

of email addresses managed by PHP (and therefore available to receive spam), the fact remains that spammers are continuing to operate at an alarming pace and show no signs of abating in the near future. They will most certainly not stop unless lawsuits of this sort are afforded the time needed to complete the hard work necessary to obtain the real identity of those responsible.

The spam messages PHP has received all have one thing in common – they advertise a host of purported products and services being sold at thousands of different websites located on computers all over the world. Of the 10 million messages PHP has received to date, however, perhaps the most pernicious have been those advertising illegal online pharmacies. The John Does responsible for these pharmacy spam messages are little more than high-tech drug traffickers. They sell counterfeit or fake prescription drugs to unwitting consumers without the benefit of a reputable doctor’s prescription. They sell their drugs at prices typically well below those charged by brick and mortar drugstores that are managed by licensed pharmacists (who are closely regulated by state and federal authorities and who dispense authentic drugs tested and approved by the FDA).

The harm caused by these drug-trafficking spammers is real. A number of public reports in recent days have focused on the growing problem of pharmacy spam, the injuries traced to it, and the difficulties encountered by those who try to identify the killers behind the business.¹

Because of the dangerous nature of spam advertising illegal online pharmacies, PHP has focused its discovery to date on the John Does responsible for this type of spam. To

¹ *Pharmacists Warn of Buying Drugs Online After Death Reported*, [CBCNews.com](http://www.cbc.ca/canada/british-columbia/story/2007/03/21/drugs-online-warning.html), March 21, 2007 (available at <<http://www.cbc.ca/canada/british-columbia/story/2007/03/21/drugs-online-warning.html>>); *Spam Hunter*, [Forbes.com](http://www.forbes.com/business/free_forbes/2007/0723/054.html), July 23, 2007 (available at <http://www.forbes.com/business/free_forbes/2007/0723/054.html>) (profiling the unsuccessful attempts by the head of technology at a major spam-filtering company to track pharmacy spam to its source); and *Damn Spam: The Losing War on Junk Email*, [The New Yorker](http://www.newyorker.com/reporting/2007/08/06/070806fa_fact_specter), August 6, 2007 (available at <http://www.newyorker.com/reporting/2007/08/06/070806fa_fact_specter>) (noting negative trends in the long fight against spam).

date, we have issued nearly three dozen subpoenas to third parties that provided services of one form or another to the John Does. Our discovery has revealed many significant facts. We have identified over 10,000 different domain names appearing in spam that lead to online pharmacies operating under questionable circumstances. We have mapped those 10,000+ domain names to fewer than 200 specific Internet “fingerprints.”² Most importantly, nearly 90% of the domain names can be mapped to less than two dozen fingerprints, and approximately half of these fingerprints are connected to only one “hand”³ that represents over 50% of the entire online pharmacy spam problem today.

While the John Does behind nearly every one of these fingerprints are going to extreme lengths to hide their identity, nearly all of them remain vulnerable to identification through the use of civil discovery. All of the major fingerprints are using Visa credit card merchant accounts to process consumer purchases on their websites. In addition, nearly all of the fingerprints have other substantial connections to the United States, including the use of IP addresses, domain name registrars, telephone numbers, and email addresses that are serviced by United States-based entities.

While we have learned much about the individuals responsible for the advertising of illegal online pharmacies, our discovery has also encountered a number of roadblocks. Some were predictable, such as the use of stolen credit cards and Web Money⁴ to buy some services that are essential to the operation of their illegal online pharmacies. Other roadblocks were not anticipated. For example, several merchants that sold essential services to the John Does have

² A “fingerprint” consists of any set of data that is likely to uniquely define an online pharmacy operation, and that serves to distinguish it from other online pharmacy operations. The data we consider includes the domain name hosting the site, the look and feel of the site, the technical data underlying the site, and any data points about the site that we may acquire through subpoena or other investigative means.

³ A “hand” is a collection of fingerprints that are unique from each other, but have connections between them.

⁴ Web Money is a form of online currency that is operated by a company headquartered in Moscow (<http://www.wmtransfer.com/>).

refused to produce the John Does' payment information without a protective order in place. We hope to complete negotiations over such an order in the near future. Other third parties have failed to respond to our subpoenas, including a major credit card issuer that has failed to produce valuable merchant account information closely tied to the John Does. While we believe the bank will respond in time, a motion to compel may unfortunately prove necessary.

For all these reasons, PHP respectfully requests it be granted through November 26, 2007 to complete John Doe discovery and to name and serve defendants.

LEGAL ARGUMENT

Courts recognize that, in certain situations, the identity of a defendant may not be known prior to the filing of a complaint. In such circumstances, courts authorize a plaintiff to undertake discovery to identify the unknown defendant. In Gordon v. Leeke, 574 F.2d 1147, 1152 (4th Cir. 1978), the Fourth Circuit explained that, if a plaintiff states a meritorious claim against an unknown defendant, the Court should allow the plaintiff a "reasonable opportunity" to ascertain the identity of the unknown defendant through discovery. Paulinus Chidi Njoku v. Unknown Special Unit Staff, No. 99-7644, 2000 U.S. App. LEXIS 15695, at *2-3 (4th Cir. July 7, 2000) (remanding the case with instructions to afford plaintiff a "reasonable opportunity to properly identify" the John Does). This power is codified in Rule 26(d), which permits the Court to authorize discovery prior to the planning conference contemplated under Rule 26(f).

In addition to authorizing discovery necessary to identify and serve the John Doe defendants, PHP is also seeking an extension of its deadline to name and serve defendants under Rule 4(m). Federal Rule of Civil Procedure 4(m) provides that a plaintiff who shows good cause for failure to effectuate service within 120 days of filing the complaint is entitled to an appropriate extension of time to serve. Courts have held that good cause exists – and that a

plaintiff is entitled to additional time to effect service – when defendants take affirmative actions to avoid service of process. For example, in Ruiz-Varela v. Velez, the District Court dismissed the plaintiff's Complaint pursuant to Rule 4(m) for failure to serve Defendant Figueroa. 814 F.2d 821 (1st Cir. 1987). Recognizing that Figueroa was attempting to evade personal service by concealing his whereabouts, the First Circuit vacated the dismissal. Because Figueroa's attempts to conceal his location were designed to frustrate the plaintiff's ability to effectuate service, the Court of Appeals explained that dismissal for failure to serve was inappropriate: “Evasion of service by a putative defendant constitutes good cause for failure to serve under Rule 4[m].” *Id.* at 824. As noted above, the defendants in this case have gone to extreme measures to evade identification and service. Their attempts at evasion are an adequate basis for extending PHP's deadline to name and serve.

This Court should also grant PHP an extension of time to identify and serve the John Does due to its diligence in prosecuting this matter. Courts have consistently held that “a showing of diligence and a reasonable effort to effect service” constitute good cause under Federal Rule of Civil Procedure 4(m). In re Hall, 222 B.R. 275, 279 (Bankr. E.D. Va. 1998) (citing T & S Rentals v. United States, 164 F.R.D. 422, 426 (N.D. W.Va. 1996) and United States v. Britt, 170 F.R.D. 8, 10 (D. Md. 1996)). In determining the type of diligence or extent of effort required to warrant an extension of the 120-day deadline, courts have examined the legislative history of amendments to Rule 4, noting that: “Inadvertent or heedless non-service is what amended Rule 4[m] is aimed at. Congress intended that a plaintiff who had made reasonable efforts to effect service would be permitted additional time, if needed, under Rule 6(b).” Arroyo v. Wheat, 102 F.R.D. 516, 518 (D. Nev. 1984) (citing to cases in which “there was no dilatory or willful delay” and in which “plaintiff's abortive efforts [were] bona fide,” as

illustrative of situations in which “good cause” was determined to exist); see also Quann v. Whitegate-Edgewater, 112 F.R.D. 649, 659 (D. Md. 1986) (citing Arroyo v. Wheat).

PHP has subpoenaed nearly three dozen third parties in possession of information likely to lead to the identity of the John Doe defendants. This information has provided valuable leads into the identity of the defendants. PHP plans to continue its John Doe discovery, and also plans to communicate with other victims of these John Does in an effort to ensure its discovery does not inadvertently compromise other pending civil and criminal investigations. All of these reasons constitute good cause for an extension of the deadline to name and serve the John Doe Defendants.

WHEREFORE, for the foregoing reasons and any additional reasons that may be adduced on this matter, PHP respectfully asks the Court to grant this Request and enter an Order substantially in the form of the attached proposed Order.

Dated: August 30, 2007

Respectfully submitted,

/s/

Jon L. Praed
VSB #40678
Attorney for Plaintiff Project Honey Pot
Internet Law Group
4121 Wilson Boulevard, Suite 101
Arlington, Virginia 22203
Phone: (703) 243-8100
Fax: (703) 243-8162
jon.praed@i-lawgroup.com

