11

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

FEDERAL TRADE COMMISSION Plaintiff, v. API TRADE, LLC, a Pennsylvania limited liability company, *et al.*, Defendants.	Civ. No. 10 C 1543 Judge Ronald A. Guzman Magistrate Judge Jeffrey Cole

FEDERAL TRADE COMMISSION'S MEMORANDUM IN SUPPORT OF ITS *EX PARTE* MOTION FOR A TEMPORARY RESTRAINING ORDER WITH ASSET FREEZE, OTHER EQUITABLE RELIEF, AND ORDER TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE

I. INTRODUCTION

The Federal Trade Commission asks that the Court take immediate action to shut down a massive international fraud scheme that has placed over $10 million in unauthorized charges on debit and credit card accounts of consumers. Since at least 2006, Defendants have fraudulently charged more than 1.3 million credit and debit cards. Significantly, Defendants never contact their victims or attempt to sell them anything before assessing the unauthorized charges. Instead, Defendants somehow obtain the consumers' account numbers and proceed to sneak the charges onto the accounts. Defendants purposely make their unauthorized charges less than $10 in the hopes that consumers will not notice them or will choose not to contest the charges. The practice is patently illegal and must be stopped.

This scheme is masterminded by "Defendant(s) John Doe" – one or more individuals whose names and addresses are currently unknown to the FTC. Defendant(s) Doe likely operate the scheme from offshore and launder the proceeds through bank accounts in Eastern Europe and Central Asia.

Defendant(s) Doe have put in place an elaborate infrastructure in the U.S. through which they operate the unauthorized charging scheme. First, Defendant(s) Doe have hired under false pretenses a group of at least fourteen individuals in the U.S., referred to here as the "money mules." Defendant(s) Doe then direct the money mules to form companies and to open one or more U.S. bank accounts in the name of those entities. A group of sixteen companies formed by the money mules are named as defendants in this action and will be referred to here as the "Money Cashing Defendants." In addition to the Money Cashing Defendants, Defendant(s) Doe themselves also have created over a hundred fake companies using false identities. These fictitious companies – some of which purport to be located in this district – are the "merchants" that place the unauthorized charges on consumers' accounts.

With this infrastructure in place, Defendants have proceeded to assess unauthorized charges to consumers' accounts and to deposit the funds into the U.S. bank accounts of the Money Cashing Defendants. Defendant(s) Doe then direct the money mules to wire the funds to offshore accounts in Lithuania, Estonia, Latvia, Bulgaria, Cyprus, and Kyrgyzstan, where the funds presumably end up in the hands of the Doe Defendants. In this way, Defendants have essentially stolen over $10 million. More than 1000 consumers have filed complaints with the FTC about these illegal practices.

The FTC brings this motion *ex parte* to seek an immediate halt to this operation and to freeze its assets. The Money Cashing Defendants possess stolen funds in their U.S. bank accounts that the Court should prevent from being transferred offshore. That is the only way to preserve the possibility of redress for consumers whose money Defendants have stolen. The perpetrators of this scheme have gone to great lengths to hide their identity and their illegal practices. Defendants' pattern of fraud, as well as their attempts to conceal their identity and location, demonstrates that they would hide or dissipate assets if they received notice of this action. The requested relief is therefore necessary to prevent continued injury to consumers, the destruction of evidence, and the dissipation of assets, thereby preserving the Court's ability to provide effective final relief.

II. DEFENDANTS' ILLEGAL ENTERPRISE

Since at least 2006, Defendant(s) Doe have tested the old adage that it is easier to steal $1 from a million people than $1 million from one person by operating an outright scam – placing

small, unauthorized charges on consumers' credit and debit cards. The thinking behind the scam seems to be that the vast majority of consumers either will not notice the charges or will not go through the trouble of contesting them. By intentionally making their unauthorized charges under $10, Defendants have tried to fly under the radar of both consumers and the credit card companies' fraud detection programs.[1]

Defendant(s) Doe use three groups to operate this sophisticated scheme from an unknown location: (1) the money mules, a group of individuals in the United States who assist Defendant(s) Doe by wiring the proceeds of the scheme to offshore accounts, (2) the Money Cashing Defendants, at least sixteen companies formed by the money mules for the sole purpose of opening multiple bank accounts used to funnel the proceeds of the scam offshore, and (3) the fake companies whose role in the scheme is to apply for merchant accounts with credit card processors that enable Defendants to place their unauthorized charges on consumers' accounts. We describe the roles of each of these groups below.[2]

A. The Money Mules

Defendants' scam uses an expansive network of money mules in the United States to cash out the unauthorized charges. Defendant(s) Doe appear to have recruited money mules by sending spam email messages announcing that an international financial services company is seeking a U.S. finance manager to process transactions and cash checks, money orders, and international wire transfers. (PX 1 ¶¶ 45-47, Atts. J-L.) These email messages sometimes claim that the company needs a U.S. partner to receive payments from U.S. customers for efficiency or tax purposes. (*Id.* at ¶ 46, Atts. K, L.) The plan is for Defendant(s) Doe to transfer their alleged sales proceeds to the money mules, who are then to forward the funds as directed in exchange for

[1] We do not yet know how Defendants obtained over a million consumers' debit and credit card numbers, but we do know that consumers did not provide the numbers to them.

[2] The FTC has submitted the following exhibits in support of its TRO motion: (1) Declaration of FTC Investigator Douglas McKenney ("PX 1"); (2) Declaration of Dennis Day, Senior Manager in the Security/Risk Department of First Data Merchant Services Corporation ("PX 2"); and (3) declarations of two individuals whose identities have been used without their authorization to further this fraud ("PX 3" and "PX 4").

commission payments ranging from 5-10% of the total funds. (*Id.*) Defendant(s) Doe have recruited at least fourteen individuals in the U.S. to serve as money mules.[3]

B. The Money Cashing Defendants

Having recruited the money mules, Defendant(s) Doe direct them to form companies and then to open bank accounts in the name of those entities. With the money mules' assistance, Defendant(s) Doe have formed at least sixteen corporate entities in the U.S. (PX 1 ¶¶ 20-22, 43, 48, Att. M.) These are the Money Cashing Defendants named in the FTC's Complaint. Under the direction of Defendant(s) Doe, the money mules have opened over a hundred bank accounts in the names of the Money Cashing Defendants. (*Id.* ¶¶ 20-22.) The proceeds from Defendants' unauthorized charges are deposited into these bank accounts before being transferred by the money mules to offshore bank accounts. (*Id.* ¶¶ 43-44.)[4] Because the proceeds of Defendants' scheme are funneled through the bank accounts of the Money Cashing Defendants, these entities are named as Defendants to prevent further laundering of illegally obtained proceeds and to preserve funds presently in the accounts for potential consumer redress.

C. Defendant(s) Doe's Fake Companies

In addition to the Money Cashing Defendants formed by the money mules, Defendant(s) Doe also have created over a hundred fake companies whose role in the scheme is to apply for merchant accounts with credit card processors that will enable Defendants to place charges on consumers' accounts. (PX 1 ¶¶ 9-18; PX 2 ¶¶ 5-6, Atts. A, B.)[5] Each fictitious company set up by Defendant(s) Doe has a different "owner," a physical address, a website, a business telephone number, and a "home" telephone number for the "owner." (PX 1 ¶¶ 22-39; PX 2 ¶ 6, Att. B.) Using these fake companies, Defendant(s) Doe apply online for merchant accounts with credit

---

[3] We have not named the money mules as individual defendants because it is unclear at this point whether they knew that they were complicit in this fraud.

[4] In some cases, the proceeds of the unauthorized charges are transferred between Money Cashing Defendants before being transferred overseas. (PX 1 ¶ 44.)

[5] To evade detection, Defendant(s) Doe use debit cards linked to the Money Cashing Defendants' bank accounts to purchase the services necessary to set up the fake companies. (PX 1 ¶ 22.) The debit card purchases are made with various names that are almost certainly fictitious. (*Id.* ¶¶ 23-41.)

card processors using different Internet connections to further hide their identity. (PX 1 ¶¶ 35-36; PX 2 ¶ 6.)[6]

In setting up the fake companies, Defendant(s) Doe use names that sound similar to legitimate companies and provide addresses located in the vicinity of the legitimate companies. Defendant(s) Doe purchase "virtual office" addresses through a company that sells business address services. (PX 1 ¶¶ 23-26.)[7] All mail sent to these office addresses is then forwarded to another company that scans the mail and uploads it onto a secure server so that Defendant(s) Doe can view it electronically from any location. (*Id.* ¶ 26.) The fake companies also use Employer Identification Number ("EIN") tax numbers of the legitimate companies. (*Id.* ¶¶ 37-38.)

Defendant(s) Doe also create a website for each fake company so that the company appears to credit card processors to be a legitimate online merchant. (PX 1 ¶¶ 32-34, Atts. E-H (examples of fake company websites).) These websites appear to only operate for a short period of time, probably just long enough for a credit card processor to would perform due diligence on the account application. (*Id.*) The websites of the fake companies purport to sell some kind of product such as electronics and office supplies. (*Id.*) Each fake company also has a toll-free telephone number, as well as a "home" telephone number for the "owner" of the company. (*Id.* ¶¶ 27-31.) The toll-free numbers forward to a cell phone number registered in Belarus. (*Id.* ¶¶ 30-31.)

Defendant(s) Doe also use the names of identity theft victims as "owners" of these fake companies. (PX 1 ¶ 39; PX 2 ¶ 15, Att. D; PX 3 (identity theft victim); PX 4 (same).) Without their knowledge, Defendant(s) Doe provide the victims' name, social security number, and date of birth on merchant account applications. (*Id.*) Before Defendant(s) Doe use an identify theft victim's name to open an account, they run credit checks on the stolen identities to ensure that the victims have good credit scores so that the merchant accounts are approved by credit card

---

[6] An example of an online merchant account application of one of the fake companies is attached as Attachment B to PX 2.

[7] At least six of the fake companies use addresses in the Northern District of Illinois. (PX 1 ¶ 23.)

processors. (PX 1 ¶ 40.) These fictitious companies are therefore "owned" by identity theft victims without their knowledge.

D. Unauthorized Charges to Consumers

With this elaborate structure in place, Defendant(s) Doe have charged over $10 million in the last four years to more than 1.3 million consumer credit and debit cards. (PX 1 ¶¶ 9-17; PX 2 ¶¶ 6-7.) The charges range from twenty cents to $10 for each credit or debit card, and each card is generally charged only once. (PX 1 ¶ 5; PX 2 ¶ 10.) The FTC has received over 1000 complaints about unauthorized charges by the fake companies relating to this operation. (PX 1 ¶ 5.)[8] The complaints show that, prior to assessing these charges, Defendants have had no contact with the card holders and have not attempted to sell them anything. (*Id.*) When consumers receive their credit or debit card statements, there is an entry for the charge, with a merchant identifier – the fake company name, such as "Adele Services" or "GFDL" – and a toll-free telephone number. (*Id.*) Because the charge is so small, many consumers likely do not even notice it. Those that do, and call the telephone number listed, find that the numbers are either disconnected or go to an automated voice recording instructing consumers to leave a detailed message, which is never returned. (*Id.*; PX 2 ¶ 14.) Because consumers have no ability to speak to a representative to dispute the charge, some consumers contact their card issuer to reverse the charges and to cancel their accounts in order to stop future charges. (PX 2 ¶¶ 8-12.) The vast majority of consumers likely give up, however, and they do not request a chargeback because the amount of the charge is so small. (*Id.* ¶ 10.)

After consumers' accounts are charged, the proceeds are deposited into the bank accounts of the Money Cashing Defendants. (PX 1 ¶¶ 19-22, 43.) Defendant(s) Doe then instruct the money mules to forward the proceeds to bank accounts in Lithuania, Estonia, Latvia, Bulgaria, Cyprus, and Kyrgyzstan. (PX 1 ¶ 44 (chart showing transferred funds).)

---

[8] The charges also have generated media articles, *see, e.g.*, "Mysterious Credit Card Charges May Have Hit Millions of Users," *Boston Globe*, accessed at http://www.boston.com/business/personalfinance/articles/2009/01/11/mysterious_credit_card_charges_may_have_hit_millions_of_users/ (last accessed March 6, 2010) (noting that "[s]everal Internet complaint boards are filled with comments from credit card customers from coast to coast who have noticed a mysterious charge for about 25 cents of their statements" from "Adele Services").

III. THE DEFENDANTS

The FTC's complaint names as Defendants the sixteen corporate entities that we have referred to as the Money Cashing Defendants, as well as defendant(s) Doe, the offshore masterminds behind the unauthorized charging scheme. The identities and addresses of defendant(s) Doe, however, are unknown to the Commission at this time.

The following sixteen Money Cashing Defendants are the entities formed by the money mules, at the direction of Defendant(s) Doe, for the purpose of opening multiple bank accounts under their corporate names. The proceeds of this scheme flow through these bank accounts to offshore accounts in Eastern Europe and Central Asia.

- API Trade, LLC, a Pennsylvania limited liability company incorporated in 2006, which has at least four bank accounts in its name;
- ARA Auto Parts Trading LLC, a limited liability company, which has at least two bank accounts in its name;
- Bend Transfer Services, LLC, a Nevada limited liability company incorporated in 2007, which has at least thirty bank accounts in its name;
- B-Texas European, LLC, a Texas limited liability company incorporated in 2006, which has at least sixteen bank accounts in its name;
- CBTC, LLC, a Delaware limited liability company incorporated in 2007, which has at least four bank accounts in its name;
- CMG Global, LLC, a Pennsylvania limited liability company incorporated in 2006, which has at least eleven bank accounts in its name;
- Confident Incorporation, a California company incorporated in 2002, which has at least three bank accounts in its name;
- HDPL Trade LLC, a Pennsylvania limited liability company incorporated in 2008, which has at least nine bank accounts in its name;
- Hometown Homebuyers, LLC, a Texas limited liability company incorporated in 2002, which has at least thirty-seven bank accounts in its name;
- IAS Group LLC, a California limited liability company incorporated in 2008, which has at least five bank accounts in its name;

- IHC Trade LLC, a New York limited liability company incorporated in 2007, which has at least seventy-one bank accounts in its name;
- MZ Services, LLC, an Arizona limited liability company incorporated in 2004, which has at least fifty-three bank accounts in its name;
- New World Enterprizes, LLC, a New Jersey limited liability company incorporated in 2005, which has at least fourteen bank accounts in its name;
- Parts Imports LLC, a Louisiana limited liability company incorporated in 2006, which has at least forty-two bank accounts in its name;
- SMI Imports, LLC, a Florida limited liability company incorporated in 2006, which has at least fourteen bank accounts in its name; and
- SVT Services, LLC, a New York limited liability company incorporated in 2008, which has at least eight bank accounts in its name.

(*See* PX 1 ¶¶ 19-21, 43-44, 48, Att. M.)

The bank accounts we have identified in the names of these sixteen corporate entities hold, or have held, the proceeds of Defendants' unauthorized charging scheme. (*See* PX 1 ¶¶ 19-21, 43-44, 48.) The FTC seeks to freeze those accounts before further funds can be transferred offshore to preserve them for redress to victimized consumers.

IV. ARGUMENT

Defendants essentially have stolen millions of dollars from U.S. consumers by illegally placing unauthorized charges on consumers' credit and debit cards. These practices unquestionably violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). The Commission seeks an *ex parte* temporary restraining order prohibiting Defendants' ongoing illegal practices. The Commission also asks that the Court freeze Defendants' assets to preserve them for restitution to victims. The Court has full authority to enter the requested relief, which is strongly supported by the evidence. Courts in this district have repeatedly granted TROs in FTC fraud actions that were not nearly so egregious as the case at hand.[9]

---

[9] *See, e.g., FTC v. 2145183 Ontario Inc., et al.*, No. 09 C 7423 (N.D. Ill. Nov. 30, 2009) (Grady, J.) (*ex parte* TRO in action alleging violations of FTC Act); FTC *v. Integration Media, Inc.*, No. 09 C 3160 (N.D. Ill. May 27, 2009) (Bucklo, J.) (same); *FTC v, Atkinson*, No. 08 C 5666 (N.D. Ill. Oct 6, 2008) (Kendall, J.) (same); *FTC v. Data Bus. Solutions, Inc.*, No. 08 C 2783 (N.D. Ill. May 14, 2008)

(continued...)

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

The FTC Act provides that "in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction." 15 U.S.C. § 53(b). Once the Commission invokes the federal court's equitable powers, the full breadth of the court's authority is available, including the power to grant such ancillary final relief as rescission of contracts and restitution. *FTC v. Febre,* 128 F.3d 530, 534 (7th Cir. 1997); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 571-72 (7th Cir. 1989). The court may also enter a temporary restraining order, a preliminary injunction, and whatever additional preliminary relief is necessary to preserve the possibility of providing effective final relief. *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1026 (7th Cir. 1997); *see also Amy Travel,* 875 F.2d at 571. Such ancillary relief may include an asset freeze to preserve assets for eventual restitution to victimized consumers. *World Travel*, 861 F.2d at 1031.

B. The Commission Meets the Applicable Legal Standard for Issuance of a Temporary Restraining Order

To grant preliminary injunctive relief in an FTC Act case, the district court must (1) determine the likelihood that the Commission will ultimately succeed on the merits and (2) balance the equities. *World Travel*, 861 F.2d at 1029. Under this "public interest" test, "it is not necessary for the FTC to demonstrate irreparable injury." *Id.* When the court balances the equities, the public interest "must receive far greater weight" than any private concerns. *Id.* Preliminary injunctive relief is therefore appropriate if the Commission shows a likelihood of success on the merits and that a balancing of the equities, giving greater weight to the public interest, favors such relief.

---

[9](...continued)
(Dow, J.) (same); *FTC v. Union Consumer Benefits*, No. 08 C 2309 (N.D. Ill. April 23, 2008) (Aspen, J.) (same); *FTC v. Spear Systems, Inc.*, No. 07 C 5597 (N.D. Ill. Oct. 3, 2007) (Andersen, J.) (same); *FTC v. Sili Neutraceuticals, LLC*, No. 07 C 4541 (N.D. Ill. Aug. 13, 2007) (Kennelly, J.) (same); *FTC v. 1522838 Ontario Inc.*, No. 06 C 5378 (N.D. Ill. Oct. 4, 2006) (Gettleman, J.) (same); *FTC v. Datacom Mktg.*, No. 06 C 2574 (N.D. Ill. May 9, 2006) (Holderman, C.J.) (same); *FTC v. Centurion Fin. Benefits LLC*, No. 05 C 5442 (N.D. Ill. Sept. 21, 2005) (Nordberg, J.) (same); *FTC v. Cleverlink Trading Ltd.*, No. 05 C 2889 (N.D. Ill. May 16, 2005) (St. Eve, J.) (same); *FTC v. 3R Bancorp*, No. 04 C 7177 (N.D. Ill. Nov. 17, 2004) (Lefkow, J.) (same); *FTC v. 120194 Canada Ltd.*, No. 04 C 7204 (N.D. Ill. Nov. 8, 2004) (Gottschall, J.) (same).

1. There is a Strong Likelihood That Defendants Have Violated Section 5(a) of the FTC Act

Defendants' practice of sneaking small unauthorized charges onto consumers' credit and debit cards plainly violates Section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a). An act or practice is unfair under the FTC Act if it causes injury to consumers that (1) is substantial, (2) is not outweighed by countervailing benefits to consumers or competition, and (3) is not reasonably avoidable by consumers themselves. *See* 15 U.S.C. § 45(n); *see also FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 945 (N.D. Ill. 2008); *Orkin Exterminating Co. v. FTC,* 849 F.2d 1354, 1364 (11th Cir. 1988); *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000). Defendants' practices here, which are tantamount to theft, qualify as "unfair" under the FTC Act. *See, e.g., J.K. Publ'ns.*, 99 F. Supp. 2d at 1202-3 (defendants engaged in unfair practices by billing the credit and debit cards of customers and non-customers without their authorization); *Windward Mktg., Ltd.*, 1997 U.S. Dist. LEXIS 17114 (N.D. Ga. Sept. 30, 1997) (defendants engaged in unfair practices by depositing bank drafts against consumers' bank accounts without their authorization).

First, the injury to consumers is substantial. An injury may be sufficiently substantial if a small harm affects a large number of people. *See IFC Credit Corp.*, 543 F. Supp. 2d at 945; *J.K. Publ'ns, Inc.*, 99 F. Supp. 2d at 1201. Here, more than 1.3 million consumers' accounts have been charged without ever receiving anything from Defendants. In total, Defendants have placed over $10 million in unauthorized charges on consumers' accounts and generated more than 1000 complaints to the FTC.

Second, Defendants' unauthorized charges harm both consumers and competition. The second element for finding unfairness is satisfied "when a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition." *J.K. Publ'ns*, 99 F. Supp. 2d at 1201 (*quoting Windward Mktg., Ltd.*, 1997 U.S. Dist. LEXIS 17114, at *32). Here, these unauthorized charges clearly offer no benefit to consumers or competition.

Third, consumer victims had no way to avoid Defendants' unauthorized charges. The final element of unfairness focuses on whether the injury was reasonably avoidable by the consumers themselves. *See IFC Credit Corp.*, 543 F. Supp. 2d at 945. Courts have focused on

"whether consumers had a free and informed choice that would have enabled them to avoid the unfair practice." *Id.* at 948; *see also J.K. Publ'ns*, 99 F. Supp. 2d at 1201. Here, consumer victims were never offered any choice; instead, Defendants simply assessed unauthorized charges without notice. Defendants' unauthorized charging practices violate of Section 5(a) of the FTC Act.

2. The Equities Tip Decidedly in the Commission's Favor

Once the Commission has shown a likelihood of success on the merits, the Court must balance the equities, assigning greater weight to the public interest than to any of Defendants' private concerns. *World Travel,* 861 F.2d at 1029. The public equities in this case are compelling, as the public has a strong interest in halting the unauthorized charging scheme, and in preserving the assets necessary to provide effective final relief to victims. Defendants, by contrast, have no legitimate interest in continuing to steal from consumers. *See FTC v. Sabal,* 32 F. Supp. 2d 1004, 1009 (N.D. Ill. 1998); *FTC v. World Wide Factors, Ltd,* 882 F.2d 344, 347 (9th 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'"). An injunction is required to ensure that Defendants' scheme does not continue while the case is pending.

C. The Court Should Enter the FTC's Narrowly-Tailored Proposed TRO Which Includes an Asset Freeze and Other Attendant Relief[10]

The FTC requests that the Court issue a TRO that prospectively prohibits law violations and preserves assets and documents to ensure that the Court can grant effective final relief at the conclusion of this case. Part of the relief sought by the Commission in this case is restitution for the victims of Defendants' fraud. To preserve the possibility for such relief, the Commission seeks, at Sections II-III of its Proposed TRO Order, a freeze of Defendants' assets and, at Sections IX and X, the repatriation of funds transferred outside of the United States.

An asset freeze is appropriate once the Court determines that the Commission is likely to prevail on the merits and that restitution would be an appropriate final remedy. *See World Travel,* 861 F.2d at 1031 & n.9. The district court at that juncture has "a duty to ensure that the assets of the corporate defendants [are] available to make restitution to injured consumers." *Id.*

[10] A Proposed TRO has been filed concurrently with the FTC's TRO motion.

at 1031. This Court has the authority to order a party to "freeze" property under its control, whether the property is within or outside the United States. *U.S. v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965). Such an order is necessary here to ensure the possibility of effective final relief.

The additional relief requested in the FTC's proposed TRO is also appropriate. Section I of the Proposed TRO enjoins Defendants from making further unauthorized charges. Section IV of the Proposed TRO enjoins third parties served with the order from processing credit and debit card payments for Defendants. Section V requires Defendants to complete financial forms. Section VI requires Defendants to preserve records, and Section VII prohibits Defendants from selling or otherwise disclosing their customers' sensitive information. Section VIII requires Defendants to turn over relevant documents to the FTC. Section XI allows for expedited discovery of information relevant to a preliminary injunction hearing. These are necessary provisions to identify the scope of the unlawful practices, other participants, and the location of ill-gotten gains.

D. The Temporary Restraining Order Should Be Issued *Ex Parte*

To prevent Defendants from dissipating or concealing their assets, the requested TRO should be issued *ex parte*.[11] An *ex parte* TRO is warranted where the facts show that immediate and irreparable injury, loss, or damage will occur before the defendants can be heard in opposition. *See* Fed. R. Civ. P. 65(b). Here, given the utterly fraudulent nature of Defendants' illegal scheme, as in similar FTC cases in this district where courts have granted restraining orders on an *ex parte* basis,[12] it is all but certain that the assets and evidence stemming from the illegal activity will disappear if Defendants receive prior notice of the Commission's motion.

As outlined above, Defendants have gone to extraordinary lengths to hide their identity and their illegal practices. Indeed, even at this point, we have been unable to identify and locate defendant(s) Doe, who are the masterminds of the scheme. Defendants also regularly wire

---

[11] *See* Declaration in Support of *Ex Parte* Motion for Temporary Restraining Order and Application to File Papers Under Seal (describing need for *ex parte* relief here and citing cases in which defendants who learned of impending FTC action withdrew funds, destroyed vital documents, and fled the jurisdiction).

[12] *See* n. 9 at pp. 8-9.

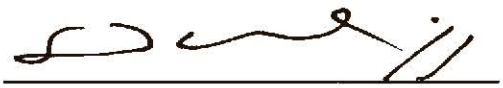
proceeds from the scam to overseas bank accounts in Eastern Europe and Central Asia. Defendants' pattern of fraud, as well as their attempts to conceal their identity and location, indicates that they would hide or dissipate assets if they receive notice of this action. At the very least, they would transfer funds in the bank accounts of the Money Cashing Defendants offshore. *Ex parte* relief is therefore necessary to preserve the status quo and ensure that Defendants cannot move assets and records outside of this Court's reach.

V. CONCLUSION

Defendants have caused and are likely to continue to cause substantial injury to consumers as a result of their violations of the FTC Act. The Commission therefore asks that the Court issue the requested injunctive relief to prevent ongoing harm and to help ensure the possibility of effective final relief, including monetary restitution.

Respectfully submitted,

WILLARD K. TOM
General Counsel



STEVEN M. WERNIKOFF
IRENE I LIU
Federal Trade Commission
55 W. Monroe St., Suite 1825
Chicago, IL 60603
(ph) (312) 960-5634
(fax) (312) 960-5600

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

Dated: March 9, 2010