusing Google's brand to such an extent the Utah Better Business Bureau refers to it as "GoogleWebIncome aka Pacific Webworks, Inc.," and reports more than 300 complaints against PWW in the past year, many alleging unauthorized charges. C. Buschmann Decl., Ex. I. Last month, a class action was filed against PWW in Illinois on behalf of consumers in that state. But sites linked to PWW are the tip of the iceberg, and discovery is required to determine whether PWW or others are the masterminds behind the scam.

As the Federal Trade Commission explained in obtaining a TRO and order for expedited discovery against others involved in the scam, enterprises like this one using electronic means to repeatedly violate consumer protection laws have both the motive and opportunity to destroy evidence. *Id.*, Ex. L. (*FTC v. Infusion Media*, No. 2:09-cv-01112, Rule 65 Certification (D. Nev. June 22, 2009)). Moreover, some of the third parties likely to have relevant evidence in this case often purge electronic files, and/or allow their clients to access the information they host, which in turn would allow Defendants to destroy evidence in the nominal control of third parties.

Both circumstances constitute good cause for expedited discovery to identify the Doe Defendants and to preserve and obtain evidence for the motion for preliminary injunction that Google intends to file as soon as it has the expedited discovery in hand. *See, e.g., Warner Bros. Records Inc. v. Does 1-4*, 2007 U.S. Dist. LEXIS 48829, at *5 (D. Utah July 3, 2007) (good cause for expedited discovery "exists where the evidence sought 'may be consumed or destroyed within the passage of time, thereby disadvantaging one or more parties'") (citation omitted); *AT&T Broadband v. Tech Communs., Inc.*, 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* seizure order where evidence showed "'defendant[], or persons involved in similar activities, ... had concealed evidence or disregarded court orders in the past'") (citation omitted).

Google thus seeks leave to serve on PWW and a few third parties limited immediate discovery – prior to the Rule 26(f) conference – to identify the Doe Defendants and to document Defendants' involvement in the scam. Without this relief, Google may be hindered in its ability to pursue this action to stop Defendants from deceiving the public through infringement of Google's trademarks. As that infringement is ongoing, the need for this relief is critical. *Sara Lee Corp. v. Sycamore Family Bakery, Inc.*, 2009 U.S. Dist. LEXIS 52648, at *3 (D. Utah June 22, 2 009).

II. BACKGROUND

1. As the U.S. Better Business Bureau warned consumers last month, work-at-home scams are common in a tight economy and one work-at-home scam currently proliferating on the Internet "pos[es] as Google." Buschmann Decl., Ex. A. A post to the Miami Herald "Action Line" noted the BBB has received more than 1,500 complaints about numerous sites "using the Google name to scam people who want to work at home." *Id.*, Ex. B. According to the Federal Trade Commission, the scheme has defrauded consumers of millions of dollars. *Id.*, Ex. J at 28 & n.94 (*FTC v. Infusion Media*, No. 2:09-cv-01112, MPA in Support of *Ex Parte* Mot. (D. Nev. June 23, 2009)). Unable to obtain refunds from those operating the scam sites, many consumers have complained to and attempted to obtain refunds from Google, even though Google does not sponsor those sites. *Id.* at 7 & n.17; Decl. of C. Louie, ¶ 9, Ex. A.

2. While the FTC has taken down some websites involved in the scheme, the BBB continues to "receive[] numerous complaints about many other work at home schemes using similar tactics" operating under such names as "Google Biz Kit, Google Cash, Google Money Profits and Google Success Kit." Buschmann Decl., Ex. A. Evidence suggests a few masterminds may be behind all the scam sites but are hiding their identity. *See* Decl. of J. Bajin, ¶¶ 17, 19-22, 24-25. Although they use Google's name and marks, these sites are not sponsored by Google, and Google has not authorized these infringing uses of its trademarks. Louie Decl., ¶ 4.[1] Google now seeks the expedited discovery necessary to move for a preliminary injunction to stop this widespread infringement by all Defendants – the Does as well as PWW.

[1] As explained in its complaint, Google owns multiple current and pending federal registrations for its logo and other trademarks being infringed by Defendants. Compl. ¶¶ 29-32. Copies of the pertinent registrations are attached as exhibits 11-12 to the complaint.

A. How The Scheme Works

3. The scam uses hundreds of websites that act like tentacles drawing in consumers. Referred to in the industry as "Affiliate Sites," they lead consumers to a smaller hub of credit card processing sites, where victims' financial information is collected. Both the Affiliate Sites and the credit card processing sites prominently feature Google's name and mark, leading consumers to believe they are sponsored or endorsed by Google and thus are safe and reputable.

4. The Affiliate Sites and credit card processing sites are not fixed or stable but frequently disappear and then reappear in slightly altered form at different Internet addresses. The Affiliate Sites and credit card processing sites are typically based on identifiable "templates" – *i.e.*, many different sites share the same basic structure and content. The widespread use of templates is one clue indicating centralized control over the scheme. Bajin Decl., ¶ 24, Ex. D.

5. Although Defendants use a series of ever-changing Affiliate Sites and credit card processing sites to promote and cash in on their scam, the sites typically follow the same two-step process: (1) lure consumers with promises of making money through a Google work-from-home program; and (2) trick consumers into providing credit or debit card information to cover nominal "shipping and handling" or "access" fees, which information Defendants then use to charge unexpected, recurring monthly fees ranging up to $79.90 per month. Louie Decl., Ex. A at 8.

6. Though the Affiliate Sites are constantly evolving, the following three examples illustrate common characteristics of the sites and typical ploys used to ensnare consumers.

(1) "LA News" Announces The "Google AdWork" Program

7. Various Affiliate Site templates take the form of fake newspaper or television news websites. These phony news sites have legitimate sounding names, like USA Job Journal,

The Waco Herald, New York Tribune News, Chicago Tribune News and News8 Chicago, to keep consumers from suspecting foul play and investigating the scam. *Compare* Bajin Decl., Ex. K (print outs of phony news sites) *with* Buschmann Decl., Ex. O (print outs of websites for the real newspapers in Waco, the *Tribune Herald*, and Chicago, the *Tribune*).

8. In one example, the Affiliate Site purports to be a newspaper called the "LA News." Here, again, the name alone seeks to confuse visitors; Los Angeles is the home of a major newspaper called the *Daily News*. The scam site features what looks like a news article reporting the announcement that "Google is hiring At Home Workers" as part of its new "Google Adwork" program. *Id.*, Ex. M. According to the site, "thousands of average people [will] earn $4000 - $8000 per month posting Google text ads online." *Id.* The article even attributes a fake quote to Google co-founder Larry Page touting the program. *Id.* ("'The key is knowing that our home workers are not required to have extensive computer or internet knowledge, if you can send and receive email, you can take part in this exciting new opportunity'[sic] Larry Page told reporters.").

9. The fake article invites consumers who want to join the program to "fill out one form" by clicking a link. *Id.* The site tells consumers they will receive a "free instructional kit" and can then "[p]ost links using the information provided and start earning money ($25-$40 per link posted)." *Id.* The site directs consumer to "[c]ash the checks that Google sends, or have the money wired directly to your account." *Id.* Like legitimate online newspapers, these fake sites appear to include comments from readers at the bottom of the page. *Id.*, *see also id.*, Ex. J. These comments uniformly reinforce the sales pitch and add a sense of urgency. *Id.*, ¶ 31, Ex. M.

10. Unfortunately for consumers, nothing about this "newspaper article" is accurate. "LA News" does not exist, and there is no "Google Adwork" program. Louie Decl., ¶ 7. As is

typical with sites in the scam, the ability to post actual messages to the comments section has been disabled, purportedly because "bandwidth [has been] exceeded." The real reason is to prevent victims from leaving comments alerting others to the true the nature of the scam.[2]

11. Clicking on any of the site's six different "Google Adwork" links directs consumers to a credit card processing website operated by Defendant PWW at https://secure1 profitcenterlearning.com/gosu/payment.asp. Bajin Decl., ¶ 31, Ex. M at 4 and Ex. N at 1. This site invites consumers to "earn up to $349 a day" by obtaining the "Google Profit Software trial kit." *Id.*, Ex. N at 1. Consumers must first "see if [they] qualify" for the program, by entering their name and address. *Id*. at 2. Consumers are then directed to a second page at the same profitcenterlearning.com domain, which prominently features Google's logo and asserts that the program is the same as the one reported on CNN, ABC, Fox News, NBC and/or USA Today. *Id.* at 1, 3. Since no "Google Adwork" program exists, there have been no such reports about it.

12. This page discloses to consumers that there is a nominal $2.95 fee for "instant access" to the Google Adwork program, which must be paid by credit card. *Id.* Providing credit card information leads consumers to a "Congratulations" web page on the same domain (profitcenterlearning.com), which says charges on their credit card will appear as "Google ATM." *Id.* at 9. But consumers do not receive "access" to materials associated with an actual Google Adwork program because no such program exists. Louie Decl., ¶ 7. Instead, consumers are surprised to learn, when they open their credit card statements, that they have been hit with recurring monthly fees of up to $79.90 in addition to the nominal access fee. *Id.*, ¶ 9, Ex. A at 8.

[2] Google does operate an advertising program under the mark AdWords, but that program is not related in any way to Defendants. The fake "Adwork" newspaper article does not describe Google's AdWords program, though no doubt the inevitable confusion is intentional.

(2) Mary Steadman, Stay-At-Home Mom, Strikes "The Next Gold Rush"

13. A key characteristic of the scheme is its use of templates, so that the same element appears across seemingly unrelated websites. For example, a number of Affiliate Sites contain a story about Mary Steadman, a "mother of 2" who "is thriving in the middle of an economic recession working in the comfort of her own home." Bajin Decl., ¶ 24, Ex. F. Even the same photograph of "Mary Steadman" appears on multiple sites that otherwise appear unrelated to one another. On many of the Mary Steadman Affiliate Sites, "Mary even share[s] ... a picture of the kind of checks she gets from Google each month." *Id.*, Ex. F at 3-4. Google, however, has never issued a check to a Mary Steadman. Louie Decl., ¶ 7. The same photograph of a check purportedly issued by Google appears on numerous other Affiliate Sites. Bajin Decl., Ex. G.

14. Other evidence of both the falsity of the Mary Steadman story and the calculating behavior of Defendants is that Mary Steadman Affiliate Sites frequently use geo-location technology to tailor the story, telling consumers that Mary Steadman is from the viewer's home area, wherever that may be. A quick comparison of the sites shows that on the same day, Mary Steadman was from both Denver, Colorado, and Salt Lake City, *compare* Compl., Ex. 1 *with id.*, Ex. 6, thus matching her purported hometown with the location of those viewing her website.

15. Like all Affiliate Sites, the Mary Steadman Sites direct the consumer to a credit card processing site, which leads to the consumer's money being taken. Bajin Decl., Ex. F.

(3) Ben, Dan and Frank "Get Green"

16. Another popular template in the scheme consists of a fake blog posting or testimonial recounting the story of how a young, hardworking man deep in debt "turned [his] life around" by using a Google work-from-home kit. *Id.*, ¶ 24, Ex. D. Various manifestations of

essentially the same site – complete with the same photographs of the handsome young man and his wife vacationing in Italy and dancing at their wedding – have appeared at the domain names bengetsgreen.com, dangetsgreen.com and frankgetsgreen.com. *Id.*

17. As with all Affiliate Sites, [name]getsgreen.com leads consumer to a credit card processing site, which seeks to get consumers to submit credit or debit card information. *Id.*

B. Defendant PWW Is A Major Player In The Scheme

18. Defendant PWW is behind a significant amount of this activity. PWW owns and has operated at least four domain names used in connection with credit card processing sites that market work-at-home schemes using Google's name – on1inetrack.com, s3curehost.com profitcenterlearning.com and visualwebtools.com. *Bajin Decl*., ¶ 20, Ex. B.[3] Dozens of websites touting the Google work-at-home scam have directed traffic to these four domain names. *Id.*, ¶ 22, Ex. C.[4] As of late November, PWW's credit card processing sites were used in conjunction with at least 75 sites promoting a money-making program supposedly sponsored by Google. *Id.*

19. PWW admits it is responsible for the products offered on the Credit Card Processing Site linked to from the "LA News" example described above. *Id.*, ¶ 31, Ex. N at 4 ("Products [are] provided by Pacific Web Works, Inc. and/or affiliated companies."). PWW's address and phone number are listed at the bottom of that credit card processing site, with an explanation of additional terms of an "agreement" between the consumer and PWW. *Id.*, at 3. PWW also operates a domain name server that directs viewers to the profitcenterlearning.com

[3] PWW's wholly owned subsidiary, Intellipay, Inc., is the WHOIS record owner of these domain names. Bajin Decl., ¶ 20, Ex. B; Buschmann Dec., ¶ 9, Ex. H.

[4] As the identities of the owners of many of these sites have been protected by privacy services, discovery may reveal that PWW actually owns these sites as well. Bajin Decl., ¶ 20, Ex. B.

domain name, where that Credit Card Processing Site is hosted. *Id.*, ¶ 20, Ex. B at 20. Charges to credit card accounts submitted through the LA News processing site ultimately show up as "PWW*GOOGLE ATM 800-497-4988." *Id.*, Ex. N at 13. Consumer inquiries are directed to "Google ATM" at PWW's address of 230 West 400 South, First Floor, Salt Lake. *Id.* at 10-11.

20. Google is not the first to make allegations of this sort against PWW. In August 2007, the Utah Division of Consumer Protection alleged PWW had committed 174 violations of the Utah Consumer Sales Practices Act, for a potential fine of more than $1.3 million, by, among other things, using "a negative option in their advertising without making the required disclosure and obtaining the appropriate consumer authorization" and "charg[ing] consumers for products and services that the consumer did not authorize." Buschmann Decl., Ex. E (*In re Pacific WebWorks, Inc., et al.*, DCP Case No. 59159).[5] PWW settled that matter by agreeing to refund certain consumers and pay a fine of $742,500, of which all but $10,000 was stayed pending PWW's compliance with other provisions of the settlement. *Id.*, Ex. F (Settlement Agreement)).

21. Last month, a class action was filed in state court in Illinois against PWW over the work-from-home scam. *Id.*, Ex. K (*Ford v. Pacific WebWorks, Inc., et al.*, No. 09CH44278). That complaint alleges five causes of action, all under Illinois law, seeks to certify a class of Illinois residents who were charged unauthorized fees to sign up for a purported Google-related work-at-home program, and seeks relief limited to the putative Illinois class.

C. <u>Other Defendants Involved In The Scheme Are Masking Their Identities</u>

22. Over the last few months, Google has identified more than 1,000 Affiliate Sites running Google "work from home" scams. Bajin Decl., ¶ 15, Ex. A. The vast majority of these

[5] In the form of negative option used in this case, consumers are charged a recurring monthly fee unless and until they "opt out" by notifying the seller they want to stop participating.

sites mask their true ownership. *Id.*, ¶ 17. It is thus unclear how many entities other than PWW have been involved, but one recent Internet blog posting noted that "investigation shows that 30% of all the Google cash, Google income and Google Kit[] types of scams that are active on the internet today are ... related to Pacific Webworks." Buschmann Decl., Ex. G.

23. The evidence indicates that other entities involved in the scam work together and/or with PWW, and that there are a limited number of masterminds behind the scam. The use of templates for the Affiliate Sites and credit card processing sites results in many seemingly unrelated sites that share the same "look and feel," indicating a common enterprise. For example, PWW has operated a credit card processing site (on1inetrack.com) that mirrors the layout of five other allegedly independent credit card processing sites (processcartcenter.com, selfprofitsmadeasy.com, safetrialoffers.com, sundaybikerides.com and googleworkstoday.com), all of which employ the privacy protection services of Domains by Proxy to shield ownership data or list what appears to be a false identity. Bajin Decl., ¶ 20, Ex. B. Tellingly, all six sites use the same coffee cup/computer keyboard configuration. *Id.*, ¶ 30, Ex. L. Yet, according to text at the bottom of the sites, several claim to be operated by companies other than PWW. *Id.*

24. In the action filed by the FTC in June 2009, the United States District Court for the District of Nevada issued first a TRO and then a stipulated preliminary injunction against five entities and four individuals operating the so-called Google Money Tree scams. Buschmann Decl., Ex. M (*FTC v. Infusion Media*, No. 2:09-cv-01112, Am. *Ex Parte* T.R.O. With Asset Freeze (D. Nev. June 24, 2009)); *id.*, Ex. P (Stip. Prelim. Inj. (D. Nev. Sept. 10, 2009)). But, as the BBB has noted, this action does not appear to have reached the heart of the work-at-home scheme using Google's name and trademarks, as both the BBB and Google continue to receive

complaints from consumers about the scam, Buschmann Decl. Ex . A, Louie Decl., ¶ 9, Ex. A, and new websites promoting the scam continue to appear. Bajin Decl., ¶ 15.

III. GOOD CAUSE EXISTS FOR FOCUSED EXPEDITED DISCOVERY OF PWW AND A LIMITED NUMBER OF THIRD PARTIES WITH KEY EVIDENCE

District courts are authorized to depart from normal discovery procedures and to fashion discovery to meet the needs of a particular case. Fed. R. Civ. P. 1, 26(d), 34(b). Although civil discovery in an action filed in federal court typically may not commence until the parties have conferred as required by Rule 26(f), "[t]he traditional sequence of discovery may ... be altered by the court in the exercise of its broad discretion." *Warner Bros.*, 2007 U.S. Dist. LEXIS 48829, at *2. Discovery may be allowed prior to the Rule 26(f) conference on a showing of "good cause." *Id.* (citing, *e.g.*, *Pod-Ners, LLC v. N. Feed & Bean*, 204 F.R.D. 675, 676 (D. Colo. 2002)).

In this case, good cause is clearly established because only expedited discovery prior to the Rule 26(f) conference can lead to the evidence necessary to deconstruct the wall behind which Defendants have hidden. Such discovery is needed so Google can learn the names of the Doe Defendants and determine the full scope of PWW's involvement in the scam. Google needs this information to pursue preliminary injunctive relief that would be effective in stopping those behind the work-at-home scam who are hiding their identities. In addition, immediate discovery is required to minimize destruction of evidence: much of the evidence is in electronic form and thus easily destroyed by the wrongdoers; defendants involved in similar schemes have discarded evidence; and Defendants in this case have shown a willingness to go to great lengths to evade detection and liability. Serving immediate document subpoenas on a limited number of third parties is also necessary to ensure they are aware of their duty to preserve evidence and do not allow Defendants to access, alter or delete evidence hosted on third parties' computer servers.

A. Good Cause For Pre-Rule 26(f) Discovery Exists To Identify Doe Defendants, Untangle Defendants Work-From-Home Scheme And Minimize The Risk Of Destruction Of Evidence Prior To Google's Motion For A Preliminary Injunction

Good cause exists to grant expedited discovery for at least three reasons.

First, the need to identify Doe Defendants constitutes good cause for discovery before the Rule 26(f) conference. *See, e.g., Warner Bros.*, 2007 U.S. Dist. LEXIS 48829, at **3–4 (granting expedited discovery to identify anonymous defendants accused of violating plaintiff's copyrights). Indeed, courts routinely permit early discovery in order to identify Doe Defendants in cases, like this one, where online wrongdoers shield their identities with technology. *See, e.g., Bremenn Research Labs, LLC v. Does 1-20*, No. 2:07-cv-45-TC (D. Utah Feb. 12, 2007) (granting expedited discovery to identify Doe defendants infringing trademarks online); *Microsoft Corp. v. Does 1-217*, No. C06-1192 (W.D. Wash. Sept. 14, 2006) (granting discovery to identify Doe Defendants who had registered and used infringing domain names); *Dynasty Zarooni Inc. v. Does 1-50*, No. C-08-05086 (N.D. Cal. Nov. 20, 2008) (granting expedited discovery to identify Doe defendants in online trademark infringement action); *America Online, Inc. v. Does 1-40*, No. 1:04-cv-00260 (E.D. Va. Mar. 19, 2004) (permitting early discovery to identify Doe defendants in CAN-Spam Act case) (attached at Buschmann Decl., Ex. N)).[6]

Here, identifying the Doe Defendants is critical to untangling the web of Defendants' schemes so that this action can ultimately be effective in shutting down the sites that use

[6] One reason this sort of expedited discovery may be routine is that circuit courts have held that district courts commit reversible error if they do not allow discovery to identify Doe Defendants. *See, e.g., Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (error to dismiss unnamed defendants where discovery may reveal identity); *Valentin v. Dinkins*, 121 F.3d 72, 75-76 (2d Cir. 1997) (*pro se* plaintiff should have been permitted discovery into identity of defendant); *Maclin v. Paulson*, 627 F.2d 83, 87 (7th Cir. 1980) (where "ignorant of defendants' true identity ... plaintiff should have been permitted to obtain their identity through limited discovery").

Google's name and marks to defraud consumers with bogus work-from-home offers.

Second, immediate discovery is appropriate where evidence may be destroyed. *Warner Bro*s., 2007 U.S. Dist. LEXIS 48829, at *5 ("Good cause exists where the evidence sought 'may be consumed or destroyed with the passage of time, thereby disadvantaging one or more parties to the litigation.") (internal quotation omitted); *Pod-Ners*, 204 F.R.D. at 676. In a case like this, there is ample reason to have serious concerns about the preservation and integrity of evidence.

In the FTC's action against the Google Money Tree defendants, an FTC attorney attested under oath that defendants accused of operating these types of consumer fraud scams "have the motivation and opportunity to ... destroy important documents," and "often attempt to ... destroy[] documents." Buschmann Decl., Ex. L at 4, ¶ 11 and 5, ¶ 13(*FTC v. Infusion Media*, No. 2:09-cv-01112, Rule 65 Cert.). The FTC listed seven examples in which defendants in similar cases had "spent the weekend destroying documents" or otherwise sought to conceal evidence. *Id.* at 5-6, ¶ 13(a)-(g). That, alone, would be good cause to warrant expedited discovery. *See, e.g., Comcast of Ill. X, LLC v. Till*, 293 F. Supp. 2d 936, 940-42 (E.D. Wis. 2003) ("grant[ing] plaintiff's request for expedited discovery" and to preserve because, in other cases, "some sellers of decoders have destroyed evidence and secreted assets," even though "defendant in the present case is different … in that he uses his real name and address in conducting business" and is "not attempting to avoid detection").

Moreover, in this case, Defendants already go to great lengths to avoid detection. The identity of the owners of most Affiliate Sites is masked by privacy protection services, and websites involved in the scheme – including those tied to PWW – frequently become disabled or are redirected to different credit card processing cites. Bajin Decl., ¶ 32. These efforts to avoid

detection, coupled with the examples cited by the FTC of defendants in similar scams destroying documents, "show that the defendant[s], or persons involved in similar activities ... had concealed evidence,'" which is sufficient to support an ex parte seizure order, let alone a more limited order for expedited discovery. *AT&T Broadband*, 381 F.3d at 1319-20 (citation omitted).

Concerns about the evidence are particularly acute here because, without the duty to preserve that subpoenas would impose, Defendants may be able to delete or remove even evidence held by third parties, such as domain name registrars and MX hosts, which often allow clients to access their databases to alter information stored on their servers. Bajin Decl., ¶ 10.[7]

Third, good cause "frequently exists in cases involving claims of infringement and unfair competition [and] may be appropriate in cases where the plaintiff seeks a preliminary injunction." *Pod-Ners*, 204 F.R.D. at 676; *Sara Lee*, 2009 U.S. Dist. LEXIS 52648, at *4 ("Given the nature of the allegations [of trademark infringement], there is good cause for expediting all discovery ... to get the case in a dispositive posture at the earliest possible date. If the allegations of the Complaint are in fact true, all parties will be benefitted by hearing the case promptly and reducing Plaintiff's damages. And, if the allegations are not true, there should be little interference with Defendant's business and any such interference will be shortened.").

Here, Google alleges and has made a substantial showing of trademark infringement. Further, Google confronts a complicated network of linked and cross-linked websites, with new sites appearing and old sites transforming at an alarming pace. Expedited discovery is necessary to find the path through the labyrinth to the principals behind the schemes and enable Google to

[7] In addition, the registered name of the domain owner can be quickly changed. *See* Bajin Decl., ¶ 10. Absent immediate discovery, then, the true identities of those behind the scam sites may not be available even after their privacy protection is stripped away.

move forward with its motion for preliminary injunctive relief. *See, e.g.*, *Sara Lee*, 2009 U.S. Dist. LEXIS 52648, at *4; *Yokohama Tire Corp. v. Dealers Tire Supply, Inc.*, 202 F.R.D. 612, 613 (D. Ariz. 2001) ("Expedited discovery has been ordered where it would 'better enable the court to judge the parties' interests and respective chances for success on the merits' at a preliminary injunction hearing.") (citation omitted); *Lindsey & Osborne P'ship, L.P. v. Day & Zimmermann, Inc.*, 2008 U.S. Dist. LEXIS 60333, at *8 (D. Kan. July 22, 2008) ("The Court finds that Plaintiff could suffer irreparable harm if it is prevented from conducting expedited discovery in order to prepare for its preliminary injunction hearing."). As in the above-cited cases, the expedited discovery sought in this case "will substantially contribute to moving this case forward." *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 277 (N.D. Cal. 2002).

B. The Expedited Discovery Google Seeks Is Limited To Providing Evidence For Its Preliminary Injunction Motion And Enabling Google To Identify Doe Defendants

The discovery Google seeks on an accelerated basis is limited in scope and will serve two related evidentiary purposes – to enable Google to identify the Doe Defendants and to file a motion for preliminary injunction. It will also cement PWW's obligation to preserve relevant evidence and notify key third parties to preserve such evidence, as well.

With respect to PWW, Google seeks to serve requests for production to PWW and its subsidiary, Intellipay, and to depose under Rule 30(b)(6) their persons most knowledgeable on a limited number of topics related to the liability of PWW and those working with PWW, both on 15 days' notice. Google's primary purpose in conducting early expedited discovery directed to PWW is to confirm the full scope of PWW's involvement and to obtain evidence about others it is involved with for the preliminary injunction motion. This is exactly the sort of expedited discovery the FTC obtained in the Google Money Tree case for exactly the same sort of activity.

Buschmann Decl., Ex. M at 24-25 (*FTC v. Infusion Media*, No. 2:09-cv-01112, Am. *Ex Parte* T.R.O. With Expedited Disc.).

Google also seeks an order allowing it to serve Rule 45 subpoenas to specific categories of entities likely to possess information identifying those behind the scheme. The subpoenas will be limited to the following categories of entities and information:

(1) Three domain name registrars, GoDaddy, Enom and NameCheap, and related proxy registration services, Domains By Proxy, WhoIs Privacy Protection Inc. and NameCheap dba WhoIsGuard. Domain name registrars are where entities and individuals can register a domain name – the language version of the numeric Internet Protocol ("IP") Address where a website can be found – and proxy registrars provide privacy services that mask who owns a domain name. The immediate discovery Google seeks is limited to records sufficient to identify who owns the domain names associated with websites used in the scam.[8]

(2) Three A-record hosts, Icon Developments, Consonus and XMission. A-record hosts own the IP Addresses for the domain names of the scam sites. Consumers' computers are directed to scam sites via records containing these IP Addresses. The immediate discovery Google seeks is limited to records identifying customers for which these entities are "hosting" the IP Addresses for these scam websites.

(3) Four telephone service providers, Accessline Communications, Network Enhanced Telecom, Paetec Communications and Qwest. The immediate discovery Google seeks is limited to records sufficient to identify who owns the phone numbers used by the scam sites.

(4) Two CPA Networks, registered to Hydra LLC and Intermark Media. CPA Networks act as middlemen between Affiliate Sites and credit card processing sites, referring consumers to the latter via links on the former and using what are believed to be cost-per-action or cost-per-acquisition (CPA) incentive models in which payment is made or received upon a triggering event (*e.g.*, a sale or clicking on a link). The immediate discovery Google seeks is limited to records sufficient to identify who operates the Affiliate Sites and credit card processing sites involved in the scam that generate revenue with and for the CPA Networks.

(5) Four entities that appear to host credit card processing sites used in connection with the scam, Bloosky, Crush, PolarisNet and VOMedia. These sites are

[8] One domain name registrar (GoDaddy) also operates an e-mail server in connection with a Google Money-Making Opportunity and thus will also be asked for records identifying those who sent or received business emails related thereto.

believed to play the same role as Defendant PWW in the scam, but are masking the identity of the entities that actually own and operate them. The immediate discovery Google seeks is limited to records sufficient to identify the CPA Networks and credit card processing sites involved in the scam, and any Affiliate Sites for which the credit card processing sites have identifying records.

(6) Two financial institutions used by the credit card processing sites, Wells Fargo and JPMorganChase. The discovery Google seeks is limited to records sufficient to identify who owns the merchant accounts linked to the scam sites.

Google seeks immediate third party discovery only to identify those operating, promoting and/or profiting from the scam websites.[9] Bank account information is critical because it will allow Google to follow the money. But it alone is not sufficient because the accounts will not identify downstream operators and may not identify the masterminds of the scam if accounts are held by shell companies. The same is true of other categories of third party data; until Google sees the records, it cannot know how many layers of the onion it will have to peel. But if it waits to see what it gets from one or two subpoenas before serving others, there is a serious risk that critical evidence identifying who is behind the scam sites may be purged or destroyed. And if Google cannot quickly obtain the evidence necessary to identify and pursue an action against those involved in the scam, they will recreate it under different names, just as the injunction the FTC obtained against the Google Money Tree defendants has not stopped other scam sites.

This is the type of discovery – primarily seeking to identify Doe Defendants and obtain (and preserve) evidence for the injunction motion – for which pre-Rule 26(f) discovery is often granted. *See, e.g., Posdata Co. Ltd. v. Seyoung Kim*, 2007 U.S. Dist. LEXIS 48359, at **27-28 (N.D. Cal. June 27, 2007) (granting expedited discovery "'to further uncover Defendants'

[9] Google proposes that the subpoenas also seek records about those identified, in order to notify subpoenaed entities about the scope of their duty to preserve evidence. In a cover letter, Google will inform those entities that only identifying records need to be produced in 15 days.

unlawful conduct prior to the preliminary injunction hearing'"); *Microsoft Corp. v. Does 1-50 d/b/a yourloanz.com*, No. 2:04-cv-02218 (W.D. Wash. Nov. 30, 2004) (permitting pre-Rule 26(f) subpoenas to depositions of third-party hosting companies and ISPs, domain name registrars, e-mail service providers, electronic payment processors and banks to identify Doe defendants in action for violation of, *inter alia*, Lanham Act and CAN-Spam Act) (Buschmann Decl, Ex. N).

IV. CONCLUSION

"'[E]xpedited discovery is particularly appropriate when a plaintiff seeks injunctive relief because of the expedited nature of injunctive proceedings.'" *Yokohama*, 202 F.R.D. at 613 (citation omitted). That is all the more true "where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *Semitool*, 208 F.R.D. at 276. That is exactly the case here. Google needs immediate discovery to identify the Doe Defendants and seek a preliminary injunction to stop the ongoing harm to it and the public from the widespread deceptive, infringing use of Google's marks. There is no prejudice to Defendants because this discovery will present "little interference with Defendant's business and any such interference will be shortened." *Sara Lee*, 2009 U.S. Dist. LEXIS 52648, at *4. Google therefore respectfully requests that the Court grant its *ex parte* application and enter an Order substantially in the form of the Proposed Order submitted herewith.

RESPECTFULLY SUBMITTED this 9th day of December, 2009.

HOLME ROBERTS & OWEN LLP

/s/ George M. Haley
George M. Haley, #1302
Blaine J. Benard, #5661
Craig Buschmann, #10696
Attorneys for Plaintiff Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on the 9th day of December, 2009, I caused a true and correct copy of the **Memorandum Of Law In Support Of *Ex Parte* Application For Leave To Take Immediate Discovery** to be served via :

Christian Larsen	_____ U.S. Mail, postage prepaid
President/Registered Agent	__X_ Hand Delivery
Pacific Webworks, Inc.	_____ Facsimile
230 West 400 South	_____ Overnight courier
Salt Lake City, UT 84101	_____ E-Mail and/or CM/ECF

By: /s/ Sherice L. Atterton