Prepared Statement of

The Federal Trade Commission

Before the

Senate Committee on Commerce, Science and Transportation
United States Senate

Washington, D.C.
July 31, 2007

Chairman Inouye, Ranking Member Stevens, and Members of the Committee, I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to tell you about the Commission's law enforcement program[2] to fight telemarketing fraud and protect consumers' privacy from unwanted telemarketing calls, as well as our enforcement of the Credit Repair Organizations Act ("CROA").

I. Anti-fraud and Privacy Initiatives Under the Telemarketing Sales Rule

An article in the May 20th issue of *The New York Times,*[3] which included some disturbing allegations about telemarketing fraud targeting the elderly, has prompted a number of inquiries from members of Congress. This article focused on the alleged practices of infoUSA, a leading purveyor of compiled consumer data. According to the article, the company marketed lists of elderly consumers and failed to implement safeguards to ensure that only legitimate companies could purchase its data. Deplorable actions like the ones described in this article are among the types of fraudulent practices targeted by the Commission's telemarketing law enforcement program. The Commission has an extensive program to battle fraudulent and abusive

---

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. 41, *et seq*. With certain exceptions, the statute provides the agency with jurisdiction over nearly every economic sector. Certain entities, such as depository institutions and common carriers, as well as the business of insurance, are wholly or partly exempt from FTC jurisdiction. In addition to the FTC Act, the agency has enforcement responsibilities under more than 50 other statutes and more than 30 rules governing specific industries and practices.

[3] Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y.TIMES, May 20, 2007 at A1.

telemarketing practices through its vigorous enforcement of the Telemarketing Sales Rule ("TSR"). The FTC's telemarketing enforcement has two components. First, the Commission focuses strongly on the anti-fraud provisions of the TSR. Second, the FTC implements and enforces the requirements of the National Do Not Call Registry, which protects the privacy of Americans who have expressed their wish not to receive telemarketing calls by entering their numbers in the Registry.

A. The Commission's Enforcement of the Telemarketing Sales Rule's Anti-Fraud Provisions

The Commission has a strong commitment to rooting out telemarketing fraud. From 1991 to the present, the FTC has brought more than 350 telemarketing cases. The vast majority of these cases involved fraudulent marketing of investment schemes, business opportunities, sweepstakes pitches, and the sales of various goods and services, including health care products. Prior to 1994, these cases were brought pursuant to Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[4]

In 1994, Congress enhanced the Commission's enforcement arsenal by enacting the Telemarketing and Consumer Fraud and Abuse Prevention Act (the "Telemarketing Act").[5] This legislation directed the Commission to issue a trade regulation rule defining and prohibiting deceptive or abusive telemarketing acts or practices. The Commission promulgated the TSR in 1995. Since 1996, the Commission has filed more than 240 cases under the TSR. In most of

[4] 15 U.S.C. § 45(a).

[5] 15 U.S.C. §§ 6101-6108. Among the principal ways the Telemarketing Act, as implemented by the Telemarketing Sales Rule, strengthened the Commission's hand is that it provides a predicate for the Commission, through the Department of Justice, to seek civil penalties for violations. The Commission is not empowered to seek civil penalties for deceptive or unfair practices in violation of Section 5 of the FTC Act.

these cases, the Commission sought preliminary relief to bring an immediate halt to ongoing law violations, and in virtually every case ultimately obtained permanent injunctions to prevent future misconduct. In addition to injunctive relief, the Commission has secured orders providing for more than $500 million in consumer restitution or, where restitution was not practicable, disgorgement to the U.S. Treasury. During this same period, the Commission, through cases filed on its behalf by the U.S. Department of Justice ("DOJ"),[6] has obtained civil penalty orders totaling nearly $17 million.

As an example, just last week the FTC halted the allegedly unlawful telemarketing operations of Suntasia Marketing,[7] which, according to the FTC's complaint, took millions of dollars directly out of tens of thousands of consumers' bank accounts without their knowledge or authorization. Suntasia allegedly tricked consumers into divulging their bank account numbers by pretending to be affiliated with the consumers' banks and offering a purportedly "free gift" to consumers who accepted a "free trial" of Suntasia's products. Once the consumer divulged his or her bank account number, Suntasia allegedly was able to debit each consumer's account for initial fees ranging from $40 to $149. Often, charges between $19.95 and $49.95 recurred on a monthly basis, and Suntasia allegedly frustrated consumers' attempts to stop them. According to the complaint, some of Suntasia's calls were directed to consumers listed in "full-data leads,"

---

[6] Civil penalty actions are filed by DOJ on behalf of the FTC. In general, for those statutes or rules for which the Commission is authorized to seek civil penalties, under the FTC Act, the Commission must notify the Attorney General of its intention to commence, defend, or intervene in any civil penalty action under the Act. 15 U.S.C. § 56(a)(1). DOJ then has 45 days, from the date of the receipt of notification by the Attorney General, in which to commence, defend or intervene in the suit. *Id.* If DOJ does not act within the 45-day period, the FTC may file the case in its own name, using its own attorneys. *Id.*

[7] *FTC v. FTN Promotions, Inc.*, 8:07-cv-1279-T-30TGW (M.D. Fla. July 23, 2007).

which already included consumers' bank account numbers. Practical Marketing, a company from whom Suntasia purchased such leads, was investigated and prosecuted by the U.S. Postal Inspection Service and the U.S. Attorney for the Southern District of Illinois, and pled guilty to one count of identity theft on November 6, 2006.[8]

Working in cooperation with the U.S. Postal Inspection Service and state and local law enforcement, the Commission moved aggressively to stop Suntasia's allegedly unlawful practices. Last week, the Commission sought and obtained an *ex parte* court order. At the Commission's request, the U.S. District Court for the Middle District of Florida halted the scheme, appointed a receiver, and froze the assets of the nine corporate defendants and six individual defendants. The defendants' assets are frozen to preserve the agency's ability to obtain funds for injured consumers, should the Commission prevail in this litigation. The *Suntasia* case is just one example of the FTC's vigorous law enforcement program – a key feature of which is partnering with other law enforcement agencies whenever possible – to protect American consumers from the pernicious practices of fraudulent telemarketers.

By no means does the *Suntasia* case stand alone. The FTC frequently works with various federal, state, local, and foreign partners to conduct law enforcement "sweeps" – multiple simultaneous law enforcement actions – that focus on specific types of telemarketing fraud,[9] and

---

[8] 18 U.S.C. § 1028(a)(7). The plea agreement included a fine in an amount to be determined at sentencing, a payment of $100,000 to the U.S. Postal Inspection Service Consumer Fraud Fund, and other costs and assessments totaling about $13,000. At the sentencing on February 9, 2007, the court imposed a fine of $10,000.

[9] Some of the sweeps in which the FTC and its law-enforcement partners have engaged over the past several years include: "Dialing for Deception" http://www.ftc.gov/opa/2002/04/dialing.shtm (a sweep by the FTC that targeted telemarketing fraud in connections with in-bound telephone calls); "Ditch the Pitch" http://www.ftc.gov/opa/2001/10/ditch.shtm (a sweep targeting fraudulent out-bound telemarketing brought by the FTC and 6 States); "Operation No Credit,"

works to promote joint filing of telemarketing actions with the States.[10] When the Commission files a lawsuit in federal district court, we seek every appropriate equitable civil remedy a court can grant it to stop telemarketing fraud.[11] Remedies may include freezing the defendants' personal and corporate assets, appointing receivers over the corporate defendants, issuing temporary and permanent injunctions, and ordering consumer redress and disgorgement of ill-gotten gains.

A sample of the FTC's recent cases illustrates the range of the FTC's enforcement program. For instance, one case resulted in a judgment of more than $8 million against Canadian telemarketers of advance-fee credit cards.[12] Another yielded a contempt order banning

---

http://www.ftc.gov/opa/2002/09/opnocredit.shtm (43 law-enforcement actions, including criminal indictments, targeting a wide range of credit-related frauds brought by the FTC, the DOJ, the U.S. Postal Inspection Service, and 11 State and local authorities); "Operation Protection Deception" http://www.ftc.gov/opa/2000/10/protectdecpt.shtm (a sweep against telemarketers of fraudulent "credit card protection" services with extensive assistance from 5 States and the Federal Bureau of Investigation ("FBI")); "Senior Sentinel" http://www.ftc.gov/opa/1995/12/sen.shtm (a sweep targeting telemarketers who defraud the elderly coordinated by the DOJ and FBI, with 5 civil cases brought by the FTC, that led to hundreds of arrests and indictments across the country); "Project Telesweep" http://www.ftc.gov/opa/1995/07/scam.shtm (nearly 100 cases filed by the FTC, DOJ and 20 States targeting business opportunity fraud often promoted through slick telemarketing).

[10] *See*, *e.g.*, *FTC and State of Maryland v. Accent Marketing, Inc.*, No. 02-0405 (S.D. Ala. 2002); *FTC and State of Washington v. Westcal Equipment, Inc.*, No. C02-1783 (W.D. Wash. 2002); *FTC and State of Illinois v. Membership Services, Inc.*, No. 01-CV-1868 (S.D. Cal. 2001); *FTC, Commonwealth of Virginia, State of North Carolina, and State of Wisconsin v. The Tungsten Group, Inc.*, No. 2:01cv773 (E.D. Va. 2001); *FTC and State of Nevada v. Consumer Credit Services, Inc.*, No. CV-S-98-00741 (D. Nev. 1998); *FTC and State of New Jersey v. National Scholastic Society, Inc.*, No. 97-2423 (D.N.J. 1997).

[11] When the Commission seeks relief in its own right, the Commission's remedies are limited to equitable relief. As noted above, if the Commission chooses instead to seek a civil penalty for violations of the TSR, the Commission must refer the matter to DOJ.

[12] *FTC v. 120194 Canada, Ltd.*, No. 1:04-cv-07204 (N.D. Ill., permanent injunction order entered Mar. 8, 2007).

a seller of bogus business opportunities from all telemarketing.[13] Still another case resulted in a permanent injunction against a Canada-based operation that allegedly telemarketed fraudulent "credit card loss protection" and bogus discount medical and prescription drug packages.[14] In one of the Commission's largest actions, which involved an international ring that allegedly sold advance-fee credit cards, the agency obtained an order banning 13 individuals and entities from telemarketing.[15]

Although the Commission does not have criminal law enforcement authority, it recognizes the importance of criminal prosecution to deterrence and consumer confidence. Accordingly, the Commission routinely refers matters appropriate for criminal prosecution to federal and state prosecutors through its Criminal Liaison Unit ("CLU"). Since October 1, 2002, 214 people have been indicted[16] in criminal cases involving telemarketing fraud that arose from referrals made by CLU, including cases where an FTC attorney was designated a Special Assistant U.S. Attorney to help with the criminal prosecution. Of those 214 charged, 111 were convicted or pleaded guilty. The rest are awaiting trial, in the process of extradition from a foreign county, or fugitives from justice.[17]

---

[13] *FTC v. Neiswonger*, No. 4:96-cv-2225 (E.D. Mo., second permanent injunction entered Apr. 23, 2007).

[14] *FTC v. STF Group, Inc.*, No. 03 C 0977 (N.D. Ill., stipulated permanent injunction entered Jul. 21, 2006).

[15] *See* http://www.ftc.gov/os/caselist/assail/assail.shtm (seven permanent injunctions entered on various dates in *FTC v. Assail, Inc.*, No. W03CA007 (W.D. Tex.)).

[16] Eight of these indictments are under seal; staff does not know the precise date of the indictments.

[17] One defendant was granted a mistrial after suffering a stroke. He has been reindicted.

As in the *Suntasia* case, the Commission targets telemarketers who obtain consumers' personal information under false pretenses. For example, in *Xtel Marketing*, the FTC sued telemarketers that masqueraded as Social Security Administration representatives and claimed that call recipients risked losing their Social Security payments if they did not provide their bank account information.[18] Just last month, based on information provided by the FTC, a federal judge sentenced one of the principals in this scheme to five years in prison.

Telemarketers' deceptive and abusive practices often are aided or made possible by third parties, such as list brokers, who sell personal information about consumers to disreputable telemarketers, or by unscrupulous payment processors that enable fraudulent telemarketers to reach into consumers' bank accounts.

The May 20th *New York Times* article highlighted the role list brokers can play in facilitating such fraud. The article described the alleged practices of infoUSA, leading purveyor of compiled consumer data. According to the article, the company marketed lists of information about elderly consumers and failed to implement safeguards to ensure that only legitimate companies could purchase its data. The FTC has brought a number of cases challenging the sale of such lists to fraudulent telemarketers. In 2002, the FTC sued three information brokers that allegedly knew or consciously avoided knowing that they supplied lists of consumers to telemarketers acting in violation of the TSR. The FTC charged that Listdata Computer Services, Inc., Guidestar Direct Corporation, and NeWorld Marketing LLC knowingly supplied lists to telemarketers that were engaging in per se violations of the TSR by engaging in advance-fee

[18] *FTC v. XTel Marketing*, No. 04c-7238 (N.D. Ill. 2005).

loan scams.[19] Misuse of lists is a practice specifically addressed in the permanent injunctions the FTC seeks in its enforcement actions against fraudulent telemarketers. A standard provision of the FTC's proposed orders bans or severely restricts telemarketing defendants from selling, renting, leasing, transferring, or otherwise disclosing their customer lists. The FTC continues to monitor the practices of list brokers in this area through ongoing, non-public investigations.[20]

The FTC also has challenged other third-party actors such as payment processors, without whose assistance telemarketers would not be able to gain access to consumers' bank accounts.[21] Generally, the FTC has alleged that these payment processors knew or consciously

---

[19] Section 310.4(a)(4) of the Rule expressly prohibits "requesting or receiving payment of any fee or consideration in advance of obtaining a loan or other extension of credit when the seller or telemarketer has guaranteed or represented a high likelihood of success in obtaining or arranging a loan or of extension of credit for a person." The orders obtained by the FTC permanently barred the list brokers from providing lists to telemarketers engaging in illegal business practices and required them to pay nearly $200,000 combined in consumer redress. *FTC v. Listdata Computer Services, Inc.*, No. 04-61062 (S.D. Fla., stipulated final order entered Aug. 17, 2004); *FTC v. Guidestar Direct Corp.*, No. CV04-6671 (C.D. Cal., stipulated final order entered Aug. 13, 2004); *FTC v. NeWorld Marketing LLC*, No. 1:04cv159 (W.D. N. Car., stipulated final order entered Aug. 12, 2004); *see also* http://www.ftc.gov/opa/2004/08/guidestar.shtm.

[20] The Commission also has challenged the practice of brokers selling sensitive customer information to third parties without having reasonable procedures in place to verify the legitimacy of these third parties. Last year, the FTC brought a lawsuit against ChoicePoint, Inc., one of the nation's largest data brokers, alleging that it violated the Fair Credit Reporting Act and the FTC Act by failing to screen prospective subscribers before selling them sensitive consumer information. *U.S. v. ChoicePoint, Inc.*, CV-0198 (N.D. Ga., consent decree entered Jan. 30, 2006). The Commission alleged that ChoicePoint approved as customers identity thieves who lied about their credentials and whose applications should have raised obvious red flags. Under the terms of a settlement, ChoicePoint paid $10 million in civil penalties and $5 million in consumer redress, and agreed to implement new procedures to ensure that it provides sensitive data only to legitimate businesses for lawful purposes.

[21] *See, e.g., FTC v. Global Marketing Group, Inc.*, No. 8:06CV- 02272 (JSM) (M.D. Fla., filed Dec. 11, 2006) (litigation ongoing); *FTC v. First American Payment Processing, Inc.*, No. CV-04-0074 (PHX) (D. Ariz, stipulated final order entered Nov. 23, 2004); *FTC v. Electronic Financial Group*, No. W-03-CA-211 (W.D. Tex., stipulated final order entered Mar. 23, 2004); *FTC v. Windward Marketing, Ltd.*, No. 1:06-CV-615 (FMH) (N.D. Ga., stipulated

avoided knowing that they were facilitating fraudulent telemarketing operations in violation of the TSR[22] and, where appropriate, also has alleged direct violations of Section 5 of the FTC Act. Two cases brought this past December illustrate Commission enforcement in this area. In the first case, *FTC v. Interbill*,[23] the FTC alleged that Interbill debited money from consumer accounts without their authorization, in violation of the FTC Act.[24] In the second, *FTC v. Global Marketing Group, Inc.*,[25] the FTC obtained a preliminary injunction to shut down a payment processor that allegedly provided services to at least nine advance-fee loan telemarketers.[26]

The Commission's consumer and business education efforts complement our law enforcement initiatives. The FTC not only publishes compliance guides for business, but also a wealth of information in English and Spanish for consumers, including brochures and fact sheets on telemarketing fraud, sweepstakes and lotteries, work-at-home schemes, and advance-fee

---

final order against certain payment-processors entered Jun. 25, 1996, summary judgment order against remaining payment-processors entered Sep. 30, 1997).

[22] 16 C.F.R. 310.3(b).

[23] No. CV-S-06 (D. Nev., filed Dec. 26, 2006).

[24] Although the FTC does not have jurisdiction over banks, the FTC coordinates with the Federal Reserve Board and the other banking agencies concerning efforts to help banks avoid accepting fraudulent checks. These entities generally are regulated by the federal banking regulatory agencies – the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. Notably, the Commission recently authorized FTC staff to issue an opinion letter to NACHA-The Electronic Payments Association in support of that organization's proposed rule changes to strengthen safeguards against fraudulent transactions in the payment processing industry. The letter is available at http://www.ftc.gov/os/opinions/070423staffcommenttonacha.pdf.

[25] No. 8:06CV- 02272 (JSM) (M.D. Fla., filed Dec. 11, 2006).

[26] As noted above, advance-fee loan schemes are per se illegal under the TSR. 16 C.F.R. 310.4(a)(4).

loans, as well as phishing and other Internet-based frauds. This information is available in print and online. The FTC and its partners also distribute consumer education information to seniors groups and other community organizations.[27] In addition to providing educational resources to consumers and organizations nationwide, the FTC partners with other organizations and people who regularly meet with seniors and send representatives to community events.

B. Enforcement of the Do Not Call Provisions of the TSR

In addition to its anti-fraud work in the telemarketing arena, the Commission amended the TSR in 2003 to strengthen its privacy protection provisions by, among other things, establishing the National Do Not Call Registry.[28] Consumers have registered more than 146 million telephone numbers since the Registry became operational in June 2003, and the Do Not Call program has been tremendously successful in protecting consumers' privacy from unwanted telemarketing calls. A Harris Interactive® Survey released in January 2006 showed that 94% of American adults have heard of the Registry and 76% have signed up for it.[29] Ninety-two percent

---

[27] While the Commission remains deeply concerned about fraud affecting older consumers, the FTC's consumer complaint data and the results of its 2003 fraud survey indicate that the experience of older consumers is not substantially different than that of the general population. *See* http://www.ftc.gov/opa/2004/08/fraudsurvey.shtm. The results of this 2003 survey indicated that consumers age 65 or older did not experience more fraud than younger consumers.

[28] The FTC promulgated the Do Not Call provisions and other substantial amendments to the TSR under the express authority granted to the Commission by the Telemarketing Act. Specifically, the Telemarketing Act mandated that the rule – now known as the TSR – include prohibitions against any pattern of unsolicited telemarketing calls "which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy," as well as restrictions on the hours unsolicited telephone calls can be made to consumers.

[29] *See* http://www.harrisinteractive.com/harris_poll/index.asp?PID=627.

of those polled reported receiving fewer telemarketing calls.[30] Similarly, an independent survey by the Customer Care Alliance demonstrates that the National Registry has been an effective means for consumers to limit unwanted telemarketing calls.[31]

While the Commission appreciates the high rate of compliance with the TSR's Do Not Call provisions, it vigorously enforces compliance to ensure the program's ongoing effectiveness. Violating the Do Not Call requirements subjects telemarketers to civil penalties of up to $11,000 per violation.[32] Twenty-seven of the Commission's telemarketing cases have alleged Do Not Call violations, resulting in $8.8 million in civil penalties and $8.6 million in redress or disgorgement ordered.[33]

A recent case against The Broadcast Team, filed by DOJ on behalf of the FTC, illustrates the enforcement of the TSR's Do Not Call provisions.[34] The Broadcast Team allegedly used

---

[30] *Id.* Discussing the effectiveness of the National Registry just one year after the inception of the program, the chairman of Harris Poll, Harris Interactive stated, "In my experience, these results are remarkable. It is rare to find so many people benefit so quickly from a relatively inexpensive government program." http://www.ftc.gov/opa/2004/02/dncstats0204.shtm.

[31] *See National Do Not Call Study Preliminary Findings*, Customer Care Alliance, June 2004. Customer Care Alliance is a consortium of companies involved in customer service, dispute resolution, and related activities. *See* www.ccareall.org.

[32] As noted above, civil penalty actions are filed by DOJ on behalf of the FTC. The Commission's ability to protect consumers from unfair or deceptive acts or practices would be substantially improved by legislation, all of which is currently under consideration by Congress, that provides the agency with civil penalty authority in the areas of data security, telephone records pretexting, and spyware, similar to that provided under the Telemarketing Act. Civil penalties are especially important in these areas because the Commission's traditional remedies, including equitable consumer restitution and disgorgement, may be impracticable or not optimally effective in deterring unlawful acts.

[33] These Do Not Call cases are included in the 240 TSR cases noted above.

[34] *United States v. The Broadcast Team, Inc.*, Case 6:05-cv-01920-PCF-JGG (M.D. Fla. 2005).

"voice broadcasting" to make tens of millions of illegal automated telemarketing calls, often to numbers on the National Do Not Call Registry. The complaint alleged that the company used an automated phone dialing service to call and deliver pre-recorded telemarketing messages. When a live person picked up the phone, The Broadcast Team allegedly hung up immediately or, in other instances, played a recording. Either course of conduct violates the TSR's restriction on "abandoning calls" – that is, failing to connect a consumer to a live sales representative within two seconds after the consumer answers the telephone.[35] The Broadcast Team agreed to pay a $1 million civil penalty to settle the charges.[36]

The largest Do Not Call case to date involved satellite television subscription seller DirecTV and a number of companies that telemarketed on behalf of DirecTV. DirecTV paid over $5.3 million to settle Do Not Call and call abandonment charges,[37] one of the largest civil penalties the Commission has obtained in any case enforcing a consumer protection law.

II. Re-Authorization of the Do Not Call Implementation Act

The Do Not Call Implementation Act ("DNCIA"), passed by Congress on March 11, 2003, authorized the FTC to promulgate regulations establishing fees sufficient to implement and enforce the Do Not Call provisions of the TSR. This section first describes generally how the Do Not Call program works for consumers, telemarketers, and law enforcement agencies. It then discusses the grant of authority in the DNCIA for the Commission to charge fees for access

---

[35] 16 C.F.R. 310.4(b)(1)(iv).

[36] *See* http://www.ftc.gov/opa/2007/02/broadcastteam.shtm.

[37] *United States of America (for the Federal Trade Commission) v. DirecTV*, File No. 042 3039, Civil Action No. SACV05 1211 (C.D. Cal. Dec. 12, 2005). *See also* http://www.ftc.gov/opa/2005/12/directv.shtm.

to the National Registry, and the Commission's use of such fees to maintain the effectiveness of the TSR's Do Not Call provisions. Finally, it addresses legislative improvements to the DNCIA that would ensure the continued success of the National Registry and strengthen the Commission's telemarketing enforcement operations.

A. How the National Do Not Call Registry Works

The National Registry is a comprehensive, automated system used by consumers, telemarketers, and law enforcement agencies. The Registry was built to accomplish four primary tasks:

(1) To allow consumers to register their preferences not to receive telemarketing calls at registered telephone numbers;

(2) To allow telemarketers and sellers to access the telephone numbers included in the National Registry and to pay the appropriate fees for such access;

(3) To gather consumer complaint information concerning alleged do not call violations automatically over the telephone and the Internet; and

(4) To allow FTC, state, and other law enforcement personnel access to consumer registration information, telemarketer access information, and complaint information maintained in the Registry.

Consumers can register their telephone numbers through two methods: by calling a toll-free number from the telephone number they wish to register, or over the Internet. The process is fully automated, takes only a few minutes, and requires consumers to provide minimal personally identifying information.[38]

[38] In the case of registration by telephone, the only personal information provided is the telephone number to be registered. In the case of Internet registration, a consumer must provide, in addition to the telephone number(s) to be registered, a valid e-mail address to which a confirmation e-mail message is sent. Once the confirmation is complete, however, the e-mail address is hashed and made unusable. Thus, only consumers' telephone numbers are maintained in the database.

Telemarketers and sellers can access registered telephone numbers, and pay the appropriate fee for that access, if any, through an Internet website dedicated to that purpose. The only information about consumers that companies receive from the National Registry is the registered telephone number with no name attached. Those numbers are sorted and available for download by area code. Companies may also check a small number of telephone numbers at a time via interactive Internet pages.

Consumers who receive unwanted telemarketing calls can register a complaint via either a toll-free telephone number, an interactive voice response system, or the Internet. To conduct investigations, law enforcement officials also can access data in the National Registry, including consumer registration information, telemarketer access information, and consumer complaints. Such access is provided to the law enforcement community throughout the United States, Canada, and Australia through Consumer Sentinel, a secure Internet website maintained by the FTC.

B. Fees Collected and Used Pursuant to the DNCIA

The DNCIA gave the Commission the specific authority to "promulgate regulations establishing fees sufficient to implement and enforce the provisions relating to the 'do-not-call' Registry of the Telemarketing Sales Rule ("TSR")."[39] It also provided that "[n]o amounts shall be collected as fees pursuant to this section for such fiscal years except to the extent provided in advance in appropriations Acts. Such amounts shall be available . . . to offset the costs of activities and services related to the implementation and enforcement of the [TSR], and other activities resulting from such implementation and enforcement."[40] Pursuant to the DNCIA and

[39] Pub. L. No. 108-10, 117 Stat. 557 (2003).

[40] *Id.*

the appropriations Acts, the Commission has conducted annual rulemaking proceedings to establish the appropriate level of fees to charge telemarketers for access to the Registry.

The fees collected are intended to offset costs in three areas. First, funds are required to operate the Registry. As described above, the development and ongoing operation of the Do Not Call Registry involves significant resources and effort.

Second, funds are required for law enforcement and deterrence efforts, including identifying targets, coordinating domestic and international initiatives, challenging alleged violators, and engaging in consumer and business education efforts, which are critical to securing compliance with the TSR. As with all TSR enforcement, the agency coordinates with its state partners and DOJ, thereby leveraging resources and maximizing deterrence. Further, given the fact that various telemarketing operations are moving offshore, international coordination is especially important. These law enforcement efforts are a significant component of the total costs, given the large number of investigations conducted by the agency and the substantial effort necessary to complete such investigations.

As noted previously, the Commission considers consumer and business education efforts important complements to enforcement in securing compliance with the TSR. Because the amendments to the TSR were substantial, and the National Registry was an entirely new feature, educating consumers and businesses helped to reduce confusion, enhance consumers' privacy, and ensure the overall effectiveness of the system. Based on the Commission's experience, this substantial outreach effort was necessary, constructive, and effective in ensuring the success of the program.

Third, funds are required to cover ongoing agency infrastructure and administration costs associated with operating and enforcing the Registry, including information technology

structural supports and distributed mission overhead support costs for staff and non-personnel expenses, such as office space, utilities, and supplies. In this regard, the FTC has made substantial investments in technology and infrastructure in response to the significantly increased capacity required by the National Registry.

Under the current fee structure, telemarketers are charged $62 per area code of data, starting with the sixth area code, up to a maximum of $17,050 for the entire Registry.[41] Telemarketers are prohibited from entering into fee-sharing arrangements, including any arrangement with any telemarketer or service provider to divide the fees amongst its various clients.

Telemarketers receive the first five area codes of data at no cost. The Commission allows such free access to limit the burden placed on small businesses that only require access to a small portion of the Registry. The National Registry also allows organizations exempt from the Registry requirements to access the Registry at no cost.[42] While these entities are not required by law to access the Registry, many do so voluntarily in order to avoid calling consumers who have expressed their preferences not to receive telemarketing calls. The Commission determined that such entities should not be charged access fees when they are under no legal obligation to comply with the Do Not Call requirements of the TSR because it may

---

[41] The Commission set the initial fees at $25 per area code of data with a maximum annual fee of $7,375. *See* 68 Fed. Reg. 45134 (July 31, 2003). The fees have increased each year to its current level. *See* 69 Fed. Reg. 45580 (July 30, 2004); 70 Fed. Reg. 43273 (July 27, 2005); and 71 Fed. Reg. 43048 (July 31, 2006).

[42] Such exempt organizations include entities that engage in outbound telephone calls to consumers to induce charitable contributions, for political fund raising, or to conduct surveys. They also include entities engaged solely in calls to persons with whom they have an established business relationship or from whom they have obtained express written agreement to call, as defined by the Rule, and who do not access the National Registry for any other purpose.

make them less likely to obtain access to the Registry, which would result in an increase in the number of unwanted calls to consumers.

C. Legislative Modifications of the DNCIA

As noted above, the DNCIA allowed the FTC to promulgate regulations to collect fees for the Do Not Call Registry. The Commission believes that reauthorizing the DNCIA will demonstrate Congress' continued commitment to protecting consumers from unwanted intrusions into the privacy of their homes, and appreciates Senator Pryor's proposed reauthorizing legislation. The Commission believes that the bill can be strengthened by statutorily mandating the fees to be charged to telemarketers accessing the National Registry, and specifically by mandating such fees in an amount sufficient to enable the Commission to enforce the TSR. The Commission believes that such an amendment to the DNCIA would ensure the continued success of the National Registry by providing the Commission with a stable funding source for its TSR enforcement activities. The Commission also believes a stable fee structure would benefit telemarketers, sellers, and service providers who access the Registry. The Commission looks forward to working with you on this matter.

III. Credit Repair Organizations Act

The Commission also enforces the Credit Repair Organizations Act ("CROA")[43] by aggressively pursuing businesses engaging in fraudulent "credit repair." CROA was enacted to protect the public from unfair or deceptive advertising and business practices by credit repair organizations. In addition to prohibiting false or misleading statements about credit repair services,[44] CROA includes a number of other important requirements to protect consumers, including a ban on collecting payment before the service is fully performed and a requirement to provide consumers with a written disclosure statement before any agreement is executed.[45]

The Commission has conducted several sweeps of fraudulent credit repair operations, including Project Credit Despair (twenty enforcement actions brought by the FTC, U.S. Postal Inspection Service, and eight state attorneys general in 2006);[46] Operation New ID - Bad Idea I and II (52 actions brought by the FTC and other law enforcement agencies in 1999);[47] and Operation Eraser (32 actions brought by the FTC, state attorneys general, and DOJ in 1998).[48]

---

[43] 15 U.S.C. §1679 *et seq*.

[44] CROA prohibits persons from advising a consumer to make false and misleading statements about a consumer's credit worthiness or credit standing to a consumer reporting agency. 15 U.S.C. § 1679b(a)(1).

[45] The written disclosure must explain consumers' right to dispute inaccurate credit information directly to a credit reporting agency and to obtain a copy of their credit reports. It also must state that neither the credit repair organization nor the consumer can remove accurate, negative information from his or her report. 15 U.S.C. § 1679(c). It also requires credit repair organizations to use written contracts that include the terms and conditions of payment and other specified information. 15 U.S.C. § 1679(d).

[46] *See* http://www.ftc.gov/opa/2006/02/badcreditbgone.shtm.

[47] *See* http://www.ftc.gov/opa/1999/10/badidea.shtm.

[48] *See* http://www.ftc.gov/opa/1998/07/erasstl.shtm.

The Commission also educates businesses and consumers about credit repair. Among other outreach efforts, the Commission publishes a large volume of educational materials designed to educate both consumers and businesses about their respective rights and obligations in the credit area. The agency's publications include: *Credit Repair: Self Help May Be Best*,[49] which explains how consumers can improve their creditworthiness and lists legitimate resources for low or no cost help; and *How to Dispute Credit Report Errors*,[50] which explains how to dispute and correct inaccurate information on a consumer report and includes a sample dispute letter.

One issue that has arisen recently is whether CROA should be amended to exempt credit monitoring services, which are offered by consumer reporting agencies, banks, and others.[51] As a matter of policy, the Commission sees little basis on which to subject the sale of legitimate credit monitoring and similar educational products and services to CROA's specific prohibitions and requirements, which were intended to address deceptive and abusive credit repair business practices. Credit monitoring services, if promoted and sold in a truthful manner, can help consumers maintain an accurate credit file and provide them with valuable information for

---

[49] *Available at* www.ftc.gov/bcp/conline/pubs/credit/repair.shtm (English); http://www.ftc.gov/bcp/conline/spanish/credit/s-repair.shtm (Spanish).

[50] *Available at* www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm.

[51] Legislation introduced in the U.S. House of Representatives would exempt from CROA's coverage those who provide a broad range of credit-related services, including credit monitoring, credit scores or scoring tools, any analysis or explanations of actual or hypothetical scores or tools. *See*, "A Bill to Amend the Credit Repair Organizations Act to Clarify the Applicability of Certain Provisions to Credit Monitoring Services, and For Other Purposes" (H.R. 2885), currently before the House Financial Services Committee. A previous set of proposed amendments to CROA, included in the Financial Data Protection Act of 2006, Sec. 6 (H.R. 3997), was passed by the House Financial Services Committee on March 16, 2006, but was not passed by the Senate.

combating identity theft.[52] However, any amendment intended to provide an exemption for legitimate credit monitoring services must be carefully considered and narrowly drawn. Drafting an appropriate legislative clarification is difficult and poses challenges for effective law enforcement. If an exemption is drafted too broadly, it could provide an avenue for credit repair firms to evade CROA. Indeed, in enforcing CROA, the Commission has encountered many allegedly fraudulent credit repair operations that aggressively find and exploit existing exemptions in an attempt to escape the strictures of the current statute.[53] Because of the drafting difficulties, the Commission urges Congress to continue to reach out to stakeholders in developing any amendments to CROA.

---

[52] Of course, these services are not the only way for consumers to monitor their credit file. The Fair and Accurate Credit Transactions Act gives every consumer the right to a free credit report from each of the three major credit reporting agencies once every 12 months.

[53] *See, e.g., FTC v. ICR Services, Inc.*, No. 03C 5532 (N.D. Ill. Aug. 8, 2003) (consent decree) (complaint alleged that defendant falsely organized as 501(c)(3) tax-exempt organization to take advantage of CROA exemption for nonprofits); and *United States v. Jack Schrold*, No. 98-6212-CIV-ZLOCH (S.D. Fla. 1998) (stipulated judgment and order for permanent injunction) (complaint alleged that defendant attempted to circumvent CROA's prohibition against "credit repair organizations" charging money for services before the services are performed fully).