

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

RECEIVED

FEB 28 2002

MICHAEL J. ...
CLERK, U.S. DISTRICT COURT

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

TLD NETWORK LTD., QUANTUM
MANAGEMENT (GB) LTD., TBS
INDUSTRIES LTD., THOMAS GOOLNIK, and
EDWARD HARRIS GOOLNIK, individually,
and as officers of the above companies.

Defendants.

Case No.

020 1475

JUDGE HOLDERMAN

MAGISTRATE JUDGE ASHMAN

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

I. INTRODUCTION

This matter involves straightforward Internet fraud. Defendants sell Internet domain names that do not work, and almost assuredly will never be usable, over the Internet.¹ Defendants send unsolicited email ("spam") falsely claiming that their domain names, ending in suffixes such as ".usa" and ".sex," work like recognized existing domain names with suffixes like ".com." Defendants sell their domain names on professional looking Web sites that conceal the deficiencies of the domain names. We ask that the Court bring this scam to an immediate end.

¹ Domain names assist Internet users to find Web sites and communicate via email. (See PX 11 ¶ 3.) For example, the domain name of the Federal Trade Commission - "ftc.gov" - is used to identify the FTC's Web site, www.ftc.gov, and email to the FTC is directed to "person@ftc.gov."

Defendants have cheated thousands of consumers out of a large amount of money, likely more than \$1 million, during the eight months they have operated this scheme. Since the September 11th terrorist events, Defendants have aggressively hawked their ".usa" domain names, apparently attempting to capitalize on the public's desire to show its patriotism. Consumers who have purchased the domain names for \$59 each, however, have not been able to use them. Defendants, who are located in the United Kingdom, then hide their whereabouts from consumers, making it nearly impossible for consumers to get refunds from Defendants.

Plaintiff Federal Trade Commission ("FTC") brings this action pursuant to the FTC Act, 15 U.S.C. §§ 45(a), 53(b), seeking to immediately enjoin Defendants' deceptive practices. Plaintiff seeks an *ex parte* temporary restraining order temporarily disabling Defendants' Web sites. Absent this relief, Defendants may transfer their Internet operation entirely overseas, depriving the Court of jurisdiction to grant effective final relief. Plaintiff also seeks an asset freeze to preserve the possibility of redress for victimized consumers.

II. DEFENDANTS

Defendants are a common enterprise of three private limited companies organized under the laws of the United Kingdom, plus the two principals who control those companies. The three companies – TLD Network Limited, Quantum Management (GB) Limited and TBS Industries Limited – have each operated Internet Web sites that sell the fraudulent domain names at issue in this matter. (*See* PX 12 ¶¶ 7, 9, Atts. D, E; PX 13 ¶¶ 6-9, Atts. E-H.) These companies are registered to the same address in London. (*See* PX 13 ¶ 4, Atts. A-C.)

Thomas Goolnik is a director of each of the above companies. (*See id.*) Edward Goolnik is a director of TLD Network and the secretary of Quantum Management. (*See id.*) Thomas

Goolnik has personally purchased domain names used to operate Defendants' Web sites that advertise the fraudulent domain names at issue. (See PX 13 ¶¶ 6, 8, 9, Atts. E, G, H.) Both Goolniks, as directors of TBS, were investigated in 1997 and 1998 by British authorities for deceptively marketing a radar detector that supposedly rendered cars "totally invisible to all major speed traps." (See PX 14.) TBS entered a "guilty" plea for false advertising and paid a £3000 fine. (*Id.*)

III. JURISDICTION AND VENUE

This matter is properly before the Court. Defendants are subject to personal jurisdiction. Defendants, based in the U.K., are amenable to process pursuant to Fed. R. Civ. P. 4(k)(1)(D) because the FTC Act provides for nationwide and extraterritorial service. See 15 U.S.C. § 53(b) ("In any suit under this section, process may be served on any person, partnership, or corporation wherever it may be found."). "Where a federal statute provides for nationwide service of process, personal jurisdiction may be obtained over any defendant having minimum contacts with the United States as a whole." *Morris v. Martino*, 1995 WL 347947, at *2 n. 4 (N.D. Ill. June 8, 1995). See also *United Rope Distributors v. Seatriumph Marine*, 930 F.2d 532, 534 (7th Cir. 1991). Here, Defendants clearly possess sufficient contacts with the United States. Among other things, Defendants have: (1) advertised their domain names to United States consumers via email solicitations and Internet Web sites accessible in the United States (*see* PX 1-6, 8-10); (2) sold domain names to numerous consumers in the United States (*see id.*); (3) contracted with U.S. companies (*see* PX 13 ¶¶ 6-9, Atts. E-H); and (4) opened a postal mailbox in the United States (*see id.* ¶ 10, Att. I).

This Court also has subject matter over this case, and venue is proper. The Court has subject matter jurisdiction over the FTC Act claims pursuant to 28 U.S.C. §§ 1331, 1337(a) & 1345. Finally, venue is proper pursuant to 28 U.S.C. § 1391(d) which provides that "[a]n alien may be sued in any district." *See also* 15 U.S.C. § 53(b) ("Any suit may be brought [under FTC Act] where such person, partnership, or corporation resides or transacts business, or wherever venue is proper under section 1391 of Title 28.").

IV. DEFENDANTS' DECEPTIVE BUSINESS PRACTICES

Defendants have sold thousands of domain names that do not work, and almost assuredly will never be usable, over the Internet. In order to understand why the domain names the Defendants are selling do not work, it is necessary to know a bit about the nature of domain names and the Internet. Domain names are essentially Internet addresses; they help users find their way around the Internet. Among other things, domain names are used to identify Internet Web sites and email addresses. (*See* PX 11 ¶ 3.) A typical domain name contains the name of the entity followed by a suffix (*e.g.*, ftc.gov). The suffix is referred to as the top-level domain name. (*Id.* ¶ 4.) Each domain name is unique, and they are kept in a computer system that is, in essence, a huge address book. (*Id.* ¶ 5.)

The entity responsible for managing and coordinating the domain name system is the Internet Corporation for Assigned Names and Numbers (ICANN), a U.S. non-profit corporation. (*Id.* ¶ 2.) ICANN oversees and coordinates the distribution of domain names to ensure that there are not duplicate addresses. (*Id.* ¶ 3.) ICANN has approved a limited number of generic top-level domains, including ".com," ".net" and ".org." (*Id.* ¶ 4.) In November 2000, ICANN selected seven new top-level domains – ".aero," ".biz," ".coop," ".info," ".museum," ".name,"

and “.pro” – placing them in the domain names system. (*Id.*) ICANN also has approved various country code top-level domains, including “.us” for the United States. (*Id.*)

ICANN also runs the domain name registration system by accrediting domain name registrars who are authorized to sell and register domain names. (*Id.* ¶ 8.) Loosely speaking, registration of a domain name with one of these registrars places the domain name in the domain name system’s “address book.” (*Id.*) Once in the “book,” an individual can utilize the domain name as an Internet address for a Web site or email. (*Id.* ¶¶ 3, 8.)

A. Defendants Sell Domain Names That Do Not Work As Represented

The domain names that Defendants sell are not part of the global domain name system described above. Since approximately July 2001, consumers have been receiving spam advertising domain names with suffixes such as “.usa,” “.sex,” “.brit,” “.scot,” “.bet,” “.store,” and “.isp.” (*See* PX 1 ¶ 2; PX 3 ¶ 8, Att. A; PX 4 ¶ 2; PX 5 ¶ 2, Att. A; PX 6 ¶ 2, Att. A; PX 7 ¶ 2, Att. A; PX 8 ¶ 2, Att. A; PX 10 ¶ 2, Att. A.)

Since the terrorist events of September 11th, the spam has often contained a subject line like “Be patriotic! Register .USA Domains!” or “God Bless America! .USA Domains!” The body of one recent email stated:

The latest domain name extension has arrived .USA!!! It's the fresh, new, exciting web address that is taking the world by storm. Who wants to be .com when you can now be .USA. Register your .USA domain name today exclusively at: <http://www.dotusa.com>

(PX 10 ¶ 2, Att. A; PX 3 ¶ 2, Att. A.) Defendants’ spam lead consumers to believe that the domain names being sold can be used, or will soon be usable over the Internet, like domain names with the “.com” extension. (*See* PX 6 ¶ 2; PX 7 ¶ 2; PX 8 ¶ 2; PX 10 ¶ 2.)

Defendants operate professionally designed Web sites that can be visited by clicking the link contained in Defendants' spam. Defendants' Web sites are similar to sites of legitimate registrars that sell ICANN-accredited domain names. (See PX 1 ¶ 3; PX 2 ¶ 2; PX 5 ¶ 3; PX 6 ¶ 3; PX 7 ¶ 3; PX 9 ¶ 3; PX 10 ¶ 3.)² The Web sites sell the domain names for \$59 each and accept various credit cards. (See PX 12 ¶¶ 3, 5, Atts. A, B.) The Web sites assert that Defendants are the "worldwide provider of web addresses" ending in the various suffixes, including ".usa" and ".sex," and assert that individuals who register domain names with Defendants will be "one of the first to profit from the next generation of Internet wealth" by "creat[ing] your own web presence." (See *id.*) Consumers who have viewed Defendants' Web sites, including many with previous experience purchasing domain names, believe that the domain names being sold can be used, or will soon be usable, over the Internet like domain names with the ".com" extension. (See PX 1 ¶ 3; PX 2 ¶ 2; PX 4 ¶ 3; PX 5 ¶ 3; PX 6 ¶ 3; PX 7 ¶ 3; PX 9 ¶ 3; PX 10 ¶ 3.)

Many consumers have purchased Defendants' domain names based on the representations made in Defendants' emails and Web sites. (See PX 1 ¶¶ 3-4; PX 2 ¶¶ 2-3; PX 4 ¶¶ 3-4; PX 5 ¶¶ 3-4; PX 6 ¶¶ 3-4; PX 7 ¶¶ 3-4; PX 9 ¶¶ 3-4; PX 10 ¶¶ 3-4.) However, those representations are false. The domain names sold by Defendants are not recognized by ICANN as part of the global domain name system, and Defendants are not ICANN-accredited domain registrars. (See PX 11 ¶¶ 10-11.) Defendants' domain names are not presently, and may never be, usable

² These Web sites – www.dotusa.com, www.dotsex.com, www.dotbrit.com, www.dotscot.com, www.dotsexregistrar.com, www.dotstore.com, www.dotisp.com, and www.tldnetworks.com – can be viewed on the Internet. Printed downloads and electronic versions of Defendants' Web sites are also attached to PX 12, Atts. A, B.

over the Internet in the same way that “.com” domain names are presently usable. (*See id.* ¶ 10.) Thus, a Web site or email address utilizing Defendants’ domain names would not be reachable by most, if any, Internet users. (*Id.*)³ Indeed, consumers who have bought Defendants’ domain names have found the domain names to be completely unusable. (*See* PX 1 ¶ 8; PX 2 ¶ 6; PX 3 ¶ 7; PX 4 ¶ 11; PX 6 ¶ 8; PX 7 ¶ 6; PX 10 ¶ 7.)

B. Defendants Hide Their Whereabouts From Consumers

After purchasing Defendants’ domain names, consumers have found it nearly impossible to contact Defendants. For starters, Defendants’ Web sites do not have a phone number. (*See* PX 12 ¶¶ 3-5, Att. A, B; PX 5 ¶¶ 3, 6, Att. B.) Although Defendants’ Web sites contain email addresses and state on their contact page that they “respond promptly to all enquiries, usually within 24hrs,” most consumers never receive a response to their email inquiries. (*See* PX 1 ¶ 6; PX 3 ¶ 6; PX 4 ¶ 5, Att. B; PX 5 ¶ 7; PX 6 ¶ 6, Att. B; PX 7 ¶ 5; PX 8 ¶ 4; PX 9 ¶ 7.) At one point, Defendants’ Web sites listed the “corporate office” as 537 Newport Center Drive, Newport Beach, California. (*See* PX 4 ¶ 7; PX 5 ¶¶ 3, 6, Att. B; PX 12 ¶ 8, Att. B.) However, this address is only a mail drop (*see* PX 13 ¶ 10, Att. I), and, according to the Better Business Bureau, mail is returned from this address as undeliverable (*see id.* ¶ 12, Att. K). Other contact information Defendants provided to Internet registries also has turned out to be false. (*See* PX 4 ¶¶ 6-7; PX 7 ¶ 5; PX 13 ¶ 11, Att. J.) Over 100 confused consumers have contacted ICANN expressing concern about the legitimacy of Defendants’ business practices. (*See* PX 11 ¶ 9.)

³ Tellingly, Defendants’ Web sites do not even utilize their own domain names.

C. Defendants Are Causing Enormous Consumer Injury

Defendants appear to be causing over \$100,000 per month in consumer injury.

According to information obtained from Visa, Defendants have charged almost \$400,000 in Visa credit card transactions alone in the last eight months. (*See* PX 13 ¶ 5, Att. D.) Since Visa accounts for only about half of the credit card market and Defendants accept other credit cards, as well as debit cards, sales likely have exceeded \$1 million. In some instances, consumers have registered multiple domain names and incurred charges ranging from hundreds to thousands of dollars. (*See* PX 1 ¶ 7 (charged over \$15,000); PX 2 ¶ 3, Att. B (charged approximately \$4,000); PX 5 ¶ 4 (purchased approximately \$600); PX 6 ¶ 7 (charged over \$400).)

Consumers have charged back over 10% of their Visa transactions with Defendants using the credit card dispute resolution process, an amount that is over 20 times the average charge back level for Visa's e-commerce merchants.⁴ Other consumers who are still in the dispute resolution process have canceled their credit cards. (*See* PX 1 ¶ 7; PX 2 ¶ 5, PX 4 ¶ 8; PX 5 ¶ 8; PX 6 ¶ 7; PX 8 ¶ 6.) Despite the tremendous amount of visible consumer dissatisfaction, many consumers have probably not complained because Defendants have led them to believe that Defendants' domain names will soon become usable like ".com" domain names. Moreover, Defendants are undoubtedly deceiving new consumers every day.

V. ARGUMENT

We ask that the Court enter an order that enjoins further deceptive claims and that temporarily disables Defendants' Web sites. We also request that the Court freeze assets to

⁴ In 1999, Visa estimated its average charge back level for e-commerce merchants to be .54 percent. *See FTC v. Crescent Publishing Group, Inc.*, 129 F. Supp. 311, 316 (S.D.N.Y. 2001).

preserve the possibility of restitution at the conclusion of this case. As discussed below, this Court has full authority to enter the relief sought by Plaintiff, and the facts strongly support such relief.

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

Section 13(b) of the FTC Act, 15 U.S.C. 53(b), provides that “in proper cases the [FTC] may seek, and after proper proof, the court may issue, a permanent injunction.” Matters involving false and deceptive advertising are “proper cases” for injunctive relief under the FTC Act. *See FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1026, 1028 (7th Cir. 1988). Moreover, “[t]he district court’s authority [under the FTC Act] to grant a permanent injunction also includes the power to grant other ancillary relief sought by the Commission” and “order any ancillary equitable relief necessary to effectuate the exercise of the granted powers.” *FTC v. Febre*, 128 F.3d 530, 534 (7th Cir. 1997).

B. This Court Should Immediately Issue a Temporary Restraining Order and Other Appropriate Equitable Relief

The injunctive relief requested by the FTC is warranted in this case. Section 13(b) of the FTC Act authorizes injunctive relief “[u]pon a proper showing that, weighing the equities and considering the FTC’s likelihood of ultimate success, such action would be in the public interest.” Unlike litigation between private parties, “it is not necessary for the FTC to demonstrate irreparable injury” under the FTC Act. *World Travel*, 861 F.2d at 1029. Instead, to determine whether to grant equitable relief under the FTC Act, the court must merely: (1) determine the likelihood that the FTC will ultimately succeed on the merits and (2) balance the equities. *Id.* As demonstrated below, the FTC has more than satisfied this standard here.

1. There Is A Substantial Likelihood That the FTC Will Prevail on the Merits

Defendants are engaging in “deceptive acts or practices” in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). “[M]isrepresentations of material facts made for the purpose of inducing consumers to purchase services constitute . . . deceptive acts or practices forbidden by Section 5(a).” *World Travel*, 861 F.2d at 1029. Moreover, “the omission of material information, even if an advertisement does not contain falsehoods, may cause the advertisement to violate Section 5.” *Id.* The “misrepresentation or practice need not be made with an intent to deceive;” instead, the FTC need merely establish that “the representations, omissions, or practices likely would mislead consumers, acting reasonably, to their detriment.” *Id.*

Here, as described above in § IV of this brief, Defendants have consistently made material representations and omissions about the usability of the domain names that they sell. The central promotional claim in, and the net impression taken from, Defendants’ email solicitations and Web sites – namely, that the domain names they sell can be used like “.com” domain names to create a Web presence – is false. Defendants are not ICANN-accredited domain registrars, and their domain names are not part of ICANN’s global domain name system. (*See* PX 11 ¶¶ 10-11.) This means that a Web site or email address utilizing Defendants’ domain names would not be reachable by most, if any, Internet users. (*Id.* ¶ 10.)

Defendants’ deception is not only “likely” to mislead consumers it already has caused substantial consumer harm by misleading consumers into believing that the domain names promoted by Defendants work like domain names with the more familiar “.com” extension. (*See* PX 1 ¶¶ 3-4; PX 2 ¶¶ 2-3; PX 4 ¶¶ 3-4; PX 5 ¶¶ 3-4; PX 6 ¶¶ 3-4; PX 7 ¶¶ 3-4; PX 9 ¶¶ 3-4; PX

10 ¶¶ 3-4.) Defendants' representations and omissions are "material" because they are likely to affect, and indeed have affected, consumers decisions to purchase Defendants' deficient domain names. In short, consumers simply would not purchase Defendants' domain names if Defendants had disclosed that those domain names do not function like existing recognized domain names. (See PX 1 ¶ 8; PX 2 ¶ 6; PX 3 ¶ 5; PX 6 ¶ 8; PX 7 ¶ 6; PX 8 ¶ 7; PX 9 ¶ 9; PX 10 ¶ 7.)

2. Provisional Relief is in the Public Interest

The balance of equities also strongly tips in the FTC's favor here. In deciding whether to grant injunctive relief, the Court must balance the equities, assigning greater weight to the public interest advanced by the FTC than to any of Defendants' private concerns. *World Travel*, 861 F.2d at 1029. In this case, immediate injunctive relief is necessary to protect the public from the future financial harm that will inevitably result from Defendants' deceptive practices. In contrast, Defendants have no legitimate interest to balance against the need for an injunction. The FTC's proposed temporary restraining order only restrains Defendants from engaging in illegal conduct. Such a restriction does not work an undue hardship on Defendants, for they have no legitimate interest in persisting with conduct that violates federal law. *See, e.g., FTC v. World Wide Factors*, 882 F.2d 344, 347 (7th Cir. 1989) (upholding district court finding of "no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation or preserve their assets from dissipation or concealment"); *FTC v. Sabal*, 32 F. Supp. 2d 1004, 1009 (N.D. Ill. 1998).

3. **The Goolniks Are Individually Liable for Injunctive and Monetary Relief**

The Goolniks are the perpetrators of this illicit scheme and are individually liable for the violations of the FTC Act described above. An individual may be held liable for violations of the FTC Act if the court finds that the individual: (1) actively participated in or had authority to control the deceptive practices, and (2) had or should have had knowledge or awareness of the practices. *See Amy Travel*, 875 F.2d at 573-74; *FTC v. Febre*, No. 94 C 3625, 1996 WL 396117, *8 (N.D. Ill. July 3, 1996). Authority to control can be evidenced by “active involvement in business affairs and the making of corporate policy, including assuming the duties of a corporate officer.” *Amy Travel*, 875 F.2d at 573. In addition, the “degree of participation in business affairs is probative of knowledge.” *Id.* at 574.

Thomas Goolnik and Edward Harris Goolnik have the authority to control the acts and practices of the companies and were clearly aware of the deceptive practices at issue here. As described in § II above, Thomas Goolnik is a director of each of the defendant companies. He also personally purchased Internet domain names through which Defendants deceptively advertised their domain names. Edward Goolnik is a director of TLD Network and the secretary of Quantum Management. Both Goolniks are therefore in positions to control the practices of these closely held entities, and, as a result of their intimate involvement with the companies, each had reason to know of their companies’ deceptive practices. *See, e.g., FTC v. Publishing Clearing House, Inc.*, 104 F.3d 1168, 1170-71 (9th Cir. 1997) (individual’s status as corporate officer and authority to sign documents on behalf of corporate defendant sufficient to demonstrate control); *FTC v. Growth Plus Int’l Marketing, Inc.*, No. 00 C 7886, 2001 WL

128139, at *3 (N.D. Ill. Jan. 9, 2001) (defendants' corporate roles demonstrated knowledge); *FTC v. Windermere Big Win Int'l, Inc.*, No. 98 C 8066, 1999 WL 608715, at *5-6 (N.D. Ill. Aug. 5, 1999) (officer and director positions with companies provided "ample evidence" that individuals had authority to control the purported practices and acts at issue and had some knowledge of the deceptive practices). In light of the Goolniks' active involvement in this scheme, they should be held individually liable.

4. The TRO Should Be Entered *Ex Parte* and Include An Order Provision Temporarily Disabling Defendants' Web Sites and An Asset Freeze

Ex parte relief is necessary here. An *ex parte* temporary restraining order is warranted where the facts show that irreparable injury, loss, or damage will result before the defendants can be heard in opposition. See Fed. R. Civ. P. 65(b). Consumer fraud cases such as this fit squarely into the category of situations where *ex parte* relief is appropriate and necessary to make possible full and effective final relief. Indeed, courts in this district have repeatedly granted the FTC *ex parte* relief in fraud cases brought under the FTC Act. See, e.g., *FTC v. 1st Financial Solutions, Inc.*, No. 01-CV-8790 (N.D. Ill. Nov. 19, 2001) (Kocoras, J.); *FTC v. Growth Plus Int'l Marketing, Inc.*, No. 00-CV-7886 (N.D. Ill. Dec. 18, 2000) (Aspen, J.); *FTC v. Med Resorts Int'l, Inc.*, No. 00-CV-4893 (N.D. Ill. Aug. 17, 2000) (Castillo, J.). As in the other cases in this district where courts have granted *ex parte* relief, irreparable injury, loss, or damage will likely result if Defendants receive notice of this action.

a. Defendants' Web Sites Should Be Immediately Disabled to Prevent Further Consumer Injury and Preserve Final Relief

An *ex parte* order provision temporarily disabling Defendants' Web sites is necessary to prevent further consumer injury and preserve final relief. Defendants use these Web sites –

including www.dotusa.com, www.dotsex.com and www.dotstore.com – to promote their scheme and fraudulently induce consumers to purchase domain names. Absent an order provision disabling the sites, Defendants, who are foreign nationals, could ignore the Court’s order and continue operating these Web sites. Moreover, absent *ex parte* action, Defendants may transfer their Internet operation entirely overseas, depriving the Court of jurisdiction to grant effective final relief.⁵ The FTC has been granted similar relief against other defendants who have utilized Internet Web sites to promote fraud. *See, e.g., FTC v. 1268957 Ontario Inc.*, 01-CV-423 (N.D. Ga. 2001) (signed order viewable over the Internet at <http://www.ftc.gov/os/2001/02/domannametro.pdf>); *FTC v. Pereira*, No. 99-1367-A (E.D. Va. 1999) (order viewable at <http://www.ftc.gov/os/1999/0909/atariztro.htm>).

b. A Temporary Asset Freeze Is Also Necessary to Preserve Effective Final Relief

In addition to the FTC’s legitimate concern regarding suspending Defendants’ Web sites, an *ex parte* asset freeze is also necessary to preserve the possibility the final relief in the form of redress for victimized consumers and full disgorgement of Defendants’ ill-gotten. Defendants’ assets should be frozen to ensure that funds do not disappear during the course of this litigation. This Court’s power to order an asset freeze derives from its equitable power to order consumer redress, *Febre*, 128 F.3d at 534, and courts in this district have repeatedly exercised this

⁵ Defendants’ Web sites may be disabled by suspending the domain names for the sites or, loosely speaking, taking the domain name out of the domain name system’s “address book.” At present, the domain names used to operate Defendants’ Web sites (*e.g.*, dotusa.com) are registered with U.S. companies, and the Court may therefore order those U.S. companies to suspend Defendants’ domain names. If the Court issues such an order, the Internet registration system will not allow Defendants to reestablish the same domain names in another country. (*See* PX 11 ¶¶ 3, 8.) Absent such a court order, however, upon receiving notice of this action Defendants could transfer the domain names used to operate their Web sites to a registry in a foreign country and continue to bilk consumers. (*Id.* ¶ 8.)

authority, see *FTC v. Growth Plus Int'l Marketing Inc.*, 2001 WL 128139 (N.D. Ill. Jan. 9, 2001) (Aspen, J.); *FTC v. Med Resorts Int'l, Inc.*, 2000 WL 1889635 (N.D. Ill. Dec. 27, 2000) (Castillo, J.); *FTC v. Windermere Big Win Int'l, Inc.*, 1999 WL 608715 (N.D. Ill. Aug. 5, 1999) (Marovich, J.).


There is significant risk that Defendants may dissipate assets during the pendency of these legal proceedings. As discussed *supra*, Defendants' business operations are permeated by, and reliant upon, deceptive practices. The FTC's past experiences have shown that defendants engaged in similar schemes may withdraw funds from bank accounts and move or shred inculpatory documents if given notice of the FTC's action.⁶ Without an immediate assets freeze, funds may not be available to satisfy any final order granting restitution to defrauded consumers.

VI. CONCLUSION

Defendants have caused and are likely to continue to cause injury to consumers because of their violations of Section 5(a) of the FTC Act. To prevent ongoing consumer harm and to help assure the possibility of effective final relief, including monetary redress, this Court should issue the requested injunctive relief.

Respectfully submitted,

William E. Kovacic
General Counsel


Steven M. Wernikoff
Federal Trade Commission
55 East Monroe, Suite 1860
Chicago, IL 60603
Voice: (312) 960-5634
Facsimile: (312) 960-5600

Dated: February 28, 2002

⁶ See Declaration of Certification of Plaintiff's Counsel Pursuant to Fed. R. Civ. P. 65(b) and Local Rule 5.5(D) In Support of Plaintiff's *Ex Parte* Motion For Temporary Restraining Order.