

pm

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FILED

MAY 14 2008
MAY 14 2008
Judge Robert M. Dow, Jr.
United States District Court

FEDERAL TRADE COMMISSION,)
)

Plaintiff,)

v.)

DATA BUSINESS SOLUTIONS INC., *et al.*,)

Defendants.)

08CV2783
JUDGE DOW
MAGISTRATE JUDGE DENLOW

**MEMORANDUM SUPPORTING PLAINTIFF'S *EX PARTE* MOTION FOR
TEMPORARY RESTRAINING ORDER WITH ASSET FREEZE AND OTHER
EQUITABLE RELIEF AND ORDER TO SHOW CAUSE WHY A PRELIMINARY
INJUNCTION SHOULD NOT ISSUE**

I. INTRODUCTION

The Federal Trade Commission ("FTC") asks this Court to bring an end to a scam that sends fake invoices to small businesses and non-profit organizations across the country. The fake invoices look like annual bills for the domain names of the consumers' Web sites. Consumers who respond and send money receive absolutely nothing in return.

The defendants in this case operate covertly out of Canada. The fake invoices and accompanying payment envelopes use a Chicago address that is simply a mail drop. The checks are then forwarded to another mail drop in the Toronto suburbs, where the defendants collect the money. This scam has been operating since at least 2004. We estimate that thousands of consumers have received these mailings and that the defendants have defrauded consumers out of millions of dollars. The Better Business Bureau ("BBB") in Chicago has received a large volume of complaints and has put the defendants on notice that these fake invoices are deceptive, yet the defendants continue to operate their scam and pocket consumers' money.

The defendants' mailings looks like typical invoices that consumers receive for existing accounts. These fake invoices consist of one two-sided sheet of paper and include information particular to the consumers' Internet Web sites, such as the consumers' current domain name or a "variant" domain names that is very similar to, and easily confused with, the consumer's

current domain name (e.g., "smallbusiness.net" instead of "smallbusiness.com"). The mailings list a customer, reference, or account number, and payment instructions with a due date. They also request payments ranging anywhere from \$35 to \$300. The mailings include a self-addressed payment envelope, as well.

Buried on the back of the invoice is a disclosure which states that the mailing is a solicitation, not a bill. It seems plain that this "disclosure" is in no way intended to cure the gross deception present in this case, but instead is nothing more than an effort to forestall the inevitable attention of law enforcement. The evidence shows that many consumers do not notice this language and make payments to the defendants under the false impression that they owe the company money for maintaining their domain name registrations. Of course, in many cases, those who pay the bills are not the same people that handle the Internet needs of the businesses, and therefore do not realize that these invoices are not from their actual domain name registrars. Moreover, the scam operates on volume and is still profitable even if some consumers do read carefully and do not pay. Those who mistakenly pay these fake invoices later receive "renewal notices" seeking more money. The "renewal notices" do not contain any disclosures at all.

The defendants' fake invoices also claim that they perform the related service of "search optimization" which supposedly prompts more people to visit the consumers' Web sites. The invoices say the defendants provide "domain name submission" to 20 or 25 "major search engines," the defendants' supposed method for providing search engine optimization services to their customers. Defendants' Web sites boast that their "search optimization" services will result in a substantial increase in traffic, even directing mass traffic, to consumers' Web sites. This is wholly false. According to Microsoft, the defendants' claimed method for providing "search optimization" will not produce effective results, let alone direct increased traffic to customers' Web sites.

The defendants' conduct violates the Federal Trade Commission Act ("FTC Act"), which prohibits unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45(a). The FTC asks this Court to enter a temporary restraining order ("TRO") bringing an immediate end to these deceptive practices and freezing the defendants' assets – including the checks that arrive every day at the Chicago mail drop – to preserve them so that money can be returned to victims at the conclusion of this proceeding.

II. THE PARTIES

A. The Federal Trade Commission

The FTC is an independent agency created by the FTC Act, 15 U.S.C. §§ 41-58. The FTC is charged with, *inter alia*, enforcement of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC is authorized to initiate proceedings in any United States District Court, by its own attorneys, to enjoin violations of the FTC Act, and to secure such equitable relief as may be appropriate in each case, including consumer redress and disgorgement of ill-gotten gains. 15 U.S.C. §§ 53(b), 57b.

B. Defendants

Defendant Data Business Solutions Inc., also d/b/a Internet Listing Service Corp., ILS Corp., ILSCORP.NET, Domain Listing Service Corp., DLS Corp., and DLSCORP.NET (“Internet Listing Service” collectively), is an Ontario corporation.¹ Since 2004, Internet Listing Service has concealed its actual location by maintaining mail drops in Chicago.² The corporate defendant has transacted business in the United States, including this district.

Ari Balabanian, Isaac Benlolo, and Kirk Mulveney are officers and/or principals of Internet Listing Service. Balabanian is the president, vice president of operations, and a director of Internet Listing Service.³ He is responsible for opening the mail drops in Chicago, where most consumers send their payments.⁴ Benlolo is a principal of Internet Listing Service. All of the mail received at the current Chicago mail drop, including customers’ payments, is shipped to Benlolo’s attention at another UPS store in Markham, Ontario.⁵ Benlolo has made payments on behalf of Internet Listing Service to its domain name registrar.⁶ Mulveney is also a principal of the company, serves as Internet Listing Service’s contact with its domain name registrar, and has

¹ PX 32 (Krause Dec. ¶¶ 4, 6, Atts. A, C).

² *Id.*; PX 24 (Uphus Dec. Att. B) (example of return envelope).

³ PX 32 (Krause Dec. ¶ 7, Att. D); PX 2, 3.

⁴ PX 32 (Krause Dec. ¶¶ 4, 6, Atts. A, C).

⁵ *Id.* at ¶ 4, Att. B.

⁶ *Id.* at ¶ 9, Atts. H, I.

made payments to its domain name registrar on behalf of the company.⁷ Mulveney is also listed as the registrant contact for many of the variant domain names that Internet Listing Service registered unbeknownst to consumers.⁸ All three individuals are actively involved in the corporation's business, and in the deceptive acts and practices alleged in the complaint.

III. DEFENDANTS' DECEPTIVE BUSINESS PRACTICES

Since at least August 2004, the defendants have been mailing fake invoices to consumers across the United States, defrauding thousands out of what is likely to amount to millions of dollars.⁹ Targeting primarily small businesses and not-for-profit organizations, the defendants' mailings are carefully crafted to look like bills from the consumers' current domain name providers (or their agents).¹⁰ Samples of the mailings are attached as Plaintiff's Exhibit 1.

Through their mailings, the defendants falsely claim that (1) the defendants have a preexisting relationship with the recipient; (2) consumers owe them money for maintaining registration of their domain names; (3) the defendants will provide continued registration of the consumer's current domain name; and (4) the defendants will provide "search optimization" services. All of these claims are completely false.¹¹

A. Defendants Misrepresent that There is a Preexisting Relationship

Defendants' fake invoices lead consumers to believe that they have a preexisting business relationship with defendants.¹² Listed at the top of the document's front page is either the consumer's own current domain name or a variant domain name - one that is very similar to, and easily confused with, the consumer's actual domain name.¹³ This is immediately followed by a

⁷ *Id.* at ¶ 9, Atts. F, G.

⁸ *Id.* at Att. F.

⁹ *Id.* at ¶ 4, Att. A; PX 5-21 (consumers received mailings between Dec. 2004-Jan. 2008).

¹⁰ PX 23 (Stephan Dec. ¶¶ 5, 11); *see also* PX 5, 7-10, 12-14, 16-20, 22, 25, 26 (same).

¹¹ PX 5-26 (never received any services).

¹² PX 27 (Jodlowska (BBB) Dec. ¶ 8); PX 20 (Parsons Dec. ¶ 10); PX 10, 12, 13, 16, 17, 25, 26.

¹³ *See, e.g.*, PX 12 (Held Dec. ¶ 12) (variant domain name); PX 7, 8, 10, 19, 26 (variant domain names); PX 9 (Fetzer Dec. ¶ 3, Atts. A, C) (consumer's actual domain name listed).

specific number, comprised of two letters followed by between seven and nine numbers, that is referred to as an “Account Number,” “Customer Number,” or “Reference Number.” Use of this individualized account number, along with information particular to the consumer’s Internet Web site, suggests that the consumer is an existing customer. *See FTC v. Cyberspace.com LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006). Thus, these fake invoices directly imply a prior or ongoing business relationship, and consumer complaints and declarations establish that this is the impression with which most consumer victims are left.

In the middle of the back page of the fake invoice, there is a disclaimer which states “THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO PAY THE AMOUNT STATED ABOVE UNLESS YOU ACCEPT THIS OFFER.” This disclosure is insufficient to cure the deception caused by the overall net impression that the document is an invoice.¹⁴ Furthermore, the FTC has had experience with similar scams and the Ninth Circuit has found that a disclosure alone does not negate other factors that mislead consumers about the sender’s intention.¹⁵ As discussed more fully in Section IV.B.1 below, this single disclosure is insufficient to cure the deception created by the overall impression that the mailing is an invoice.

After consumers make the initial payment to the defendants, they receive subsequent “renewal notices”¹⁶ or e-mails¹⁷ each year requesting additional payments. These later mailings do not contain the disclosure that is printed in the original mailing.¹⁸

B. Defendants Misrepresent that Consumers Owe Money

Defendants’ fake invoices request payments ranging from \$35 to \$75, with package prices of up to \$300 that supposedly offer the “best value.”¹⁹ Most of the defendants’ mailing is devoted

¹⁴ PX 8, 10, 13, 17, 23, 25 (does not remember seeing disclosure).

¹⁵ In *Cyberspace.com*, 453 F.3d at 1198, 1201, the Ninth Circuit held that various elements, including the use of an invoice and account number, suggested the existence of a preexisting business relationship despite disclosures to the contrary on both the invoices and the checks.

¹⁶ PX 5, 8-10, 12, 15, 20, 21 (consumers received renewals and/or final notices).

¹⁷ PX 16, 22, 24 (received e-mail that resembled invoice and requested a renewal payment).

¹⁸ PX 10 (Fowler-Trinchera Dec. ¶ 12, Att. C, D, G); PX 9 (Fetzer Dec. ¶ 8, Att. C).

¹⁹ PX 5-26 (various amounts); *see also* PX 19 (Nilsson Dec. Att. C) (\$300 for 5 years of service).

to addressing payment - leaving consumers with the impression that they owe the defendants the amount requested. The mailing is a one-page document, with text on both sides, that looks like a bill and even includes a perforated bottom, to be torn off and returned with the consumer's payment, and a self-addressed payment envelope.²⁰ The text on the front page includes bold headings like "HOW TO MAKE PAYMENT" and "PAYMENT INFORMATION," along with the particulars. The terms "payment" or "payable" are employed seven times on the front page of the document alone. The front page even includes a "pay by" date.²¹

Of course consumers believe that the payment they are asked to make is needed in order to keep active their current domain names.²² The mailing identifies the services for which consumers are being billed as "WEBSITE ADDRESS LISTING." This heading itself suggests that the services relate to the registration of the consumer's current domain name, which is listed at the top of the invoice. The names Internet Listing Service and Domain Listing Service likewise suggest that the company provides domain name registration services.

C. Defendants Misrepresent that They will Provide Continued Registration of the Consumer's Current Domain Name

The defendants are not the consumers' current providers, nor do consumers owe them money for the continued registration of their domain names. These consumers already have domain names and do not need to obtain them from the defendants. To add insult to injury, some consumers not only lose money after paying the defendants, but also lose their Web sites because they fail to pay their current providers and their current registrations lapse.²³

Most consumers who make payments to the defendants do not receive any domain name registration services whatsoever from the defendants.²⁴ Only in extremely rare instances, when

²⁰ Examples of mailings at PX 1. *See also* PX 9, 13 (Fetzer Dec. ¶ 3).

²¹ PX 20 (Parsons Dec. ¶¶ 4, 10).

²² PX 8 (Davis Dec. ¶ 4) (mailing "had a sense of urgency"); PX 5, 9, 14, 17, 18, 20, 26 (mailing gave impression that they had to pay to renew their Web site service).

²³ PX 20 (Parsons Dec. ¶¶ 6-8, 11) (lost domain name).

²⁴ PX 21 (Schetrompt Dec. ¶ 8); PX 8 (Davis Dec. ¶ 10); PX 6, 7, 10, 12-14, 18-20, 22, 23, 25 (received no services).

consumers contact the defendants via e-mail, does the company even offer to provide such services.²⁵

Curiously, defendants began registering some variant domain names in November 2006, over two years after they began operating. But those registrations are worthless to consumers. First, consumers who have these variant domain names registered never even know that these new domain names exist. Consumers have only made payments to defendants because they mistook these domain names to be their own due to the confusing similarities in the domain names. In fact, many consumers do not realize that they have been mistakenly paying for these variant domain names for years.²⁶ Moreover, even in the unlikely event that consumers did know about these variant domain names, they hold no rights to the domain names, nor do they have the ability to access and utilize them. This is because the domain names do not belong to the consumers; instead, the defendants hold the rights to them.²⁷ Thus, registering these variant domain names does not benefit the consumer victims.

D. Defendants' Misrepresent that They will Provide "Search Optimization"

Although consumers typically make payments to the defendants because they believe that they are being billed by their actual domain name registration provider, a small subset of consumers make payments to the defendants solely for the supposed "search optimization" services mentioned in the fake invoices.²⁸ The defendants' mailing indicates that the service "INCLUDES . . . domain name submission" to 20 or 25 "major search engines." Consumers understand this to be search engine optimization services.²⁹ The defendants' Web sites further boast that by submitting customers' Web sites to search engines like Google, Yahoo, MSN, and

²⁵ PX 31 (Long Dec. ¶ 7).

²⁶ PX 12 (Held Dec. ¶ 12); PX 7, 8, 19 (same); PX 10 (Fowler-Trinchera Dec. ¶¶ 11-14).

²⁷ Only a domain name's registrant is given the password and username information needed to access the web page. As the registrant, defendants could have licensed the use of the domain name, but they did not take any of the necessary steps to do so. PX 28 (Pritz (ICANN) ¶ 6 (registrant holds exclusive rights to domain name unless the registrant licenses the domain name and provides the correct contact information to ICANN); PX 30 (Christiansen (Wild West) Dec. ¶ 4).

²⁸ PX 21 (Schetrompt Dec. ¶ 3); PX 6 (Bosse Dec. ¶ 6).

²⁹ *Id.*

others four times a year, their “proven . . . Search Optimization” services will “substantially increase” and direct “mass traffic” to consumers’ Web sites to help them “reach an enormously larger viewing population than ever before.”³⁰ Some mailings also promise to provide periodic “search engine position and ranking” reports as well.³¹

According to Microsoft, however, defendants’ supposed method for providing search engine optimization services is ineffective. The only truly effective search engine optimization services are more involved than just submitting domain names and keywords to search engines, and require editing the HTML code and the actual content of the Web site.³² The defendants do not claim to do either of these things, and there is no indication that they have ever done so. Therefore, defendants’ claims to provide “search optimization” that will substantially increase and direct mass traffic to consumers’ Web sites are false.³³

Not surprisingly, consumers who paid defendants in the hopes of increasing traffic to their Web sites noticed no difference in the number of hits on their sites.³⁴ Moreover, customers who were told they would receive “quarterly search engine position and ranking reports” did not receive any such reports.³⁵

E. Consumers’ Unnecessary Payments and Difficulties Obtaining Refunds

Many consumers fail to realize that they have been making unnecessary payments to the defendants, in many cases for years. But even for consumers who figure out that they have been scammed, the defendants have made it very difficult to obtain refunds. Consumers are typically unable to find a telephone number for the company³⁶ and those who have tried to e-mail the

³⁰ See, e.g., PX 21 (Schetrompt Dec. Att. A); PX 29 (Grote (Microsoft) Dec., Atts. A, B).

³¹ PX 21 (Schetrompt Dec. ¶¶ 3) (mailing promised quarterly reports).

³² PX 29 (Grote (Microsoft) Dec. ¶ 5).

³³ Although it also appears that defendants have created “link pages” that list Web sites, Microsoft’s review of those pages has confirmed that such pages are also unlikely to change a site’s search engine ranking. PX 29 (Grote (Microsoft) Dec. ¶ 7).

³⁴ PX 21 (Schetrompt Dec. ¶¶ 4, 8); PX 24 (Uphus Dec. ¶ 12); PX 6 (Bosse Dec. ¶¶ 8-11).

³⁵ PX 21, 23 (did not receive any quarterly reports).

³⁶ PX 8, 17, 23, 25, 26 (could not find any contact information).

company sometimes received messages back stating that the e-mail address is no longer active or their e-mail attempt failed “because the user’s mailfolder is full.”³⁷ When consumers did manage to communicate with the company’s representative, they report that they usually had to make numerous requests before receiving a refund.³⁸ Some consumers only receive partial refunds.³⁹ When the BBB contacted the company about consumer complaints, the responses it received were “short, fragmented, and [did] not address the core issues of deception raised in consumers’ complaints.”⁴⁰ Some consumers became so frustrated with the whole process that they eventually gave up or put stop payments on their checks to defendants, thus incurring fees from their banks.⁴¹ The FTC has submitted the declarations of twenty-two representative consumers who were misled into sending money to defendants.⁴²

IV. ARGUMENT

The FTC seeks injunctive relief to prevent further illegal conduct pending final resolution of this case. The FTC also seeks an asset freeze and an accounting to preserve the possibility of effective final relief. As discussed below, this Court has full authority to enter the relief sought by the FTC, and the facts strongly support such relief.

A. This Court Has the Authority to Grant the Relief Requested

A district court may issue injunctions to enjoin violations of the FTC Act. *See* 15 U.S.C. 53(b); *FTC v. Febre*, 128 F.3d 530, 534 (7th Cir. 1997); *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1028 (7th Cir. 1988). Implicit in the Court’s authority to grant injunctions is the power to grant “any ancillary equitable relief necessary to effectuate the exercise of the granted powers.” *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 572 (7th Cir. 1989). Such ancillary relief includes, *inter alia*, rescission of contracts, restitution, disgorgement, freezing of

³⁷ PX 16 (Johnson Dec. ¶ 6); PX 25 (Uwagbale Dec. ¶ 11) (mail box full).

³⁸ PX 14 (Holine Dec. ¶¶ 7, 8); PX 16 (Johnson Dec. ¶¶ 7, 8); PX 24 (Uphus Dec. ¶ 7); PX 5 (Baum Dec. ¶ 7); PX 18 (Lehman Dec. ¶ 5, Att. A); PX 16 (Johnson Dec. ¶ 7).

³⁹ PX 20 (Parsons Dec. ¶¶ 9, 12).

⁴⁰ PX 27 (Jodlowska (BBB) Dec. ¶ 14).

⁴¹ PX 8, 18, 26.

⁴² *See* PX 5-26.

assets, and the appointment of a receiver. *See, e.g., Febre*, 128 F.3d at 534 (court has power to order redress as restitution or rescission); *World Travel*, 861 F.2d at 1026, 1031 (asset freeze appropriate); *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1102-03 (9th Cir. 1994) (restitution and disgorgement appropriate); *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1432 (11th Cir. 1984) (asset freeze and appointment of receiver appropriate under § 13(b)). Courts appropriately invoke the remedies of Section 13(b) in cases involving fraud. *World Travel*, 861 F.2d at 1024-28; *FTC v. H. N. Singer, Inc.*, 668 F.2d 1107, 1111 (9th Cir. 1982).⁴³

B. The FTC Is Overwhelmingly Likely to Prevail on the Merits

The evidence submitted in support of the FTC's motion for a TRO and Preliminary Injunction establishes an overwhelming likelihood that the FTC can prove that the defendants have violated the FTC Act.

1. Defendants have violated Section 5 of the FTC Act

The defendants' false claims about their services are "deceptive acts or practices" prohibited by Section 5 of the FTC Act. *See* 15 U.S.C. § 45(a). The FTC can establish liability under Section 5 of the FTC Act by demonstrating "material representations likely to mislead a reasonable consumer." *FTC v. Bay Area Bus. Council, Inc.*, 423 F.3d 627, 635 (7th Cir. 2005); *see also FTC v. QT, Inc.*, 448 F. Supp. 2d 908, 957 (N.D. Ill. 2006). The FTC is not required to prove intent to deceive. *Bay Area*, 423 F.3d at 635. The FTC may demonstrate the deceptive nature of advertising claims by either: (1) demonstrating the falsity of the claims; or (2) showing that the defendant lacked a reasonable basis for making the claims, *i.e.*, "substantiation." *See, e.g., QT, Inc.*, 448 F. Supp. 2d at 958-59; *FTC v. Sabal*, 32 F. Supp. 2d 1004, 1007 (N.D. Ill. 1998). Moreover, in deciding whether particular statements or omissions are deceptive, courts must look to the "net impression" of consumers. *See Kraft, Inc. v. FTC*, 970 F.2d 311, 314 (7th Cir. 1992), *cert. denied*, 507 U.S. 909 (1993); *Cyberspace.com* 453 F.3d at 1200; *FTC v. Gill*, 265 F.3d 944, 956 (9th Cir. 2001); *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 993, 1010 (N.D. Ind. 2000), *aff'd*, 312 F.3d 259 (7th Cir.); *FTC v. U.S. Sales Corp.*, 785 F. Supp. 737, 745 (N.D. Ill. 1992).

⁴³ Courts in this district regularly enter TROs in FTC fraud cases. *See, e.g., FTC v. Spear Systems, Inc., et al.*, 07 C 5597 (N.D. Ill. Oct. 3, 2007); *FTC v. Sili Neutraceuticals, LLC*, 07 D 4541 (N.D. Ill. Aug. 13, 2007); *FTC v. 120194 Canada, Ltd., et al.*, 04 C 7204 (N.D. Ill. Nov. 8, 2004).