

S. HRG. 110-1170

**OVERSIGHT OF TELEMARKETING PRACTICES AND  
THE CREDIT REPAIR ORGANIZATIONS ACT (CROA)**

---

---

**HEARING**

BEFORE THE

**COMMITTEE ON COMMERCE,  
SCIENCE, AND TRANSPORTATION**

**UNITED STATES SENATE**

**ONE HUNDRED TENTH CONGRESS**

**FIRST SESSION**

—————  
**JULY 31, 2007**  
—————

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

75-784 PDF

WASHINGTON : 2012

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, <i>Vice Chairman</i>
JOHN F. KERRY, Massachusetts	JOHN McCAIN, Arizona
BYRON L. DORGAN, North Dakota	TRENT LOTT, Mississippi
BARBARA BOXER, California	KAY BAILEY HUTCHISON, Texas
BILL NELSON, Florida	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	GORDON H. SMITH, Oregon
FRANK R. LAUTENBERG, New Jersey	JOHN ENSIGN, Nevada
MARK PRYOR, Arkansas	JOHN E. SUNUNU, New Hampshire
THOMAS R. CARPER, Delaware	JIM DEMINT, South Carolina
CLAIRE McCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	JOHN THUNE, South Dakota

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*

LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*

CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*

KENNETH R. NAHIGIAN, *Republican Deputy Staff Director and Chief Counsel*

## CONTENTS

---

	Page
Hearing held on July 31, 2007 .....	1
Statement of Senator Klobuchar .....	42
Statement of Senator Pryor .....	1
Statement of Senator Thune .....	46

### WITNESSES

Cerasale, Jerry, Senior Vice President, Government Affairs, Direct Marketing Association, Inc. ....	20
Prepared statement .....	21
Faulkner, Joanne S., Attorney, on Behalf of National Association of Consumer Advocates, National Consumer Law Center, U.S. PIRG, Consumer Federation of America .....	28
Prepared statement .....	30
Holland, Robin, Senior Vice President, Global Operations, Equifax Inc. ....	25
Prepared statement .....	26
Johnson, Richard, Member, Board of Directors, AARP .....	15
Prepared statement .....	17
Parnes, Lydia B., Director, Bureau of Consumer Protection, Federal Trade Commission .....	2
Prepared statement .....	3
St. Clair, Steve, Assistant Attorney General, State of Iowa .....	37
Prepared statement .....	39

### APPENDIX

Faulkner, Joanne S., Attorney, National Association of Consumer Advocates, supplemental statement .....	55
Holland, Robin, Senior Vice President, Global Operations, Equifax Inc., supplemental statement .....	53
Response to written questions submitted by Hon. Frank R. Lautenberg to:	
Jerry Cerasale .....	57
Richard Johnson .....	57
Lydia B. Parnes .....	55



**OVERSIGHT OF TELEMARKETING PRACTICES  
AND THE CREDIT REPAIR ORGANIZATIONS  
ACT (CROA)**

---

**TUESDAY, JULY 31, 2007**

U.S. SENATE,  
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,  
*Washington, DC.*

The Committee met, pursuant to notice, at 2:35 p.m. in room SR-253, Russell Senate Office Building, Hon. Mark Pryor, presiding.

**OPENING STATEMENT OF HON. MARK PRYOR,  
U.S. SENATOR FROM ARKANSAS**

Senator PRYOR. I'll go ahead and call the meeting to order, and I want to thank our witnesses for being here.

We're going to have some other Senators join us. I understand we're going to have a number of Senators that will be coming and going throughout the hearing, and I'd like to thank Chairman Inouye and Co-Chairman Stevens for holding this hearing and allowing me to chair this hearing on telemarketing practices and the Credit Repair Organizations Act, or CROA, under the FTC.

I'd also like to thank them for their past leadership on this issue, in allowing these issues to come before the Committee on previous occasions. Both of these topics are very important to American consumers and important in the American marketplace.

I'm a sponsor of the legislation to reauthorize the Do Not Call Registry, I'm particularly interested in the testimony of the witnesses that are here today to offer insight into the efficacy of the program and how to try to improve that program, if possible. I'm also concerned about whether CROA is achieving the intended protections Congress created in 1993, and whether the Act is preventing consumer access to needed financial tools and resources.

By analyzing the important issues of these laws and regulations, I'm optimistic that Congress can create legislation that is forward-thinking to—and considerate of—the interested and impacted parties. I believe Congress has a duty to protect the most vulnerable Americans from scams and other actions of unscrupulous businesses, and I hope through careful consideration of the testimony today, and emerging issues, we can protect consumers from identity theft, and undue intrusion, while ensuring the stream of commerce as efficiently as possible.

So, I'd like to go ahead and open the discussion, we may have other Senators join us here in a few moments, and we may allow them to make opening statements when they come.

But first, on our panel today—I guess we'll do 5-minute rounds? We'll allow each of the panelists to have opening statements of up to 5 minutes. We'll do this in two panels. Then we'll ask questions of the two panels separately. We'll do panel one first, and then we'll do panel two and have questions after each panel.

First, let me introduce Ms. Lydia Parnes; she's the Director of Bureau of Consumer Protection at the Federal Trade Commission here in Washington, D.C.

Ms. Parnes?

**STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF  
CONSUMER PROTECTION, FEDERAL TRADE COMMISSION**

Ms. PARNES. Chairman Pryor, thank you. I appreciate the opportunity to appear here today to discuss three of the Commission's important consumer protection initiatives: Our longstanding commitment to fight telemarketing fraud, the FTC's widely used and highly regarded Do Not Call Registry, and our aggressive enforcement of the Credit Repair Organizations Act.

As part of its mandate to protect consumers, the Commission devotes significant resources to combating fraudulent, deceptive and abusive telemarketing practices. We do this by enforcing Section 5 of the FTC Act, and the Commission's Telemarketing Sales Rule, both of which prohibit false and misleading claims, unauthorized billing, and other practices used by fraudsters to steal money from consumers.

The Commission also implements and enforces the Do Not Call Registry, which protects the privacy of Americans who have expressed their wish not to receive telemarketing calls.

The Commission has been pursuing fraudulent telemarketers for more than 20 years. Since 1991, we have filed more than 350 telemarketing cases, challenging an array of scams, including bogus investment schemes, business opportunities, and sweepstakes pitches.

In addition to the strong injunctive relief we obtained in these cases, the Commission has secured orders providing for more than \$500 million in consumer redress, or disgorgement.

We share your concern about telemarketers targeting the elderly. The May 20 *New York Times* article on this issue, highlighted the role that third parties play in facilitating telemarketing fraud. Fraudulent telemarketers have always required the participation of third-party businesses. Lead list generators and brokers, third-party telemarketing firms, fulfillment houses, money transmitters, payment processors, banks and telephone companies are just some of the entities that telemarketers need to run their business. That is why Congress, in the Telemarketing Act, gave the Commission the authority to regulate and challenge practices that assist and facilitate fraudulent telemarketing, and the Commission has used that authority.

In addition to its anti-fraud work in the telemarketing area, the Commission administers the National Do Not Call Registry. Since its implementation in June 2003, consumers have registered more

than 146 million telephone numbers. The humorist, Dave Barry, called it “the most popular Government program since the Elvis stamp.”

According to a Harris Interactive Survey released last year, 92 percent of those polled reported receiving fewer telemarketing calls. The success of the Registry is due, in part, to vigorous enforcement, and a high rate of industry compliance. The Commission has brought 27 cases to enforce the Do Not Call rule, resulting in orders for \$17.4 million in civil penalties and disgorgement.

Reauthorizing the Do Not Call Implementation Act, and with it, our ability to collect fees from those who access the Registry, will ensure the continued success of the Do Not Call Program, and underscore our collective commitment to this important privacy protection.

We do believe the bill can be strengthened, by statutorily mandating the fees charged to telemarketers accessing the registry, and look forward to working with you on this matter.

The Commission also enforces the Credit Repair Organizations Act by aggressively pursuing businesses engaged in fraudulent credit repair. CROA was enacted to protect the public from unfair and deceptive practices by credit repair organizations.

Together with its Federal and State law enforcement partners, the Commission has conducted several law enforcement sweeps against fraudulent credit repair outfits, resulting in over 100 enforcement actions. We’ve also engaged in outreach to businesses and consumers, and have published numerous educational materials designed to educate both consumers and businesses about their respective rights and obligations in the credit area.

The Commission will continue to take aggressive action to enforce CROA, combat fraudulent, deceptive and abusive telemarketing practices, and to continue the success of the Do Not Call Registry.

Again, I appreciate the opportunity to appear before the Committee, and would be pleased to take any questions you may have.

[The prepared statement of Ms. Parnes follows:]

PREPARED STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

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”).<sup>1</sup> I appreciate the opportunity to appear before you today to tell you about the Commission’s law enforcement program<sup>2</sup> 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 20 issue of *The New York Times*,<sup>3</sup> 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 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."<sup>4</sup>

In 1994, Congress enhanced the Commission's enforcement arsenal by enacting the Telemarketing and Consumer Fraud and Abuse Prevention Act (the "Telemarketing Act").<sup>5</sup> 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 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"),<sup>6</sup> 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,<sup>7</sup> 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," 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.<sup>8</sup>

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,<sup>9</sup> and works to promote joint filing of telemarketing actions with the states.<sup>10</sup> 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.<sup>11</sup> 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.<sup>12</sup> Another yielded a contempt order banning a seller of bogus business opportunities from all tele-

marketing.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>

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<sup>16</sup> 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.<sup>17</sup>

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.<sup>18</sup> Just last month, based on information provided by the FTC, a Federal judge sentenced one of the principals in this scheme to 5 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 20 *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 loan scams.<sup>19</sup> 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.<sup>20</sup>

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.<sup>21</sup> Generally, the FTC has alleged that these payment processors knew or consciously avoided knowing that they were facilitating fraudulent telemarketing operations in violation of the TSR<sup>22</sup> 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*,<sup>23</sup> the FTC alleged that Interbill debited money from consumer accounts without their authorization, in violation of the FTC Act.<sup>24</sup> In the second, *FTC v. Global Marketing Group, Inc.*,<sup>25</sup> the FTC obtained a preliminary injunction to shut down a payment processor that allegedly provided services to at least nine advance-fee loan telemarketers.<sup>26</sup>

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 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.<sup>27</sup> 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.<sup>28</sup> 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<sup>®</sup> Survey released in January 2006 showed that 94 percent of American adults have heard of the Registry and 76 percent have signed up for it.<sup>29</sup> Ninety-two percent of those polled reported receiving fewer telemarketing calls.<sup>30</sup> 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.<sup>31</sup>

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.<sup>32</sup> 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.<sup>33</sup>

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.<sup>34</sup> The Broadcast Team allegedly used "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 2 seconds after the consumer answers the telephone.<sup>35</sup> The Broadcast Team agreed to pay a \$1 million civil penalty to settle the charges.<sup>36</sup>

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,<sup>37</sup> 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 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.<sup>38</sup>

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”).”<sup>39</sup> 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.”<sup>40</sup> Pursuant to the DNCIA and 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.<sup>41</sup> 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.<sup>42</sup> 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 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")<sup>43</sup> 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,<sup>44</sup> 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.<sup>45</sup>

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);<sup>46</sup> Operation New ID—Bad Idea I and II (52 actions brought by the FTC and other law enforcement agencies in 1999);<sup>47</sup> and Operation Eraser (32 actions brought by the FTC, state attorneys general, and DOJ in 1998).<sup>48</sup>

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*,<sup>49</sup> 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*,<sup>50</sup> 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.<sup>51</sup> 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 combating identity theft.<sup>52</sup> 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.<sup>53</sup> Because of the drafting difficulties, the Commission urges Congress to continue to reach out to stakeholders in developing any amendments to CROA.

### Endnotes

<sup>1</sup> 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.

<sup>2</sup> 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 in-

surance, 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.

<sup>3</sup> Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. TIMES, May 20, 2007 at A1.

<sup>4</sup> 15 U.S.C. § 45(a).

<sup>5</sup> 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.

<sup>6</sup> 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.*

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

<sup>8</sup> 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.

<sup>9</sup> 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,” <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/protectdecept.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).

<sup>10</sup> 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).

<sup>11</sup> 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.

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

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

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

<sup>15</sup> 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.)).

<sup>16</sup> Eight of these indictments are under seal; staff does not know the precise date of the indictments.

<sup>17</sup> One defendant was granted a mistrial after suffering a stroke. He has been re-indicted.

<sup>18</sup>*FTC v. XTel Marketing*, No. 04c-7238 (N.D. Ill. 2005).

<sup>19</sup>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>.

<sup>20</sup>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.

<sup>21</sup>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 final order against certain payment-processors entered Jun. 25, 1996, summary judgment order against remaining payment-processors entered Sep. 30, 1997).

<sup>22</sup>16 C.F.R. 310.3(b).

<sup>23</sup>No. CV-S-06 (D. Nev., filed Dec. 26, 2006).

<sup>24</sup>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>.

<sup>25</sup>No. 8:06CV-02272 (JSM) (M.D. Fla., filed Dec. 11, 2006).

<sup>26</sup>As noted above, advance-fee loan schemes are *per se* illegal under the TSR. 16 C.F.R. 310.4(a)(4).

<sup>27</sup>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.

<sup>28</sup>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.

<sup>29</sup>See [http://www.harrisinteractive.com/harris\\_poll/index.asp?PID=627](http://www.harrisinteractive.com/harris_poll/index.asp?PID=627).

<sup>30</sup>*Id.* Discussing the effectiveness of the National Registry just 1 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 ben-

efit so quickly from a relatively inexpensive government program.” <http://www.ftc.gov/opa/2004/02/dncstats0204.shtm>.

<sup>31</sup>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](http://www.ccareall.org).

<sup>32</sup>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.

<sup>33</sup>These Do Not Call cases are included in the 240 TSR cases noted above.

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

<sup>35</sup>16 C.F.R. 310.4(b)(1)(iv).

<sup>36</sup>See <http://www.ftc.gov/opa/2007/02/broadcastteam.shtm>.

<sup>37</sup>*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>.

<sup>38</sup>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.

<sup>39</sup>Pub. L. No. 108–10, 117 Stat. 557 (2003).

<sup>40</sup>*Id.*

<sup>41</sup>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).

<sup>42</sup>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.

<sup>43</sup>15 U.S.C. § 1679 *et seq.*

<sup>44</sup>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).

<sup>45</sup>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).

<sup>46</sup>See <http://www.ftc.gov/opa/2006/02/badcreditbgone.shtm>.

<sup>47</sup>See <http://www.ftc.gov/opa/1999/10/badidea.shtm>.

<sup>48</sup>See <http://www.ftc.gov/opa/1998/07/erasstl.shtm>.

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

<sup>50</sup>Available at [www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm](http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm).

<sup>51</sup>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.

<sup>52</sup>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.

<sup>53</sup>*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).

Senator PRYOR. Thank you, Ms. Parnes, and let me apologize for mispronouncing your name earlier.

But, let me go ahead and start with Do Not Call questions. You talk about how the program has been a great success—I'd like to put some quantifications on that, if I can. How many people have signed up for it and what can we do to improve it?

Ms. PARNES. Well, there are 146 million separate telephone numbers that have been registered on the Do Not Call list. Our experience is that it really is, it really is working, it's working well. There are—we believe that we have the legislative tools to pursue those who are violating Do Not Call, and as I indicated, compliance is generally high. And I think part of the reason it's high, is because legitimate businesses know how strongly consumers feel about receiving unwanted telemarketing calls.

Senator PRYOR. You say compliance is "generally" high—have you had some problems on the enforcement side?

Ms. PARNES. We have engaged in some enforcement, absolutely. We've—since the Do Not Call Registry was adopted, I believe—I believe we've brought 17 cases, challenging Do Not Call violations.

Senator PRYOR. And have those been concluded successfully, for the most part?

Ms. PARNES. They have been. They have been. One of the cases against a telemarketers, DIRECTV, involved—at the time—the largest civil penalty that we had obtained in the consumer protection area.

Senator PRYOR. Let me ask about Do Not Call, and the structure of it.

With the advent, and the explosion, really, of cell phone usage, and Voice-over-Internet Protocol phones, VoIP, service—are those included in the current Do Not Call Registry, and if so, are all of those phone numbers included?

Ms. PARNES. Well, cell phones are interesting—every so often there is an e-mail that goes around on the Internet, encouraging everybody to register their cell phones on the Do Not Call List. In fact, telemarketing calls to cell phones really shouldn't be a problem. The FCC rule prohibits telemarketers from using automated dialers to call cell phones, and automated dialers are really the standard in the industry. So, as a practical matter, telemarketers can't call cell phones.

But, we do register any phone. So, if a consumer is concerned, they can go ahead and register their cell phone on the Registry.

In terms of VoIP, one of the things we find generally, is that convergence of technologies—Internet and telephone services, I mean, that poses challenges in the consumer protection area. We held 4

days of hearings at the Commission last November, to look at convergence and other emerging issues in the consumer protection area. So far we haven't seen a problem, we've actually brought one telemarketing case involving VoIP technology. But certainly, if we see a problem, we would—and it raises legislative issues, we would come to the Committee with that.

Senator PRYOR. Thank you.

Ms. PARNES, as you know, the Committee and my staff, and the Committee staff and the Senators and their staffs have been working to reauthorize the Do Not Call Registry, and I want to thank you and your staff for being available, and for helping in that endeavor. Because you all have provided some very valuable insight, and I want to thank you for that.

And also, I think you know the reauthorization bill is on this week's calendar for the Thursday markup in this Committee, so I want to thank the Chairman and the co-Chairman again for their assistance on that. And, I understand that you've had a chance to look at the legislation?

Ms. PARNES. I have looked at it, yes.

Senator PRYOR. Do you think it meets the needs of the program? Do you think it is good legislation?

Ms. PARNES. Well, we—the one recommendation that we had is that the reauthorization should statutorily set the fees for accessing the Registry. As the system stands right now, the Commission engages in an annual rulemaking to set the fees, and it just seems as if—from the perspective of the industry, as well as the Commission—having the certainty of a set fee would be very useful.

Senator PRYOR. OK, thank you for that.

Let me also ask this: with the laws that currently exist there—when you register, you register for 5 years, is that right?

Ms. PARNES. Yes.

Senator PRYOR. So, you're going to start to see the people who registered initially to sunset here soon. Do you have a sense of how many will sunset in the first year? Do you know that number off the top of your head?

Ms. PARNES. I don't.

Senator PRYOR. OK.

Ms. PARNES. But I'm certain—I'm actually certain that we can easily get that—

Senator PRYOR. That's really more of a background for my question—

Ms. PARNES.—for you.

Senator PRYOR.—and that is, what will the Federal Trade Commission do to try to educate consumers that their registration will expire and that they need to re-register. Do we have any plans for that?

Ms. PARNES. We do. We were very sensitive to the need to roll out the Do Not Call Registry very carefully when it was just implemented. And we—I think—did a very good job of explaining the Registry, and getting the word out to consumers—I believe in the first two or 3 days, before people even, you know, knew how well this was going to work, we registered over 10 million phones. So, we will put together a consumer education campaign, and we will

definitely reach out to the media, both local and national, to get the word out about re-registration.

Senator PRYOR. Great. Well, thank you because on that type of program, consumer information is very critical.

Let me ask now, let me change gears and ask about CROA. I know that this is something that you're also very familiar with, and you've been very helpful in providing your insights to the Committee, and to my staff, and I appreciate that.

You may not know off the top of your head, but how many cases have you brought under CROA, do you know?

Ms. PARNES. I believe that the FTC alone has brought about 60 cases in the last 9 or 10 years, but working together with our law enforcement partners on the Federal and State level, we've participated in sweeps, and in total, we've brought over 100 cases.

Senator PRYOR. All right, now, many people—including yourself—have expressed reservations about credit monitoring services being subject to specific requirements under CROA. A number of proposals have been suggested and offered to amend this aspect of CROA, including carve-outs for specific entities and carve-outs for specific practices. In this debate, tell us where you are on those issues, and why?

Ms. PARNES. Of course credit monitoring services, as you mentioned, can be very useful for consumers. And we understand the credit reporting agencies have offered these services, and have expressed concern about coverage under CROA. And while we are—and have been—very sympathetic about this, it's been very difficult to come up with some way of crafting an exemption.

We would not favor a status-based exemption for the credit reporting agencies, because it would certainly give them an unfair competitive advantage over others that offer credit monitoring services, and would have to comply with CROA.

And in terms of defining credit monitoring services alone and just carving that out from the statute—our experience with credit repair outfits is that they use every exemption to try and evade the law.

And so, I could easily see your typical fraudulent credit repair guy, you know, setting up a scam that would take advantage of a credit monitoring exemption, and that's really our concern.

Senator PRYOR. So tell me what you think the best approach would be for the new law.

Ms. PARNES. I think that, over the years as we have, as we've really thought about this, we just, you know—so far we have not been able to come up with anything that we could really recommend as carving out an appropriate exemption, and still providing adequate protection to consumers.

Senator PRYOR. OK.

Let's see—you mentioned in your testimony that Congress should continue to reach out to stakeholders in developing any amendments to CROA—do you think that we've found some common ground on changing CROA, or—?

Ms. PARNES. I think the common ground is that, you know, we all agree that—that credit monitoring offered by—I think we all agree with the general principles: Credit monitoring offered by the CRAs doesn't particularly pose a risk to consumers.

I don't think that we've come up with a solution to carve out an exemption from the statute. And, it's something that we will—we would be happy to kind of head to, yet again. But, but we've certainly tried to—and haven't yet—come up with a fix there.

Senator PRYOR. OK, great.

I'd like to move onto the second panel. I want to thank you for your responses to questions. I want to leave the record open for 2 weeks and allow my colleagues to submit questions in writing. And so, don't be shocked if you receive some written questions from the Committee. I know that we have a hectic day in the Senate today, with a lot of things happening on the floor and other Committees meeting. So, my colleagues are trying to get here as best they can.

But, thank you. Your statement will be made part of the record. You're free to go.

Ms. PARNES. Thank you very much.

Senator PRYOR. We'll get the second panel up here.

Thank you. Thank you for your time and your testimony.

Now, I'd like to go ahead and introduce the second panel and call everyone's name. And I'd like to put them in this order, if possible: Mr. Richard Johnson, Member of the Board of Directors at AARP; Mr. Jerry Cerasale, Senior Vice President, Governmental Affairs, Direct Marketing Association; Ms. Robin Holland, Senior Vice President of Global Operations, Equifax; Ms. Joanne Faulkner, testifying on behalf of the National Association of Consumer Advocates; and Mr. Steve St. Clair, Assistant Attorney General for the State of Iowa.

I want to welcome all of you all to the Committee.

I would like to start with Mr. Johnson and Mr. Cerasale. We're going to have 5 minutes to make opening statements, and then we'll have some questions for you. Go ahead.

**STATEMENT OF RICHARD JOHNSON, MEMBER,  
BOARD OF DIRECTORS, AARP**

Mr. JOHNSON. Thank you. Chairman Pryor, thank you so much for the opportunity to testify at this important matter.

AARP strongly supported the establishment of the Do Not Call Registry, or the DNCR. And we thank you for your efforts in this area. And we also commend the regulators for their implementation and enforcement of this important consumer protection.

The DNCR is highly successful. The public overwhelmingly views telemarketing sales calls as an invasion of privacy. It is not surprising, then, that as of now, there are 146 million phone numbers registered with the DNCR. Yet, despite the success of the program, more can be done to protect the consumers.

For example, in a 2005 AARP study, 62 percent of the respondents with telephone numbers registered with the DNCR indicated that they still receive more telemarketing calls than they would like.

We urge Congress and regulators do the following:

First, ensure that the DNCR continues to be funded by the telemarketing industry. Taxpayers and consumers should not have to pay for the cost of operating the system.

Second, prohibit all unsolicited, pre-recorded telemarketing calls, including those to establish business customers. AARP surveys

show that customers and consumers consider pre-recorded telemarketing calls particularly coercive or abusive.

Third, strengthen call-abandonment rules. Telemarketers typically abandon calls when predictive dialing reaches more than one person at the same time. Consumers pick up and hear a click, and older consumers are especially concerned about who was trying to call them. Abandoned calls should include identifying information, in order to remove some of the uncertainty that currently exists when older persons hear the click.

Fourth, narrow the definition of established business relationships. The current definition is too broad. For example, the consumer who simply inquires about a company's products and services, should not have to deal with incessant telemarketing calls from that company. Regulators should change the definition to require that the relationship be ongoing.

Unfortunately, even these consumer protections cannot stop thieves from committing telemarketing fraud, which is already illegal. In our written testimony, we provided statistics to show that telemarketing fraud is largely targeted at older Americans, who have a lifetime of savings that the thieves go after.

Real people behind the statistics bear the burden of this fraud. Consider a few examples: Richard Guthrie was a 92-year-old Army veteran, living on just \$800 in Social Security benefits each month. InfoUSA, a company which compiles vast databases of consumer information, sold Mr. Guthrie's information to thieves, who defrauded him of \$100,000 in a telemarketing fraud.

In another case, 86-year-old Claire Wilson was desperate for money when her son-in-law needed a liver transplant. She was conned out of \$8,000 in savings, after receiving a call that she had won \$100,000 in a Canadian lottery.

These are just a few of the thousands of examples of older Americans who have suffered because of telemarketing fraud.

There are clearly many issues for Congress, regulators and the states to address. One of the key areas for Congress to investigate and potentially take action on, relates to how thieves get money from the victims' bank accounts. Often, this happens through demand drafts, unsigned paper checks.

Demand drafts are so often connected to fraudulent transactions, that Attorneys General in 35 states, plus the District of Columbia and American Samoa, have called for an outright ban on them. AARP also believes that the FTC should strengthen the Telemarketing Sales Rule to address problems that remain, including unauthorized access to consumer bank accounts, disclosures regarding premiums, and prize promotions, repeat calling of telemarketing fraud victims, and the contacting of consumers who have placed their telephone numbers on the DNCR. Additional civil and criminal penalties should be imposed for violations of telemarketing laws and regulations, including prison terms for those who knowingly deceive consumers.

In summary, the Do Not Call Registry has been largely successful. But consumers still receive unwanted telemarketing calls. AARP recommends strengthening the DNCR with additional consumer protections. Federal and State lawmakers should work together to establish a strong set of anti-telemarketing fraud laws

and regulations to bring enforcement action against thieves. Thank you.

[The prepared statement of Mr. Johnson follows:

PREPARED STATEMENT OF RICHARD JOHNSON, MEMBER, BOARD OF DIRECTORS, AARP

Chairman Pryor, Ranking Member Sununu, and Members of the Subcommittee, on behalf of AARP's 39 million members, thank you for the opportunity to testify on the Do Not Call Registry (DNCR) and telemarketing fraud.

#### **Do Not Call Registry**

AARP's members are among the millions of Americans who have taken the initiative to place their phone numbers (over 132 million as of 2006)<sup>1</sup> into the DNCR in an effort to reduce the number of unwanted telemarketing calls. Survey results show that the Registry has been very successful from the consumer standpoint. A December 2005 Harris Interactive survey<sup>2</sup> found that 76 percent of respondents had signed up for the Registry, and 92 percent of them had received fewer telemarketing calls.

AARP's own surveys indicate that an overwhelming number of people view telemarketing sales calls as an invasion of privacy and have supported the creation of "do not call" lists as a way to stop these unwanted intrusions.<sup>3</sup> The DNCR is considered one of the best consumer programs ever implemented, and regulators should be commended for their capable implementation and enforcement of this important consumer protection. There is more that can be done to enhance the protections of the DNCR, and AARP believes that it should continue to be funded by the telemarketing industry, rather than by taxpayers or consumers who place their name on the DNCR.

Notwithstanding the success of the DNCR, consumers still believe they receive too many telemarketing calls. For example, in a 2005 study conducted by AARP, 62 percent of respondents with telephone numbers *registered with the DNCR* indicated that they still received more telemarketing calls than they would like. In order to make the DNCR an even bigger success for consumers, the FTC should adopt additional rules to further decrease the number of telemarketing calls.

AARP is pleased that the FTC is considering changes in two areas that could help achieve this outcome: (1) prohibiting all unsolicited prerecorded telemarketing calls, including those from sellers to established business customers, and (2) retaining and strengthening call abandonment measures. AARP recommends that the FTC act to further relieve consumers of unwanted telemarketing calls from companies with which they have an established business relationship.

#### *Prerecorded Telemarketing Calls*

AARP believes that all unsolicited prerecorded telemarketing calls, including those from sellers to established business customers should be prohibited. Consumers consider prerecorded telemarketing calls a particularly "coercive or abusive" infringement on their right to privacy.<sup>4</sup>

AARP believes that the prohibition on prerecorded telemarketing calls should apply whether the calls are received by a person, an answering machine, or a voice mail system. A simple prohibition on prerecorded telemarketing calls is the best course for consumers. AARP has submitted comments to this effect to the FTC in its ongoing proceeding reviewing the Telemarketing Sales Rule.

#### *Retaining and Strengthening Call Abandonment Measures*

Telemarketers typically abandon calls when predictive dialing techniques reach more than one person at the same time; they speak to one person and drop the call to the others who pick up. Unfortunately, in far too many cases, the consumer rushes to pick up the phone only to hear dead air or a click as the phone call is terminated with these "abandoned" calls.

For mid-life and older Americans, these calls are more than just a nuisance. In addition to the inconvenience and risk associated with rushing to answer the tele-

<sup>1</sup>"FTC Annual report to Congress for FY 2006 pursuant to the Do Not Call Implementation Act on the National Do Not Call Registry," page 4. See <http://www.ftc.gov/os/2007/04/P034305FY2006RptOnDNC.pdf>.

<sup>2</sup>Note that the survey was conducted online, which may limit the survey's ability to generalize to the entire (online and offline) population. For more information on the survey, see [http://www.harrisinteractive.com/harris\\_poll/index.asp?PID=627](http://www.harrisinteractive.com/harris_poll/index.asp?PID=627).

<sup>3</sup>2005 AARP Public Policy Institute survey.

<sup>4</sup>2005 AARP Public Policy Institute survey.

phone, there is the uncertainty and concern of the consumer, especially for women living alone. When no one is on the other end of the line, or a consumer hears a “click” when answering the telephone, a number of different scenarios may begin to play out in the individual’s mind. Is the caller attempting to know if the consumer is home alone or away from the home? Was this an important call that the consumer just missed answering? For these reasons, abandoned calls should be required to include some identifying information conveyed to consumers in order to remove some of the uncertainty that currently exists when older persons answer abandoned calls.

AARP is concerned with proposals by industry to change the rules in a way that could increase the number of calls abandoned by telemarketers. A change in the measure for abandoned calls could provide an opportunity for telemarketers to “game” the system and alter call abandonment rates over the course of each calling campaign. Instead, we reiterate our recommendation that the rule be retained and strengthened to provide stronger consumer protections outlined above.

#### *Established Business Relationship Calls*

AARP has continually expressed the concern that the current definition of an “established business relationship” is too broad, increasing the likelihood that consumers get unwanted telemarketing calls. Specifically, we do not believe every contact between a consumer and a business should establish a business relationship between them. For example, a consumer who merely inquires or provides an opinion about a company’s products and services should not be subjected to subsequent telemarketing calls from the company.

We suggest that the FTC change the definition of “established” to require that the relationship be ongoing, *i.e.*, where the consumer has completed a transaction (making a purchase or a payment) with a company within the 12 consecutive months prior to the call. In addition, if a consumer requests placement on a company’s Do Not Call list, that request should be extended to all of the company’s affiliates with whom the consumer does not have an ongoing relationship.

#### **Telemarketing Fraud**

Despite the success of the Registry, and the requirement that telemarketers review their lists against the DNCR every month, telemarketing fraud—in particular, fraud targeting older Americans—remains a major problem. Thieves continue to evade the law to commit fraud that can potentially wipe out the lifetime savings of unsuspecting older Americans.

According to the National Consumer League,<sup>5</sup> 50 percent of telemarketing fraud victims were 50 or older and 32 percent were 60 or older. At the other end of the spectrum, people under 30 represented just 15 percent of all telemarketing fraud reports, and those under 20 just 1 percent. The NCL statistics also show that 46 percent of thieves initially target people by phone, suggesting that even in the age of the Internet, telemarketing fraud remains a significant problem. AARP research sheds light on part of the reason that seniors are targeted in telemarketing fraud schemes: most older victims do not realize that the voice on the phone could belong to someone who is trying to steal their money.<sup>6</sup>

In 2005, the average reported loss for telemarketing fraud was \$2,892.<sup>7</sup> The Federal Trade Commission estimates that consumers lose \$40 billion a year in telemarketing fraud, and the FBI estimates that there are 14,000 illegal telephone sales operations active each day.<sup>8</sup> But behind the statistics are real people who are scammed—sometimes out of their entire life savings. Consider the following:

- A recent *New York Times* story highlighted telemarketing fraud against Richard Guthrie, a 92-year-old Army veteran living off of approximately \$800 in Social Security benefits each month. He said that he once enjoyed telemarketing calls because they helped stem the loneliness he had felt since his wife’s death.<sup>9</sup> infoUSA, a company which compiles vast databases of consumer information, sold Mr. Guthrie’s information to thieves who defrauded him of \$100,000 through telemarketing.

<sup>5</sup> See <http://fraud.org/stats/2006/telemarketing.pdf>.

<sup>6</sup> *Off the Hook: Reducing Participation in Telemarketing Fraud*, AARP Foundation, 2003. See [http://assets.aarp.org/rgcenter/consume/d17812\\_fraud.pdf](http://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf).

<sup>7</sup> See [http://www.fraud.org/toolbox/2005\\_Telemarketing\\_Fraud\\_Report.pdf](http://www.fraud.org/toolbox/2005_Telemarketing_Fraud_Report.pdf).

<sup>8</sup> See <http://www.ftc.gov/os/comments/dncpapercomments/04/lsap3.pdf>.

<sup>9</sup> “Bilking the Elderly, With a Corporate Assist,” by Charles Duhigg, *New York Times*, May 20, 2007. See <http://www.nytimes.com/2007/05/20/business/20tele.html?ex=1337313600&en=38f9ae54aac348d4&ei=5090>.

- 86-year-old Claire Wilson, desperate for money when her son-in-law needed a liver transplant, was conned out of \$8,000 in savings after receiving a call that she had “won” \$100,000 in a Canadian lottery.<sup>10</sup> The Canadian lottery scam is one of the Federal Trade Commission’s top two scams, costing unsuspecting Americans \$120 million each year.<sup>11</sup>
- Patricia Candelaria, 83, fell prey to a similar scam, paying nearly \$200,000 on supposed taxes and insurance for a sweepstakes prize that did not exist.<sup>12</sup> The supposed contest representative, who identified himself as David Sommers of the National Contest Association, called Ms. Candelaria incessantly and sent her invoices for past due payments.
- 50-year-old Yvette Jones, a single mother and office worker, was scammed by someone who identified herself as Lisa James of the Department of Housing and Urban Development.<sup>13</sup> Jones had submitted several applications for what she thought were government grants to cover the cost of her new roof, and the fraudster told Ms. Jones that she had been awarded a \$5,500 grant that required a \$349 application fee. Ms. Jones paid it but of course never received the grant. She later found out that she had visited bogus websites that had put her information into “sucker lists.”

Telemarketing fraud is already illegal, but more can and should be done. One of the issues we recommend Congress study and potentially take action on relates to how thieves are able to take money out of their victims’ bank accounts. Often, this happens through “demand drafts,” unsigned paper checks that state “authorized by drawer” or “signature on file” in lieu of the signature. The FTC addressed the use of demand drafts to commit fraud in testimony before the Senate Banking Committee:

Demand draft fraud, or the unauthorized debiting of a consumer’s checking account, is a growing problem. Currently, it is the favorite method of fraudulent actors for taking consumers’ money through fraudulent telemarketing and other scams. . . .

Many fraudulent actors persuade consumers, either over the telephone or through the mail, to divulge their checking account numbers by telling them that their bank account numbers are needed to verify prizes or to deposit prize money directly into consumers’ bank accounts. In other cases, fraudulent actors tell consumers that only a small amount will be withdrawn, but in fact withdraw huge amounts of money from the consumer’s checking account. As a further insult, the unauthorized demand draft may generate significant overdraft charges to the consumer if the consumer does not have the additional money in the first instance or has written subsequent checks. Little do consumers know that once they give fraudulent actors access to their bank account information, their money will disappear.<sup>14</sup>

Demand drafts are currently the subject of a case against Payment Processing Center (PPC) brought by the U.S. attorney in Philadelphia. According to this lawsuit, fraudulent telemarketers deposited \$142 million in demand drafts from PPC into their bank accounts.<sup>15</sup>

Demand drafts, unlike Automated Clearing House (ACH) debits, are not subject to the rules of the National Automated Clearing House Association (NACHA). Attorneys General in 35 states plus the District of Columbia and American Samoa have called for an outright ban on demand drafts because they are so frequently used to commit fraud against consumers.<sup>16</sup> This is clearly an issue ripe for further consideration by Congress.

<sup>10</sup>“Can’t Win for Losing,” By Carole Fleck, *AARP Bulletin*, December 2004. See <http://www.aarp.org/bulletin/consumer/a2004-12-09-cantwin.html>.

<sup>11</sup>For more information on this scam, see <http://www.ftc.gov/bcp/online/pubs/alerts/intlalrt.pdf>.

<sup>12</sup>“Scam Alert: Misplaced Trust,” by Sid Kirchheimer, *AARP Bulletin*, July August 2007. See [http://www.aarp.org/bulletin/consumer/scam\\_alert\\_misplaced\\_trust.html](http://www.aarp.org/bulletin/consumer/scam_alert_misplaced_trust.html).

<sup>13</sup>“Scam Alert: Uncle Sham Wants you,” by Sid Kirchheimer, *AARP Bulletin*, December 2006.

<sup>14</sup>Prepared Statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC, before the Senate Banking Committee on 4/15/06. See <http://www.ftc.gov/speeches/other/ddraft.shtm>.

<sup>15</sup>“Bilking the Elderly, With a Corporate Assist,” by Charles Duhigg, *New York Times*, May 20, 2007, at <http://www.nytimes.com/2007/05/20/business/20tele.html?ex=1337313600&en=38f9ae54aac348d4&ei=5090>.

<sup>16</sup>See complaint in *Mary Faloney v. Wachovia Bank*, U.S. District Court for the Eastern District of Pennsylvania, at <http://www.langergrogan.com/LangerGrogan/home.nsf/wachovia.pdf>.

AARP believes that the FTC should strengthen the Telemarketing Sales Rule. Rulemaking and enforcement efforts should address problems that remain in the telemarketing industry, such as online fraud, unauthorized access to consumer bank accounts, disclosures regarding premiums and prize promotions, repeat calling of telemarketing fraud victims, and the contacting of consumers who have placed themselves on the DNCR. The Department of Justice should also be vigorous in enforcing efforts to combat telemarketing fraud.

Civil and criminal penalties should be imposed for violations of telemarketing laws and regulations, including prison terms for those who knowingly deceive consumers. These penalties should be assessed based on the degree of fraud committed, regardless of the actual dollar amount lost. Appropriate investigative and enforcement tools should also be available to regulators.

States are also key players in this area. Because of the serious gap in consumer protections in the area of telemarketing, states play an invaluable role in preventing, deterring, and prosecuting telemarketing fraud. Reducing the pervasiveness of telemarketing fraud and obtaining restitution for victims requires strong enforcement by all levels of government.

#### **Summary**

In summary, the Do Not Call Registry has been largely successful, but AARP recommends additional consumer protections. Such protections include the prohibition of all unsolicited prerecorded telemarketing calls and narrowing of the definition of "established business relationship." We also believe that industry should continue to fund the DNCR; this cost should not be borne by taxpayers or consumers who place their name on the Registry.

Despite the success of the DNCR, telemarketing fraud remains a significant problem for older Americans, who are targeted because of their higher level of savings than the general population. Federal and state lawmakers need to work together to establish a strong set of anti-telemarketing fraud laws and regulations and to bring enforcement actions against thieves.

Senator PRYOR. Thank you.  
Mr. Cerasale?

#### **STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.**

Mr. CERASALE. Thank you, Chairman Pryor. Thank you very much for inviting us here, the Direct Marketing Association is an association of multi-channel marketers, their suppliers, use the mail, the Internet, television, radio and telephone to reach customers, and potential customers. These issues today are important to them, as they try and reach those customers.

We thank you for your leadership concerning the fees for the Do Not Call list, which has been very, very successful. Since its inception in October of 2003, when there were 56 million phone numbers on the list at that time—less than 4 years ago—fees grew from \$7,300-plus to \$17,000—about 263 percent. If you look at 2002, with the estimated \$3,000 fee, the increase is double that 263 percent.

The DMA has run a Do Not Call Registry, and still does it for three States, with a cost of \$700 a year. Now, granted it has a smaller number of phone numbers on it. But that \$700 would include a supplier purchasing it for all of its customers, not each customer having to purchase that \$700. We believe that the fees should cover the cost of running the Do Not Call Registry. It should not be a tax on marketers, to cover other Federal Trade Commission programs. And we support your efforts to put a cap—set the fee with a cost-of-living, or CPI index increase.

Moreover, one other problem with the list is the hygiene of the list. Our members tell us that 30 to 40 percent of the phone num-

bers on the list are not usable—meaning they are business numbers, they are fax numbers, they are abandoned telephone numbers that have not been removed from the list, and they also—as Ms. Parnes said—include cell phone numbers, which are covered by the TCPA, and can be added on here, but increase the size of the list, increase the cost of the list to marketers, to the Government, and increase the probability of errors, as you have more and more numbers. So, we hope that we can do something to try and increase the hygiene of this list.

We don't know the specifics underlying the article in *The New York Times* which promoted—prompted Senator McCaskill to write her letter to the Federal Trade Commission. But the DMA has a longstanding, self-regulatory program, which looks toward correction—correction of errors in trying to fix it. If there is no cooperation, the DMA will then publicize the name of the company, take other corrective actions, such as removing them from the DMA membership publicly, transferring the information to the appropriate authorities.

Two years ago, the DMA was concerned with the issue of list compilers, and trying to clarify its guidelines for them, and we started a revision process, which we have since completed. In the area of sensitive information, which we define as including seniors, we now require—for DMA membership and all list compilers—examine the promotion for appropriateness, so that we ensure that the compiler themselves has a duty—an affirmative duty, in sensitive information—to take a look at what the offer is. We hope that this will strengthen our guidelines, and clarify the guidelines for compilers, and try and help reduce fraud initially, right away, in this process.

These individuals are the customers of our members—or potential customers of our members. They have to treat them as such, and that's what our guidelines are meant to do, and try and push forward ethical business practices.

Thank you, and we're ready for any questions.

[The prepared statement of Mr. Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT,  
GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

#### **I. Introduction and Summary**

Good morning, Mr. Chairman and Members of the Committee. I am Jerry Cerasale, Senior Vice President for Government Affairs of the Direct Marketing Association, and I thank you for the opportunity to appear before the Committee today to discuss telemarketing registry fees and responsible practices for compilers of marketing lists.

The Direct Marketing Association, Inc. (“DMA,” [www.the-dma.org](http://www.the-dma.org)) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA and our members appreciate the opportunity to present our views as the Committee considers permanently funding the do-not-call registry, setting fees for

telemarketers to access the registry, and issues related to the operation of the registry. In addition, we would like to address issues relating to list compilers raised by Senator McCaskill and, in that context, describe DMA's list compiler guidelines.

## II. Fees Paid by Telemarketers to Access the Do-Not-Call Registry

DMA strongly supports capping fees imposed on telemarketers to access the do-not-call registry. We thank Senator Pryor for his leadership in this area. Current fees are sufficient and, in fact, we believe, higher than necessary to administer the do-not-call registry. Fees collected from telemarketers should be used to operate the registry and not for broader enforcement of the telemarketing rules or other purposes. Finally, we believe that the operator of the registry should improve the hygiene of the list to ensure it does not include changed telephone numbers.

### A. Current Fees are Sufficient and, in Fact, Higher than Necessary to Administer the Do-Not-Call Registry and Should be Capped

The level of increase in do-not-call registry access fees seen in the last few years makes it clear that Congress needs to establish a cap on the cost for access. In addition, any necessary fee adjustments should be tied to a fixed index such as the consumer price index or the rate of inflation. The Federal Trade Commission ("FTC" or "Commission"), in 2002, proposed to cap the maximum annual fee per telemarketer to obtain access to the entire registry at \$3,000.<sup>1</sup> By the time the Commission made the registry available in 2003, the cost for access had already increased to \$7,375, a 145 percent increase.<sup>2</sup> Less than a year later, the Commission increased fees 67 percent to \$11,000.<sup>3</sup> The following year, the Commission increased fees by 40 percent to \$15,400.<sup>4</sup> In 2006, the Commission increased fees to \$17,050.<sup>5</sup> That was an 11 percent increase. This amounts to a 263 percent increase in 4 years.

DMA has a great deal of experience in operating its own telemarketing suppression list, the Telephone Preference Service ("TPS"), as well as in administering the state lists of Pennsylvania, Maine, and Wyoming.<sup>6</sup> This experience also indicates a much less costly means of running a registry. DMA's entire list was available for entities to purchase for \$700 per year. While the Commission's registry contains many more numbers than does the TPS, we do not believe that the \$17,050 fee—more than 24 times the cost of the TPS—is justified by the incremental costs that correspond to the increased amount of numbers on the registry.

### B. Fees Collected from Telemarketers should be Used Solely to Operate the Registry and not for Broader Enforcement of the Telemarketing Rules or Other Purposes

DMA believes that fees collected for providing access to the registry should be used solely to administer the operations of do-not-call registry. An analysis of the costs to run the registry and the amounts collected by the Commission suggest that a significant amount of the money spent is on enforcement and other costs. DMA does not believe that the registry fees should be used for telemarketing enforcement based on fraud or other violations of the Telemarketing Sales Rule, even where there may also be an incidental violation of the registry. Prior to the establishment of the registry, such enforcement actions were funded from the Commission's general appropriations. DMA does not believe that legitimate, law-abiding telemarketers should bear the burden of funding enforcement against bad actors. This is not the case for other laws administered by the FTC. For example, Internet sites that are targeted to children, which are subject to the Children's Online Privacy Protection Act, do not fund the Commission's enforcement against entities that violate that law. We are very supportive of increased budgets for enforcement by the FTC in telemarketing, as well as other areas such as spam and identity theft. We believe, however, that such additional funding should come from the normal FTC appropriations and not in fees collected from users of the registry.

### C. The Operator of the Registry Should Improve the Hygiene of the List to Ensure it does not Include Changed Telephone Numbers

Finally, DMA would like to bring one additional issue regarding the "hygiene," or accuracy, of the do-not-call registry to the Committee's attention. We are told by our

<sup>1</sup> *Telemarketing Sales Rule User Fees, Notice of Proposed Rulemaking*, 67 Fed. Reg. 37362, at 37364 (May 29, 2002).

<sup>2</sup> *Telemarketing Sales Rule Fees, Final Rule*, 68 Fed. Reg. 45134, at 45141 (July 31, 2003).

<sup>3</sup> *Telemarketing Sales Rule Fees, Final Rule*, 69 Fed. Reg. 45580, at 45584 (July 30, 2004).

<sup>4</sup> *Telemarketing Sales Rule Fees, Final Rule*, 70 Fed. Reg. 43273, at 43275 (July 27, 2005).

<sup>5</sup> *Telemarketing Sales Rule Fees, Final Rule*, 71 Fed. Reg. 43048 (July 31, 2006).

<sup>6</sup> While DMA no longer adds new names to the TPS list, we will continue to operate the list for five more years. DMA, however, does continue to administer the state lists for Pennsylvania, Maine, and Wyoming.

members that 30 percent to 40 percent of the telephone numbers on the registry are included incorrectly, such as dropped numbers, fax numbers, and wireless numbers. We believe that this, in part, results from the fact that there is a significant time lag from when an individual moves and changes their telephone number to the time when that number is removed from the registry. This time period is longer than the amount of time it takes for the phone company to reassign the number. As a result, there are telephone numbers on the registry for households that did not register to be included on it.

This is particularly problematic because many reassigned telephone numbers are given to subscribers who recently have moved to new geographic regions and are, therefore, most likely to respond to telemarketing calls for items such as home security systems, home insurance, lawn care, and newspaper delivery. For this reason, DMA believes that telephone numbers should be removed from the registry as soon as they are dropped by the consumer and before they are reassigned. This would make for a much more accurate list recognizing the desires of consumers and preserving the ability to call households that have not placed their numbers on the registry. We have raised this issue with the FTC and believe that they understand and appreciate our concern. We hope that this concern can be addressed going forward.

### III. Responsibilities of List Compilers

The Committee has asked us to discuss issues related to list compilers. In particular, the Committee requested testimony on this issue in response to a May 23, 2007 letter that Senator McCaskill sent to the Chairman regarding a May 20, 2007 *New York Times* article entitled “Bilking the Elderly, With a Corporate Assist.” We completely agree with the Senator’s concerns about the types of practices alleged in the article.

DMA fully supports responsible practices by compilers of marketing lists, and has long been a leader in establishing comprehensive self-regulatory guidelines for its members on important issues related to telemarketing, among many others. Understanding the importance of standards and best practices in protecting consumer welfare, DMA, in June 2007, working with its members, adopted guidelines for database compilers as part of our Guidelines for Ethical Business Practice (“Guidelines”).<sup>7</sup>

These guidelines were developed over the course of the past year through the DMA process for guideline establishment. We believe that these guidelines will go a long way to prevent illegitimate marketing practices that threaten to undermine relationships between consumers and marketers. In our experience, industry guidelines are the most effective way to address evolving marketing practices while being sensitive to consumer welfare. Such guidelines are flexible and adaptable in a timely manner so as to address bad practices and not unintentionally or unnecessarily cover legitimate actors.

In her letter, Senator McCaskill expressed concern about the use of seniors’ personal information for fraudulent purposes to exploit seniors for financial gain. We could not agree more with the Senator that seniors and other groups of individuals should not be exploited based on such vulnerabilities. Our guidelines have always prohibited such conduct, and we believe that our list compiler guidelines directly address concerns about seniors by further clarifying that such lists must only be used for appropriate purposes and defining new duties for list compilers.

Specifically, as I will describe in more detail below, these guidelines require that for sensitive marketing data, which includes data pertaining to children, older adults, health care or treatment, account numbers, or financial transactions, compilers should review materials to be used in promotions to help ensure that their customers’ use of the data is both appropriate and in accordance with their stated purpose.

This list compiler guidelines define additional appropriate standards for companies that assemble personally identifiable information about customers for the purpose of facilitating renting, selling, or exchanging information to non-affiliated third-party organizations for marketing purposes. These guidelines require, among other things, as a condition of DMA membership, that companies that compile and sell marketing lists adhere to the following practices:

- establish contractual agreements with customers that define the rights and responsibilities of the compiler and customer with respect to the use of marketing data;

<sup>7</sup> Responsibilities of Database Compilers, DMA Guidelines for Ethical Business Practice, Article #36, (attached).

- suppress the consumer's information, upon request, from the compiler's database;
- prohibit an end-user marketer from not divulging the database compiler as the source of the marketer's information;
- explain to consumers the nature and types of sources they use to compile marketing databases;
- include language in their contractual agreements that requires compliance with applicable laws and DMA guidelines;
- require customers to state the purpose for which the data will be used;
- use marketing data only for marketing purposes; and
- monitor, through seeding or other means, the use of their marketing databases to ensure that customers use them in accordance with their stated purpose.

\* \* \* \* \*

Thank you for your time and the opportunity to speak before the Committee. I look forward to your questions, and to working with the Committee on these issues.

#### ATTACHMENT

### Responsibilities of Database Compilers

#### Article #36

For purposes of this guideline, a *database compiler* is a company that assembles personally identifiable information about consumers (with whom the compiler has no direct relationship) for the purpose of facilitating renting, selling, or exchanging the information to non-affiliated third party organizations for marketing purposes. *Customer* refers to those marketers that use the database compiler's data. *Consumer* refers to the subject of the data.

Database compilers should:

- Establish written (or electronic) agreements with customers that define the rights and responsibilities of the compiler and customer with respect to the use of marketing data.
- Upon a consumer's request, and within a reasonable time, suppress the consumer's information from the compiler's and/or the applicable customer's database made available to customers for prospecting.
- Not prohibit an end-user marketer from divulging the database compiler as the source of the marketer's information.
- At a minimum, explain to consumers, upon their request for source information, the nature and types of sources they use to compile marketing databases.
- Include language in their written (or electronic) agreements with DMA member customers that requires compliance with applicable laws and DMA guidelines. For non-DMA member customers they should require compliance with applicable laws and encourage compliance with DMA's guidelines. In both instances, customers should agree *before* using the marketing data.
- Require customers to state the purpose for which the data will be used.
- Use marketing data only for marketing purposes. If the data are non-marketing data but are used for marketing purposes, they should be treated as marketing data for purposes of this guideline.
- For sensitive marketing data, compilers should review materials to be used in promotions to help ensure that their customers' use of the data is both appropriate and in accordance with their stated purpose. Sensitive marketing data include data pertaining to children, older adults, health care or treatment, account numbers, or financial transactions.
- Randomly monitor, through seeding or other means, the use of their marketing databases to ensure that customers use them in accordance with their stated purpose.
- If a database compiler is or becomes aware that a customer is using consumer data in a way that violates the law and/or DMA's ethics guidelines, it should contact the customer and require compliance for any continued data usage, or refuse to sell the data and/or refer the matter to the DMA and/or a law enforcement agency.

Senator PRYOR. Thank you.

Ms. Holland?

**STATEMENT OF ROBIN HOLLAND, SENIOR VICE PRESIDENT,  
GLOBAL OPERATIONS, EQUIFAX INC.**

Ms. HOLLAND. Thank you for the opportunity to testify on behalf of Equifax, and in support of the reform of the Credit Repair Organizations Act, or CROA. We have submitted written testimony for the record, but I'd like to take a few minutes to highlight that testimony.

Let me first say a quick word about Equifax. Equifax is the oldest, the largest, and the only domestically publicly traded national credit bureau. Equifax is proud of its history, and proud of its services, including its credit monitoring services. We are proud of these services, because they have proven to help consumers to understand their credit score and their credit report, to better manage their use of credit, and to help consumers guard against identity fraud.

Let me emphasize at the outset that Equifax very much supports CROA and its comprehensive and strict regulation of credit repair organizations. These organizations routinely make promises to consumers that they cannot deliver on. They tell consumers they will help them to improve their credit score, or their credit report, by removing adverse—but nonetheless, accurate and timely—information from their reports. This is a deceptive and fraudulent, and ultimately quite incorrect, representation, and the victims are both the consumers and the national credit bureaus, including Equifax.

Ironically, however, CROA has been used wrongly and inappropriately to attempt to punish consumer reporting agencies for offering credit monitoring products. Let me be very clear about the difference between credit monitoring products and so-called “credit repair services.”

Credit monitoring products—including the product offered by Equifax—allow consumers access to their credit reports and credit scores, provide proactive notifications of changes in their reports and scores, provide an explanation of scoring algorithms, and provide consumers with a number of credit score-related tools. Simply stated, monitoring products are the very best strategy to promote consumer financial literacy, and they are also consumers' very best strategy to prevent and mitigate the cruel impact of identity theft.

CROA's definition of a credit repair service is so broad, that it can arguably, but wrongly, be interpreted as covering any of these vital credit monitoring services, because these services, directly or indirectly, can be used to improve a consumer's credit record, credit history, or credit score.

CROA defines a “credit repair organization” as an entity which purports—directly or indirectly—to help consumers improve their credit record. For this reason, Equifax urges the Senate to enact legislation to make absolutely clear that credit monitoring is not credit repair.

The FTC has expressed the same sentiment—that there is no basis for applying CROA to credit monitoring services. If CROA were to be misapplied to credit monitoring services, it would mean that consumers would be unable to buy these services on a subscription basis; that consumers would receive notices and warnings

which are appropriate for consumers faced with sales pitches for credit repair services, but entirely inappropriate—indeed, confusing and deceptive—when applied to credit monitoring service; and it would mean that entities offering credit monitoring services would potentially be faced with liability that could include the disgorgement of all monies paid by all persons in a class action suit, at least. Quite frankly, this would virtually drive credit monitoring services out of the marketplace. It is for this reason that we, very much, appreciate this Committee’s interest in CROA reform.

We also appreciate efforts in the House, where bipartisan legislation has been introduced that makes clear that credit monitoring activities are not credit repair activities. The House bill also provides consumers with additional protection, including a very detailed description of their free report rights, and ID fraud protections under FACTA and the Fair Credit Reporting Act. And it further gives the consumer the ability to cancel a credit monitoring contract with a right to a pro rata refund.

This is a time when concerns about identity theft are at an all-time high, and when the need to improve consumers’ credit and financial literacy has never been greater. This is the time—now is the time—to enact CROA reform.

Thank you for the opportunity to testify, and I’d be happy to answer any questions.

[The prepared statement of Ms. Holland follows:

PREPARED STATEMENT OF ROBIN HOLLAND, SENIOR VICE PRESIDENT,  
GLOBAL OPERATIONS, EQUIFAX INC.

#### **Introduction**

Mr. Chairman and Members of the Committee, I am Robin Holland, Senior Vice President, Global Operations for Equifax. I want to thank you for this opportunity to testify regarding the Credit Repair Organizations Act, frequently referred to as CROA. I commend your efforts, Mr. Chairman, the Members of the Committee and your excellent staff for taking up the long-overdue issue of CROA reform.

In this statement, I briefly describe Equifax; the original reasons for CROA’s enactment; the credit monitoring products that Equifax has developed since the passage of CROA to assist consumers to understand their credit histories and to protect their credit histories from fraud and identity theft; and the CROA reforms that, we believe, should be put into place to protect these vital credit monitoring services and to protect consumers.

#### **Equifax**

Founded in 1899, Equifax is the oldest, the largest, and the only publicly traded of the national companies that provide consumer information for credit and other risk assessment decisions. As one of the three “national” credit bureaus, Equifax’s activities are highly regulated under the Fair Credit Reporting Act (FCRA) and dozens of other related Federal and state statutes. Equifax is a responsible steward of sensitive consumer information and, as such, is committed to consumer privacy. We have been steadfast in working with governments, consumers, and businesses to forge effective solutions to complex information and privacy issues. Equifax believes that the marketplace can offer solutions that enlighten, enable and empower consumers. Equifax has developed products, such as credit monitoring products, which directly assist consumers in understanding their credit files and in empowering them to prevent identity theft and to manage their financial health.

#### **The Credit Repair Organizations Act (CROA)**

In 1996, Congress enacted CROA to address the consumer threat posed by credit repair organizations, commercial entities which charge consumers for providing services that purportedly would improve a consumer’s credit record, credit history or credit rating. In our view, promising to alter or remove negative, but accurate and timely, information from a consumer’s credit report constitutes an unfair and deceptive practice that ultimately undermines consumer confidence in the credit re-

porting system. In order to protect the integrity of the credit reporting system, consumer reporting agencies, including Equifax and the other national credit bureaus, urged Congress to enact CROA to attempt to stop these entities from making false promises to consumers about their ability to change or alter accurate and timely data contained in credit reports. CROA imposed a number of appropriately harsh requirements on credit repair organizations, including consumer disclosures about the limits of any possible changes to a credit file.

Thus, CROA's intent is to protect consumers from paying money for a service which, almost by definition, cannot be provided and indirectly, at least, protect consumer reporting agencies and legitimate consumer reporting activities from the deceptive and fraudulent actions of credit repair organizations. Ironically, by crafting an intentionally broad definition of "credit repair organization", CROA's definition of a credit repair organization (any entity which, directly or indirectly, purports to "improve" a consumer's credit record) has been misread to cover credit monitoring products offered by consumer reporting agencies—the very entities that originally sought passage of the legislation.

### **Credit Monitoring**

Accurate credit reports are important to individual consumers and to the economy. Individual consumers who fall victim to identity theft can be denied employment or credit and may be forced to expend significant resources correcting fraudulent credit report information. Further, identity theft ends up costing financial institutions, including the national credit bureaus, well in excess of \$1 billion annually. The Federal Trade Commission (FTC) recommends that consumers regularly review their credit report files to help guard against identity theft.

As public awareness and concern grows over the risk of identity theft, the national credit bureaus have developed products to assist consumers to monitor their credit files and to detect and to prevent identity theft.

The market for providing credit monitoring products is highly competitive in both product features and price. Credit monitoring products offered by the national credit bureaus are widely popular with consumers and recognized as a highly effective consumer protection service by Federal and state consumer protection agencies. These products give consumers a first line of defense against identity theft, and are routinely made available to victims of security breaches. Indeed, credit monitoring has become a staple requirement of most state security breach notification laws. The FTC has explicitly endorsed credit monitoring as part of a consumer strategy to protect against identity theft.

Equifax offers several credit monitoring products, including:

- *Equifax Credit Watch Silver*: provides consumers with weekly credit monitoring of their Equifax credit file, one copy of their Equifax Credit Report™, and identity theft insurance in the amount of \$2,500 per consumer, with a \$250 deductible (not available to consumers in New York), to cover injuries arising from an occurrence of identity theft (subject to limitations and exclusions).
- *Equifax Credit Watch Gold*: provides consumers with daily credit monitoring of their Equifax credit file, unlimited copies of their Equifax Credit Report™, and identity theft insurance in the amount of \$20,000 per consumer (not available to consumers in New York) to cover injuries arising from an occurrence of identity theft (subject to limitations and exclusions).
- *Equifax Credit Watch Gold with 3-in-1 Monitoring*: provides consumers with daily credit monitoring of their Equifax, Experian and Trans Union credit files, unlimited copies of their Equifax Credit Report™, a 3-in-1 Credit Report which provides consumers with their credit history as reported by the three major credit reporting agencies, and identity theft insurance in the amount of \$20,000 per consumer (not available to consumers in New York) to cover injuries arising from an occurrence of identity theft (subject to limitations and exclusions).
- *Score Watch™*: provides consumers with continuous monitoring of their FICO® credit score and notification when a change in their FICO score impacts the interest rate they are likely to receive, detailed explanations for key score changes and specific tips for understanding their score, daily credit monitoring of their Equifax credit file, and two free Score Power® (which include the consumer's Equifax Credit Report™ and FICO credit score).

### **The Need for CROA Reform**

CROA was enacted before any of these recently developed positive and popular consumer education and credit file monitoring products were created. Unfortunately, a broad (and, ultimately, incorrect) interpretation of CROA could include consumer reporting agencies and their credit monitoring products under the definition of cred-

it repair organizations. Inclusion of consumer reporting agencies under CROA restrictions would inappropriately restrict and complicate consumer access to credit file monitoring products and to the beneficial features offered by these products.

Without CROA reform, plaintiffs' class action suits threaten the viability of credit monitoring products. Under CROA, these suits could require the disgorgement of all revenues from the sale of the monitoring products. Several of the first wave of these kinds of lawsuits has been settled, but this kind of litigation is an ongoing threat and, if successful, could drive credit monitoring products from the marketplace or, at the very least, adversely distort their pricing and delivery.

CROA, quite rightly, prohibits the collection of fees before completing the promised service. This requirement is appropriate for credit repair organizations but inappropriate for credit monitoring products which customarily are sold through instant online delivery and an annual subscription.

Further, CROA requires that covered entities provide prospective consumer subscribers with notices that address the inability of credit repair organizations to remove adverse, but accurate, data from a credit report. Warnings against the deceptive practices of credit repair organizations would be confusing and inappropriate if given to a consumer seeking credit monitoring products.

Further, credit repair organizations are subject to a number of appropriately harsh and specific penalties, including a requirement to disgorge all revenues if CROA is violated. These penalties are not appropriate for credit monitoring products.

#### **Proposed Legislation to Reform CROA**

Enforcement authority under CROA was placed with the Federal Trade Commission (FTC). The FTC staff states that it sees no basis for subjecting the sale of credit monitoring and similar educational products and services to CROA.

As you know, the bipartisan House bill (H.R. 2885) being offered by Representatives Paul E. Kanjorski (D-PA) and Ed Royce (R-CA) provides that an entity providing legitimate credit monitoring products, and not credit repair services, would not fall within the definition of a credit repair organization and, therefore, would not be subject to CROA. The bill would also provide for a complete and detailed notice to be sent to consumers on their rights under the Fair Credit Reporting Act, including a right to a free report.

In addition, the House bill guarantees subscribers to credit monitoring products a *pro rata* refund in the event that they cancel their service.

#### **Conclusion**

CROA reform is straight-forward and narrowly tailored to simply effectuate Congress' intent to apply CROA to credit repair organizations and not to other products and services that did not even exist in 1996 and which benefit, rather than harm, consumers. The fraudulent efforts of credit repair agencies harm consumers and the safety and soundness of the credit system. The objective of CROA always was and is to target companies which engage in fraudulent practices such as promising to delete accurate information from a consumer's credit report.

CROA reform, as proposed in the House bill, does not provide a *per se* exemption from CROA for consumer reporting agencies, based simply on their status as consumer reporting agencies. Rather, entities are exempt from CROA only if they do not engage in credit repair activities. Thus, CROA reform does not, in any way, weaken consumers' protections from deceptive practices enforced by the FTC and State Attorneys General which address the activities of credit repair organizations or address unfair or deceptive practices involving credit repair services.

Senator PRYOR. Thank you.  
Ms. Faulkner?

#### **STATEMENT OF JOANNE S. FAULKNER, ATTORNEY ON BEHALF OF THE NATIONAL ASSOCIATION OF CONSUMER ADVOCATES, NATIONAL CONSUMER LAW CENTER, U.S. PIRG, CONSUMER FEDERATION OF AMERICA**

Ms. FAULKNER. Good afternoon, Mr. Chairman. I'm pleased to have the opportunity to testify this afternoon about the Credit Repair Organizations Act for the National Association of Consumer Advocates and our testimony is joined by the National Consumer

Law Center, on behalf of its low-income clients, by U.S. PIRG, and by the Consumer Federation of America.

Credit repair clinics prey on consumers with false promises that they can remove accurate adverse items, such as bankruptcies, chargeoffs, late payments. It cannot be done. Based on publicly available information, we estimate that credit repair clinics are submitting about 4 million meritless disputes per year to the credit bureaus. That means consumers are tossing money down the drain based on false promises, it also means the credit bureaus are diverted from investigating the real disputes, such as identity theft, or mixed files.

The credit repair scam is over two decades old. I attach to my testimony an article from 1988, from *The New York Times*, involving a scam that is still in use today, and that is, flooding the bureaus with meritless disputes.

The strong law that was enacted in 1996, the CROA, was subject to the credit repair clinics immediately looking for loopholes. We have recommended eight improvements in the Act, I'm only going to discuss three of them.

The first loophole is in the Act itself, and that is, the Act says you cannot charge for the credit repair services, until they have been fully performed. What the credit clinics are doing is breaking these services down into baby steps, so that they will charge \$75 for a setup file, they will charge \$40 for a monthly report—even though nothing has been done during that month. So, I think that the CROA needs to be changed to make it clear that the clinic cannot charge for the repair services until the requested improvement has taken place.

The second and third changes we need are external to the statute, so that consumers can enforce the law better. Like other scams, many credit repair organizations are inserting mandatory pre-dispute arbitration clauses in their contracts. That means, whenever there's wrongdoing, and the consumer wants to rectify it, it's swept under the rug, because it's in secret proceedings before some arbitration forum.

The other thing they're doing is imposing distant forum clauses, which means that a consumer from Connecticut, for instance, would have to go to Washington State in order to enforce his or her rights. Those two things are external to the statute, the statute needs to be amended to protect consumers to limit those.

Credit monitoring from the consumer perspective should not be exempt. Credit bureaus already have the grave responsibility to monitor credit reports, to make sure they are accurate, and to prevent mixed files and identity theft.

What credit monitoring services do is make the consumer pay for monitoring their own credit report, even though credit bureaus are supposed to be doing that for free. We think credit monitoring should not be exempted, because, mainly because the credit repair clinics will find another loophole, as sure as can be.

And second, in my testimony, there are examples of the Federal Trade Commission going after some of these credit monitoring services for deceptive practices. No one should be exempt from the deceptive practices prohibited by CROA.

The credit reporting system is largely broken. And one of the reasons is the drain on consumer resources, and on credit bureau resources, caused by these credit clinics. They must be stopped.

We urge you to strengthen the laws to prevent exploitation of both consumers, and credit bureaus. Thank you.

[The prepared statement of Ms. Faulkner follows:]

PREPARED STATEMENT OF JOANNE S. FAULKNER, ATTORNEY ON BEHALF OF THE NATIONAL ASSOCIATION OF CONSUMER ADVOCATES, NATIONAL CONSUMER LAW CENTER, U.S. PIRG, CONSUMER FEDERATION OF AMERICA

Chairman Inouye, Vice Chairman Stevens and other distinguished Members of the Commerce, Science, and Transportation Committee, thank you for inviting me to testify today in this important hearing to consider the improvements necessary for the effective implementation of the Credit Repair Organizations Act. I offer this testimony today on behalf of the National Association of Consumer Advocates, the low income clients of the National Consumer Law Center, U.S. PIRG, and Consumer Federation of America. We oppose changing the Act to protect credit monitoring services since the proposed changes instead facilitate evasion of the Act's salutary protections by credit repair organizations. Instead, we offer suggestions for improving the Act to strengthen its protections against deceptive credit repair services.

I am Joanne Faulkner, a founding member of NACA. A brief description of my background in consumer protection law, and a description of the consumer organizations named above, is appended.

I have first hand experience in trying to enforce the Credit Repair Organizations Act, 15 U.S.C. § 1679 *et seq.* (CROA). Enforcing the CROA is frustrating, not because of what has been enacted, but because the targets of the law have devised methods of evasion. While the Federal Trade Commission has enforcement power, it does not have the resources to address the burgeoning and emboldened number of entities that prey on already financially overburdened consumers with false promises of credit repair.

The law desperately needs to be strengthened to prevent evasive tactics. If Congress considers watering down the Act by exempting credit monitoring services, the exemption will simply provide a roadmap that will be exploited by those seeking to avoid CROA's protections against deceptive practices.

In order to prevent evasion, and encourage private attorneys to effectively participate in stemming the abuses and dislocations caused by credit repair entities, the CROA should be strengthened. The Act needs:

1. An express prohibition on pre-dispute arbitration clauses, commonly inserted by credit repair organizations (CROs) both to insulate them from liability as well as to keep their deceptive practices out of the public eye and under the rug.
2. A prohibition on distant forum clauses, commonly imposed by CROs to deter consumer enforcement of their rights under the CROA.
3. A provision affirmatively allowing the consumer to sue the CRO in the Federal or state judicial district where the consumer resides irrespective of any contractual provision to the contrary.
4. A provision that the consumer may obtain injunctive relief.
5. A prohibition on any contract provision that prevents class actions, particularly important here because an individual's damages may not be sufficient to interest competent attorney representation.
6. An amendment to § 1679b(4) of the CROA to effectuate the intent of Congress to bar unfair and deceptive practices. Because the word "fraud" is used in that subsection only, some courts are demanding a higher burden of proof and pleading than normally imposed for unfair or deceptive practices.
7. A provision preventing CROs from evading § 1679b(b) by charging for discrete services ("set up fee"; "monthly report on progress" and the like).
8. Non-profits should not be exempt. CROs have set up elaborate structures whereby the consumer contracts with a non-profit "educational" entity but that entity outsources books and services to profit-making friends, relatives and associates.

Moreover, as discussed below, we strongly oppose weakening the CROA by enacting the deceptively named "Credit Monitoring Clarification Act," H.R. 2885, which

is virtually identical to last year's Senate companion bill, S. 3662. This bill would allow almost any business currently covered by CROA to escape the Act's important protections. Even a slight change in description from promising to "improve credit" to providing "access to credit reports, credit monitoring notifications, credit scores . . . , any analysis, evaluation or explanation of credit scores . . ." would mean that CROA's current strict prohibition against deception would no longer apply to entities abusing the consumer, deceiving the credit bureaus, and harming the economy.

*Abuses by the Credit Repair Industry continue and cry out for a stronger CROA*

Congress has found that "the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system." Fair Credit Reporting Act, 15 U.S.C. § 1681(a)(a). To further that purpose, Congress enacted the CROA, 15 U.S.C. § 1679, finding that "Certain advertising and business practices of some companies engaged in the business of credit repair services have worked a financial hardship upon consumers, particularly those of limited economic means and who are inexperienced in credit matters." 15 U.S.C. § 1679(a)(2). The CROA was enacted "to protect the public from unfair or deceptive advertising and business practices by credit repair organizations." § 1679(b)(2).

"As Americans' reliance on credit has increased, so-called 'credit repair clinics' have emerged, preying on individuals desperate to improve their credit records. These organizations typically promise they can have any negative information removed permanently from any credit report . . . for a fee." *FTC v. Gill*, 265 F.3d 944, 947 (9th Cir. 2001) (sanctions against lawyer operating credit repair clinic in violation of CROA). Because of well-known abuses, thirty eight states have also enacted laws restricting credit repair operations, including my state of Connecticut, Conn. Gen. Stat § 36a-700.

CROs are designed to undermine accurate credit reporting. Despite the CROA, the CROs have established elaborate ruses to intentionally profit from obtaining payment before credit repair services are fully performed. Some intentionally solicit consumers on the representation that a law firm is involved, and that consumers will benefit by being represented by a law firm. CROs intentionally and systematically deceive credit bureaus about the source and nature of the dispute correspondence, and intentionally deceive consumers before and during the course of their representation.

The CROs' volume of mailings to the credit bureaus causes harm to the credit reporting system because of the resources of bureau staff and time devoted to responding to the volume of letters generated by CROs, as well as the dislocation of bureau efforts from the disputes of individuals who have legitimate accuracy complaints, such as victims of identity theft or of mixed files (similar names). The volume and spurious nature of the disputes sent by CROs intentionally interferes with the credit bureaus' business of providing accurate reports. These practices ultimately cause creditors to extend credit in reliance on credit bureau reports that are not accurate because the CROs' dispute volume is intended to force bureaus to delete tradelines that they cannot investigate within thirty days. The CROs' systematic deception of the credit bureaus and of consumers undermines the banking system and harms consumers and creditors alike. Appended to this testimony is a 1988 *New York Times* article recognizing the type of abusive practices that are still taking place today.

Let me quote from the testimony of Stuart K. Pratt, President of the Consumer Data Industry Association, before the House Committee on Financial Services (June 19, 2007), showing credit repair is an ongoing and still significant problem:

Historically credit repair operators would promise to delete accurate but negative data from a consumer's file for fees that in some cases exceeded \$1,000. Their primary tactic was to flood the reinvestigation system with repeated disputes of the same negative data in an effort to "break" the system and cause the data furnisher to both give up and not respond or to simply direct the consumer reporting agency to delete the data. Today, operators are savvier and often avoid making false promises but even now they suggest that they will assist the consumer with disputing inaccurate or unverifiable information. In many cases "unverifiable" equates to the same practice of flooding the system and trying to have accurate, predictive derogatory data removed.

Our members estimate that on average across our members operating as nationwide consumer reporting agencies, no less than 30 percent of disputes filed are tied to credit repair. Repetitive disputes can be particularly harmful to smaller data furnishers such as community banks, thrifts, credit unions and re-

tailers. These data sources are often a key to ensuring full and complete data on all credit-active consumers, but their ability to absorb costs is limited. In extreme cases, small-business data sources may simply choose not to report at all if costs of responding to disputes are too high.

Thankfully, no one data source is usually the target of a credit repair operator and credit repair efforts most often end up in failure. But this failure is at a cost to our members and to consumers. Consumers spend money on a service that cannot deliver. Industry incurs costs as well when it has to dedicate resources which could be used to service legitimate disputes, to disputes that are not likely to be valid.

Thus, consumers and credit bureaus alike are eager to strengthen the CROA. The present credit reporting system is broken. Every analysis or study in this decade, including the FACTA authorized FTC Pilot Study has found inaccuracies in a significant percentage of the reports considered. The CROs are one cause of the inaccuracies. The amendments we suggest are essential to stop them, or at least provide a more effective means of deterring noncompliance than we have now.

*CROA has successfully deterred other deceptive credit services*

The CROA should not be watered down because it has also proved useful against entities other than traditional credit repair organizations when those entities have made deceptive claims about improvement of credit history. The Act has been held to apply to:

- Credit counseling agencies that promise to improve participants' credit ratings;
- Debt collectors who offer improvement of the debtor's credit rating in return for payment of the debt (even when the effect is actually to worsen the credit rating);
- A company that generated subprime auto financing leads by advertising that it could restore consumers' credit.

Payday lenders have also operated under the guise of credit services organizations in order to evade state interest rate caps.

**Strengthen CROA By Adding Important Protections**

Rather than weakening the CROA, the Act should be strengthened to ensure that it will protect consumers from deceptive credit repair practices.

*1. Pre-dispute Arbitration Clauses must Be Prohibited*

Arbitration clauses are commonly inserted in contracts by credit repair organizations to insulate them from liability as well as to keep their deceptive practices out of the public eye and under the rug. One court mastered this issue, *Alexander v. U.S. Credit Management, Inc.*, 384 F. Supp. 2d 1003, 1014 (N.D. Tex. 2005), but others have endorsed arbitration clauses. Congress can reduce the volume of litigation over the effectiveness of unilaterally imposed arbitration clauses by prohibiting them in the CROA.

Mandatory pre-dispute arbitration clauses unilaterally imposed by creditors and scam artists alike cause significant harm to consumers, deter and indeed eliminate effective enforcement and keep corporate wrongdoing under the rug and out of the public's scrutiny.

Although arbitration can be a fair and efficient way to resolve a dispute when both parties choose it after the dispute arises, arbitration is particularly hostile to individuals attempting to assert their rights. High administrative fees, and a lack of discovery proceedings, jury trials and other civil due process protections, and meaningful judicial review of arbitrators' decisions all act as barriers to the fair and just resolution of an individual's claim. When arbitration is required rather than voluntarily chosen, the likelihood that these problems will occur and that arbitrators will favor repeat corporate players over individual claimants is increased.

*2. Distant Forum Clauses must Be Prohibited*

CROs commonly include a clause in their contracts requiring that any suit or arbitration be brought in some location distant from the consumer and expensive to travel to. Plainly, this type of provision effectively precludes any effort to enforce the CROA. "Distant forum abuse is 'unconscionable' and 'insidious' conduct employing 'an ostensibly legitimate legal process to deprive consumers of basic opportunities which should be afforded all litigants.'" *Yu v. Signet Bank/Virginia*, 69 Cal. App. 4th 1377, 1389 (1999) (citations omitted). "[M]isuse of the courts in this manner contributes to an undermining of confidence in the judiciary by reinforcing the unfortunate image of courts as 'distant' entities, available only to wealthy or large interests," and leads consumers "to conclude that the legal system is merely a 'rub-

ber stamp' for the improper practices utilized by predatory agencies." *Barquis v. Merchants Collection Assn.*, 7 Cal. 3d 94, 108, 101 Cal. Rptr. 745, 496 P.2d 817 (1972) (filing in a distant venue for the ulterior purpose of impairing consumer's rights to defend the suits to coerce inequitable settlements or default judgments is abuse of process).

In *Spiegel, Inc. v. FTC*, 540 F.2d 287 (7th Cir. 1976), the practice of filing collection lawsuits in distant forums was held unfair and unconscionable. This practice has been attacked successfully in both private and public enforcement actions. *E.g.*, *Schubach v. Household Finance Corporation*, 376 N.E.2d 140, 141-142 (Sup. Jud. Ct. Mass. 1978) (practice unfair or deceptive even when permitted by venue statute); *Celebrezze v. United Research, Inc.*, 482 N.E.2d 1260, 1262 (Ohio App. 1984); *Zanni v. Lippold*, 119 F.R.D. 32 (C.D. Ill. 1988) (class composed of defendants subject to distant forum abuse certified).

The CRO should not be allowed to sue the consumer in a distant forum. The consumer should not be required to sue the CRO in a distant forum.

### 3. Venue must Be Local

Lack of a venue provision is one obvious gap in the provisions of the CROA. Venue is the locale where the consumer can sue or be sued. The CROA should have an affirmative provision, like other subtitles of the Consumer Credit Protection Act, placing the location of lawsuits at the consumer's residence, such as: "An action to enforce any liability credited by this subchapter may be brought in any appropriate United States District Court without regard to the amount in controversy, or in any other court of competent jurisdiction, located in the judicial district or similar legal entity in which the consumer resides at the commencement of the action."

### 4. Injunctive Relief Is Essential

The CROA allows States and the FTC to obtain injunctive relief. By omission, there may be an implication that United States District Courts do not retain their normal injunctive power in individual CROA cases. While it is likely that Congress did not intend to so divest Federal courts of their injunctive powers, any judicial confusion can be corrected with a short addition to the statute expressly acknowledging such a remedy. This would provide a faster and less burdensome remedy for consumers and facilitate their "private attorneys general" in obtaining effective relief.

### 5. Class Action Waivers Should Be Explicitly Disallowed

Another way the CROs reduce their exposure to wrongdoing is by inserting a clause prohibiting class actions, or prohibiting the individual consumer from participating in a class action against the CRO. The CROA allows class actions; it should also override any effort by the CRO to undermine this salutary provision by attempting to preclude class litigation.

The Supreme Court has long recognized that without class actions, claimants with small claims would not be able to obtain relief. See *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797 (1985). "Class actions . . . may permit the plaintiffs to pool claims which would be uneconomical to litigate individually. For example, this lawsuit involves claims averaging about \$100 per plaintiff; most of the plaintiffs would have no realistic day in court if a class action were not available." *Id.* at 809. The 1966 Advisory Committee Notes to Rule 23 echo this concern: "These interests [in individual litigation] may be theoretical rather than practical: . . . the amounts at stake for individuals may be so small that separate suits would be impracticable." Similarly, the leading treatise on class actions has stated:

The desirability of providing recourse for the injured consumer who would otherwise be financially incapable of bringing suit and the deterrent value of class litigation clearly render the class action a viable and important mechanism in challenging fraud on the public.

Newberg, *Class Actions* at §21.30. See also *Watkins v. Simmons and Clark, Inc.* 618 F. 2d 398, 404 (6th Cir. 1980) (class action certifications to enforce compliance with consumer protection laws are "desirable and should be encouraged.")

### 6. The Word "Fraud" Should Be Deleted from § 1679b(4)

The CROA is a broadly worded enactment, a uniquely potent consumer protection statute that both provides for punitive damages and voids the violative contract. The type of intentional conduct required by a fraud standard is taken into account only in determining the amount of punitive damages. Yet, courts unfortunately have been drawn by the word "fraud" in § 1679b(4) to impose a higher burden of pleading and proof on the consumer.

What Congress actually said, and notably the only place the word “fraud” was used, does not require a CROA plaintiff to exclusively plead fraud; the plain language encompasses fraud, but is much broader than that:

(4) engage, directly or *indirectly*, in *any* act, practice, or course of business that constitutes or *results in* the commission of, or an attempt to commit, a fraud or *deception* on any person in connection with the offer or sale of the services of the credit repair organization.

The legislative history shows that the section was meant to prohibit deceptive and unfair practices, even if they do not amount to fraud.<sup>1</sup> The subsection should be reworded to clarify that intent. We suggest the following:

(4) engage, directly or indirectly, in any act, practice, or course of business that INVOLVES ANY FALSE, DECEPTIVE OR MISLEADING REPRESENTATION OR MEANS constitutes or results in the commission of, or an attempt to commit, a fraud or deception on any person in connection with the offer or sale of the services of the credit repair organization.

#### 7. Close the “services” loophole

CROs contract to perform credit repair. However, in order to evade the statutory prohibition on charging before services are rendered, they break services down into each step. They separately charge a set-up fee (setting up the file is a “service”) and a monthly report fee (mindlessly transmitted by computer). Another charge is described as for “time and expense for commencing the representation of the client.” There is a “rush fee” for expedited services. This breakout of each small step in the ultimate service should be prohibited. No money should change hands, in escrow or otherwise, until the credit repair itself is actually performed. We request the following amendment.

1679b(b) Payment in advance.—No credit repair organization may charge or receive any money or other valuable consideration for the performance of any service FOR THE EXPRESS OR IMPLIED PURPOSE OF IMPROVEMENT IN ANY CONSUMER’S CREDIT RECORD, CREDIT HISTORY OR CREDIT RATING which the credit repair organization has agreed to perform for any consumer before such service IMPROVEMENT is fully performed.

#### 8. Non-Profits Should Not Be Exempt

The FTC has sued “educational” entities that have nonprofit status but are structured so that founders and their family and friends have high-price contracts for goods or services sold to the nonprofit. Section 1679a should be amended to at least add a qualifying phrase, “and is not for its own profit or that of any person directly or indirectly associated with the organization.” The change would endorse the thoughtful interpretation limiting the section’s exemption to true nonprofits by the First Circuit Court of Appeals in *Zimmerman v. Cambridge Credit Counseling Corp.*, 409 F.3d 473 (1st Cir. 2005).

#### Deceptive Credit Monitoring Services

Although the national credit bureaus are victims of many credit repair scams, they themselves have also engaged in deceptive practices. The national credit bureaus have developed another new and lucrative profit center based on consumer fear of inaccuracies in credit reports. Each agency markets a credit-monitoring product directly to consumers. As the agency reported to its shareholders on May 23, 2007:

Consumer Direct [*online credit reports, scores and monitoring Services*] delivered excellent growth throughout the period, with strong demand from consumers for credit monitoring services, which led to higher membership rates.

<sup>1</sup>Section 404, as described in H.R. Rep. 104–486, 103d Cong. 2d Sess., 1994 WL 164513 \*57–58.

Section 404 prohibits credit repair organizations from (1) making untrue or misleading statements or advising consumers to make such statements with respect to a consumer’s credit worthiness, credit standing, or credit capacity to a consumer reporting agency or to a person extending credit to the consumer; (2) making statements or advising consumers to make statements to consumer reporting agencies or a person extending credit to the consumer that are intended to alter the consumer’s identification to prevent the display of adverse credit information that is accurate and not obsolete; (3) making or using untrue or misleading representations of the services the credit repair organization can provide; (4) *engaging in deceptive acts*; and (5) charging or receiving payment in advance of fully performing services for the consumer.

In its most recent quarterly filing, the agency reported that its sale of these reports and its credit monitoring products directly to consumers had generated no less than 10 percent of its operating revenue and one-sixth of its credit reporting revenue.

Whether or not their credit monitoring services offer any benefit to consumers, these services have been marketed in a deceptive way to induce consumers to pay for reports they are legally entitled to receive for free, and for fraud monitoring services that the CRAs are already legally obligated to perform. For example, Experian has branded and marketed its misnamed service *www.freecreditreport.com*.

Concerns over these services must be kept in mind because the CRAs are pushing for an exemption from CROA. We strongly oppose such an exemption.

Experian has been penalized twice by the Federal Trade Commission for deceptively linking subscription-based credit monitoring offers to the Federal free annual credit report on request right established by the 2003 FACT Act. In August 2005, *Consumerinfo.com* paid \$950,000 to settle charges by the FTC that Experian offered consumers a free copy of their credit report and “30 FREE days of Credit Check Monitoring” without adequately explaining that after the free trial period for the credit-monitoring service expired, consumers automatically would be charged a \$79.95 annual membership unless they notified the defendant within 30 days to cancel the service. *Consumerinfo.com* billed the credit cards that it had told consumers were “required only to establish your account” and, in some cases, automatically renewed memberships by re-billing consumers without notice. The settlement required *Consumerinfo.com* to pay redress to deceived consumers, barred deceptive and misleading claims about “free” offers, and required clear and conspicuous disclosure of terms and conditions of any “free” offer.

Experian then violated this settlement agreement, and in February 2007 was fined a second time by the FTC for \$300,000 to settle charges that its ads for a “free credit report” continued to fail to disclose adequately that consumers who signed up would be automatically enrolled in a credit-monitoring program and charged \$79.95.

Although *Consumerinfo.com* now contains the disclosures, they are in fine print, and the website implies that the truly free report is not “user-friendly” like the free one that comes with the monitoring service.

Moreover, the main Equifax, TransUnion and Experian websites all are worse. All prominently mention free credit reports with links that lead to a sign up for their paid monitoring service. Although they each have disclosures somewhere about the price and the distinction between the truly free report, they are obscure and easy to overlook. All three websites make it very difficult to learn about how to get a truly free report, and very easy to respond to a prominent “get my free report” link and inadvertently sign up for a paid services.

Beyond the free report, it is not clear what these credit monitoring services offer beyond the CRA’s existing legal duties. The bureaus have been charged by Congress with maintaining “maximum possible accuracy” in consumers’ credit reports. Yet, their credit monitoring services ask the consumer to pay to review the accuracy of their credit files. The bureaus should be preventing identity theft, mixed files, and other errors on their own and without charging the consumer for so doing.

### **Resist Efforts to Weaken CROA**

The variety of forms that deception can take, the creativity of those who would exploit consumer’s concern for their credit rating, and the variety of actors involved, are all a strong warning against creating any loopholes in CROA’s protections against deceptive practices. I have seen a draft of a proposal whose short title is the “Credit Monitoring Clarification Act,” (H.R. 2885). NACA, NCLC and U.S. PIRG and other consumer organizations oppose the bill. The line between an offer to help ensure that credit reports “are accurate and free of fraud,” as on Equifax’s website, and offers to improve a credit report or credit score, covered by CROA, is a fine one. We believe that credit monitoring services should comply with CROA’s protections against deception just like other credit repair services.

Unfortunately, H.R. 2885 opens wide, wide loopholes for CROs as well. The proposed amendment to CROA for credit monitoring activities includes broad and sweeping exemptions. Anyone who characterizes their services as providing “access to credit reports, credit monitoring notifications, credit scores . . . , any analysis, evaluation or explanation of credit scores . . .” would be *exempted* from coverage under CROA as long as they provide a new disclosure and cancellation rights for credit monitoring services. In fact, the business would remain exempt *even if it offered to improve credit scores or modify credit reports*, as long as the offer did not promise to remove accurate items that are not obsolete.

Yet as Stuart Pratt of the Consumer Data Industry Association noted in the testimony quoted above, “Today, operators are savvy and often avoid making false

promises but even now they suggest that they will assist the consumer with disputing inaccurate or unverifiable information. In many cases 'unverifiable' equates to the same practice of flooding the system and trying to have accurate, predictive derogatory data removed."

In other words, any business that is currently defined to be a credit repair organization under CROA could simply escape the coverage of CROA by slightly changing the description of what they do and offering, for example, to provide analyses and projections of a person's credit score. CROA's current strict prohibition against deception and fraud would no longer apply to that business.

Below are some examples of the consumer protections in the current law that would not be available under H.R. 2885.

- When run-of-the-mill *credit repair businesses* deceptively advertise their ability to improve consumers' credit scores by exaggerating what they can accomplish, CROA offers protections against this deception.
- When *debt collectors* collect debts by deceptively promising improvement of a consumer's credit rating, CROA's prohibition against deception can be brought to bear.
- Some *payday lenders* are now advertising themselves as credit repair specialists to evade state restrictions on interest rates; activities to which CROA's protections clearly apply.

Moreover, credit monitoring services—which themselves have been marketed in a deceptive manner—would be completely exempt from CROA's prohibition against untruthful or deceptive practices. In fact, it is not even clear that the CRA's need an exemption from CROA. See *Hillis v. Equifax Consumer Servs.*, 237 F.R.D. 491, 515 (D. Ga. 2006) (discussing why credit monitoring services do not seem to be within CROA, but stating "if a credit reporting firm decides to offer a service that falls within the purview of the CROA, there is no reason that the CROA should not apply").

Thank you for the opportunity to testify. Please feel free to contact me for any additional information.

---

*The New York Times*—July 23, 1988

#### NEED CREDIT? BE WARY OF CLINICS OFFERING HELP

By Leonard Sloane

It was the most extreme case of credit-repair abuse ever uncovered: 9,000 people around the Nation defrauded of about \$2 million they had paid Credit-Rite Inc. to restore their eligibility for various forms of credit. Two of the operators of Credit-Rite, a New Jersey concern, were sentenced to prison terms this week in Federal District Court in Trenton, and the third received a suspended sentence.

Credit-repair clinics are profit-making ventures that, by their very nature, often operate at the edge of the law, thwarting the maintenance of orderly credit records in behalf of clients who have bad credit histories.

The clinics promise to help remove derogatory information from individuals' credit files, and charge as much as \$2,000 for the service. They take advantage of a provision of the Fair Credit Reporting Act that gives consumers the right to challenge the information about them that credit bureaus have on file. This provision requires a credit bureau to verify the information upon request, generally within 30 days. If verification is not completed on time, the disputed data must be deleted.

#### **Company Guaranteed Results**

Charlie Mae McCray of Cleveland testified at the Credit-Rite trial that she had paid more than \$500 to clear up her credit record. The company had guaranteed results, but nothing was done. "I complained, I wrote letters, but I didn't get any response to my satisfaction," she said. "I still haven't received any money back."

Anne C. Singer, the Assistant United States Attorney in New Jersey who handled the Credit-Rite case, said: "It's impossible to perform this service as promised if someone's credit history is correct. The people involved in running these businesses raise the hopes of low- and moderate-income people, and then their hopes are dashed."

In another credit-repair clinic case this week in Los Angeles, the operator of Wise Credit Counselors was convicted and sentenced to probation and community service by a Municipal Court judge, who also ordered full restitution to the 13 victims.

### Corrections Without Fees

Individuals who feel their credit records have inaccuracies can go directly to a local credit bureau and ask that they be corrected. There are also nonprofit credit counseling services around the country that will help consumers develop workable budgets and pay off their bills.

Many credit-repair clinics also promise to obtain credit cards for people who have been refused by card issuers. There are about 30 million such people in the United States, cutoff from such basic transactions as renting a car or making travel reservations because they do not have a card. Cards provided through credit-repair clinics are usually secured by a deposit made by the card holder in the bank that issues the card.

But some banks offer secured cards directly to consumers without charging the hundreds of dollars in application and membership fees exacted by many credit-repair clinics. Beyond that, only 4 out of every 10 applicants who pay fees for secured cards eventually get cards, according to H. Spencer Nilson, the publisher of the *Nilson Report*, a credit-card newsletter in Los Angeles.

But the blizzard of challenges to credit bureaus is the essential operating method of credit-repair clinics.

"The objective is to overwhelm the established system," said Walter R. Kurth, the president of Associated Credit Bureaus, a trade association.

Credit-repair operators do not necessarily disagree. "The credit bureaus have exercised too much power," said Paul Turk, general manager of City Wide Financial Services, a clinic in Los Angeles.

TRW Information Services, a credit-bureau chain based in Orange, Calif., refuses to do business with credit clinics. "We have a procedure in place when we feel consumers have been involved with a credit clinic, whereby we notify them we don't deal with third-party contacts," said Delia Fernandez, a spokeswoman. This policy is being contested in a lawsuit by the American Association of Credit, a Glendale, Calif., clinic. The case is pending. Equifax Inc., which owns a chain of credit bureaus, also makes "every effort to circumvent dealing with clinics," said Annette Aurrecocher, a vice president of the Atlanta company. "But if a clinic has a notarized letter from a consumer, we feel there is an obligation to deal with it."

### 'Fly-by-night' Companies

Bills were proposed in both houses of Congress early last year to restrict the practices of credit-repair clinics, but no hearings have been scheduled. Seventeen states have passed laws regulating the clinics' advertising and business practices, yet residents of those states are often solicited by clinics in nearby states.

"We continue to be very concerned," said Kathleen V. Buffon, the Federal Trade Commission's assistant director of credit practices. "These companies tend to be fly-by-night."

Whether or not consumers use a credit-repair clinic, information that has been correctly recorded in a credit bureau file cannot be permanently removed until the problem is corrected or until the time provided by law has elapsed.

"The only way to acquire a good credit record is to straighten up your act," said Jeanne Hogarth, an assistant professor of consumer economics and housing at Cornell University. "There is no magic wand that these repair clinics can raise."

Senator PRYOR. Thank you.

Mr. St. Clair?

### STATEMENT OF STEVE ST. CLAIR, ASSISTANT ATTORNEY GENERAL, STATE OF IOWA

Mr. ST. CLAIR. Thank you.

I've been asked to address law enforcement efforts directed—

Senator PRYOR. Is your microphone on?

Mr. ST. CLAIR. It should—I think it is.

Senator PRYOR. OK, thank you.

Mr. ST. CLAIR. I've been asked to address law enforcement efforts directed at the facilitators of telemarketing fraud.

Fraudulent telemarketers have been cheating—stealing from Americans, elderly Americans, in particular—for many years. That much, sadly, is a constant. But what has evolved are the techniques, methods, operational details that characterize the par-

ticular scams and schemes of the day. It's been something of an arms race with law enforcement. The authorities develop techniques for preventing, detecting, addressing, apprehending the scammers, and the scammers develop new variations on old themes, in an effort—a continuing effort—to avoid being brought to justice.

Now, about 15 years ago, the Iowa Attorney General's office developed some very effective techniques for capturing on tape some of the fraudulent pitches that were being directed at various elderly citizens of our State, and those pitches were typically being—emanating from other States—Iowa generally supplies the victims, and other States have—used to supply—the telemarketers that would harvest the Iowa victims.

But, things have changed, and since then the predatory telemarketers have moved across international boundaries. So—where before we could capture pitches on tape, and use those tapes to charge, extradite, prosecute, and very seriously deter the telemarketers—fraudulent telemarketers that were calling from other States, now we've been dealing with international boundaries, and the challenges in dealing with international boundaries by State law enforcement, in terms of investigation and prosecution are pronounced, to say the least.

So, increasingly, we tried to focus our attention on the stable, U.S.-based operations that provide something of a platform—or the necessary infrastructure for the telemarketers to operate. The thinking is that by making the facilitators answer for the frauds to which they provide support, they will withdraw that support—in part or in whole—from the dubious operators, and thus make it more difficult for the perpetrators to complete their frauds, to claim their victims.

So, attention has been directed, for example, to banks and to third-party processors that provide the means through which the fraudulent telemarketers can extract money from the accounts of victims. And, attention has also been paid to the list builders, list brokers, list managers that—in effect—help scammers to identify elderly Americans who would be especially vulnerable to being cheated by a stranger over the phone.

List building—list builders, are operations that actually create lists of people vulnerable to being scammed. And, they may do it by sending prospecting mailings, screening mailings, to tens—or hundreds of thousands—of individuals, and they uniformly, in our experience, these mailings promote vague and misleading opportunities to win prizes, sweepstakes, and the like.

So, the prize-oriented mailings ask the consumer to send back to the mailer, a small check—it might be \$20 or so, as an administrative fee, or an acquisition fee, a transfer fee—often a fee they designate in such a way as to suggest that you're paying for processing the prize.

The people who send a check in response to such mailings are prime candidates for further victimization, which is the whole point. They're typically older, and they've demonstrated a willingness to send money to a stranger in a distant place in response to vague representations regarding a sweepstakes or a prize—that is the ideal profile, for a fraudulent telemarketer to pursue.

List-building mailings often ask for information just to enhance the value of the list in the wrong hands—information such as telephone numbers and credit card numbers.

And—I see my time is out, so I’ll conclude my remarks. We’ve continued to focus our attention, as much as possible, as has the FTC, on these facilitating structures, and we’ll take any questions. Thank you.

[The prepared statement of Mr. St. Clair follows:]

PREPARED STATEMENT OF STEVE ST. CLAIR, ASSISTANT ATTORNEY GENERAL,  
STATE OF IOWA

Fraudulent telemarketers have been stealing from Americans, particularly elderly Americans, for many years. That much is constant. But techniques and operational details have changed over time. It’s been an arms race with the authorities. Law enforcement develops techniques for catching the scammers, and they in turn develop new ways to work the scams and avoid being caught.

About 15 years ago the Iowa Attorney General’s Office developed an effective method for capturing fraudulent phone pitches on tape and criminally prosecuting the telemarketers, who were typically calling Iowans from another state. But since then, the predatory telemarketers have moved their operations across international boundaries—to Canada, Costa Rica, and elsewhere—which makes investigation and prosecution by state authorities extremely challenging.

So increasingly we’ve focused our attention on the stable, U.S.-based operations that facilitate the telemarketing scams. The thinking is that by making the facilitators answer for the frauds to which they provide support, they’ll withdraw that support from dubious operators and make it more difficult for the perpetrators to claim victims.

So attention has been directed to banks and payment processing operations that provide the means for scammers to extract money from the bank accounts of victims. And attention has also been directed to the list builders, list brokers, and list managers that help scammers identify elderly Americans who would be especially susceptible to being cheated by a stranger over the phone.

List builders are operations that actually create lists of people vulnerable to being scammed. They may do prospecting mailings to tens or hundreds of thousands of individuals, promoting vague and misleading opportunities to win prizes or cash in on a sweepstakes. These prize-oriented mailings ask the consumer to send back a small check, say \$20, as an “administrative fee” or the like.

People who send a check in response to such mailings are prime candidates for further victimization. They are typically *older*, and have demonstrated a *willingness to send money to a stranger in a distant place* in response to vague claims *regarding a sweepstakes or a prize*.

These list building mailings often ask for information that will make it easier for fraudulent telemarketers later. They may ask for the consumer’s telephone number, and credit card information. And, of course, they also obtain access to the consumer’s bank account, because the routing numbers appear at the bottom of the small check the consumer is asked to send in.

These lists of responsive, sweepstakes-oriented elderly may then be rented out through the efforts of list brokers and list managers. These list brokers and managers may be stable, well-established businesses that deal in a wide variety of customer and prospect lists. Too often such dealers in lists may exhibit little or no interest in how the lists were made—that is, whether the people on the list are fraud victims—and how someone obtaining the list plans to use it.

In summary, law enforcement attention on the facilitators is continuing, on the part of the FTC, enforcing the Telemarketing Sales Rule (TSR), and on the part of states, enforcing the TSR as well as state law counterparts to the FTC Act. We believe that these efforts are making it harder for scammers to claim victims, elderly and otherwise, by making needed support structures less available.

**Possible Legislative Approaches**

*Broadly address the standard for imposing liability on facilitators*

Under the Telemarketing Sales Rule, a person who is providing “substantial assistance or support” to a telemarketer can be held responsible when that person “knows or consciously avoids knowing” that the telemarketer is violating the law. That involves establishing the mental state of the facilitator, which is very chal-

lenging. A better approach would be to hold a facilitator responsible if he or she “knows or should know” that the telemarketer is violating the law. This is more in the nature of an objective standard—what a reasonable person should be expected to conclude from the surrounding circumstances—and would be a helpful change.

*Address payment systems and banking abuses*

Eliminate “demand drafts,” a.k.a. “remotely created checks,” which are used by many telemarketing scammers to reach directly into the bank accounts of their elderly victims—victims who may not know what happened or know what to do about it.

Lift the preemption constraints that hinder state attorneys general from enforcing laws against national banks. Some national banks have neglected any semblance of a gate-keeping function by making their banking services available to fraudulent operators. Banks in that position should not be shielded from having to answer to state law enforcement authorities, as well as to Federal banking authorities.

*Addressing the creation and exchange of victim lists*

The broadest approach, and perhaps the least realistic in terms of legislative feasibility, would be to require solicitors that intend to market their lists to expressly inform consumers, before the transaction is consummated, that by responding the consumer’s name and other information will be made available to other phone and mail solicitors. Consumers for whom that was an important consideration could simply choose not to enter into the transaction, and could thus stay off the list.

A narrower and presumably more realistic approach would be to create additional safeguards that apply to lists of the elderly. List brokers and list managers could be required to make it their business whether a given list contains a disproportionate number of older consumers, and, if it does, they should have to determine how the list was compiled and how it will be used. This would require list dealers to perform a limited but meaningful gate-keeping function, rather than turning a blind eye, or worse.

Yet another approach worthy of consideration is the creation of a “Do Not Mail” database, a counterpart to the “Do Not Call” registry that has been so popular with consumers. Differences in the two contexts—receiving mail and receiving phone calls—may require significant differences in scope and implementation. However, consumers would likely be grateful for a means of controlling the flow of unsolicited mail, and it could serve to impede exploitive efforts to identify and prey upon vulnerable consumers.

Senator PRYOR. Thank you.

Mr. JOHNSON, let me start with you if I may. In general terms on the Do Not Call Registry—has it made things better for your members?

Mr. JOHNSON. I think it’s a great improvement, and I think the Do Not Call Registry has been a great success.

Senator PRYOR. Well, thank you for saying that. And does your organization have an emphasis on educating your members about the availability of the Registry and the fact that they will have to re-register?

Mr. JOHNSON. We’ve made a great emphasis on the Do Not Call Registry. We have not started to tell people about the need to re-register, I think that’s something that needs to be done.

Senator PRYOR. You know, you probably heard me talk to the witness from the Federal Trade Commission a few moments ago. In hearing her answers to this, did you have any concerns about the FTC’s initiative to educate consumers?

Mr. JOHNSON. I’m not sure that I recall what she said, but the need for education is something that we’re really, always in favor of.

Senator PRYOR. OK, and do you think we should strengthen the current law that we have on the books?

Mr. JOHNSON. I think it needs to be strengthened to the extent that the ability to have fraud perpetrated can be limited, or removed.

Senator PRYOR. OK, let me ask this—I think in your opening statement, you mentioned the established business relationship exception, and you expressed some concerns here. Could you run through that again for the Committee?

Mr. JOHNSON. What we have found is the business relationship has to be strengthened, and better identified. Because if someone merely responds, or asks for information about a product, that puts them in, in effect, as being in a business relationship. And so, the relationship has to be something that's ongoing, rather than just a mere close call.

Senator PRYOR. Mr. Cerasale—am I pronouncing your name right?

Mr. CERASALE. You are correct.

Senator PRYOR. Thank you.

I believe in your testimony, I want to make sure I heard this correctly, but I believe in your testimony you said that the Do Not Call program had been very, very successful with—?

Mr. CERASALE. Yes, it has been very successful. The FTC has said it's been overwhelmingly successful.

Senator PRYOR. OK, could you explain the impact the Do Not Call Registry has had on your industry?

Mr. CERASALE. There has been, clearly, closure of some call centers. So that has changed, changed the industry that way. Looking for a prospect, trying to find somebody with an offer, is generally not, cannot be done as well through the telephone. But all of our members have gone—have gone before, and are continuing to go forward—with being multi-channel, including potentially, opening retail stores, but reaching out through the Internet, reaching out through the telephone, reaching out through the mail, and coordination with—like that.

For example, you could get a telephone call with—when a mail piece is supposed to be received. So, there's a greater emphasis on being multi-channel, with less emphasis on outgoing telephone calls. This is a significant increase, however, in telephone calls coming back to companies. And going to consumer representations, and so forth, increase on the companies.

So that has really, I would say, exploded during this time. But outgoing telemarketing has had a significant, if not, dramatic turn.

Senator PRYOR. Let me ask this—on the fee structure of the Federal Do Not Call Registry—tell me how that has impacted the industry, and how you all deal with that, and how it should be structured in your view. I think you've touched on this in your opening statement, but if you could elaborate a little bit.

Mr. CERASALE. Sure. The fees have gone up, significantly. And we don't have any complaints about how the fee structure is applied. In other words, if I am a marketer, I have to obtain the registry. If I'm doing it nationwide, I get a national list. Also, if I'm a supplier, someone who does calling for another company—I have to obtain the list, as well as ensure that my client has, also has permission to use the list. We have no trouble, problem with that.

What's happened is, that we believe that, the cost of the contract with AT&T to run the Do Not Call Registry, I think, is \$3.5 million. The fees that are coming into the Federal Trade Commission amount to approximately \$18 million. So, we think that that's too much. Our view is that we should use the fees to cover the cost of the Government running the list, and that, that's where it should be. But, in any event, going up 263 percent, since 2000—October 2003, is a little bit too high an increase. So, therefore we support your efforts to put a—to set the fee, statutorily—so the FTC doesn't have to go forward, every year, with rulemaking, and to them put—we agree—cost go—sadly, costs go up not down, to put an CPI index to it.

Senator PRYOR. Thank you.  
Senator Klobuchar?

**STATEMENT OF HON. AMY KLOBUCHAR,  
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. Thank you very much, Senator Pryor. Thank you for the work, chairing this Committee, and for your work in guiding us as we go forward with these important issues. I must say, that I was involved in these issues as a prosecutor and, in fact, worked with AARP on a State level. We did a series of forums for seniors around the State on identity theft and fraud that were very successful.

I most remember, Mr. Johnson, one of your most diligent members in Rochester, Minnesota, in front of 400 seniors, suggesting to them that it's not just enough to shred documents, that he took his dog out for a walk, and then placed the dog droppings on top of the shreddings in the garbage can—

[Laughter.]

Senator KLOBUCHAR.—so potential thieves would not break in. I then said, at that moment, “You're not suggesting, sir, that everyone in this room,” as they diligently took notes, “do that?” It's an example of how people make their own decisions in their own lives? And he said, “Well, unfortunately, Senator, my dog is no longer with us, but I now use maple syrup.”

[Laughter.]

Senator KLOBUCHAR. That memory is strong in my mind, as we have these discussions in terms of making sure that we make things available, Mr. Cerasale, and at the same time, that we protect people. I'm a big fan of the Do Not Call List, and I appreciate the work that's been done in the Senate before my time, and I believe that we need to do everything we can to keep that in place, and make it stronger than ever.

And I guess, I'm first interested, Mr. Johnson, in any ideas that you would have about involving more seniors in this, in the Do Not Call List. I know that we encountered some issues of people not knowing how to get on the registry, and that was a lower—correct me if I'm wrong—a lower percentage of some of them registering on the Do Not Call list than other demographic age groups?

Mr. JOHNSON. The thing that we've established is the original emphasis on the Do Not Call Registry, and the Do Not Call listing. We now have State offices, in every one of the States in the United States, and the Virgin Islands, and so we have an ability to get a

better emphasis through to our members, and we will do this again through the members' gatherings and forums, and utilization of our State offices.

Senator KLOBUCHAR. OK, thank you.

And, Mr. St. Clair, in your prepared remarks, you talked about how some of the telemarketing issues that are plaguing seniors and others have, in fact, become a global enterprise. And, I certainly encountered that, where we would have people—either by e-mail or by phone—calling from all over the world, and it was very hard, as a local prosecutor, to go after those cases.

Could you talk a little bit about your experiences, and what law enforcement tools are available for you to investigate these offshore criminals, and how you think it best be done?

Mr. ST. CLAIR. Well, it is extremely difficult for local, State law enforcement authorities to deal with international boundaries. And we have certainly cooperated, passed information to Federal authorities, who may be better situated, and we've worked closely, as far as passing information to the Canadian authorities. And, I think, when the telemarketing fraud was just getting started in Canada, for example, it was a little slow—the authorities there, I dare say, were a little slow—in recognizing the scope of the problem, and for the most part, victims were not being claimed within Canada.

But after, perhaps, this slow start, we've seen great work by Canadian authorities, and what—part of what we've had to do, given the limitations for an Attorney General's office in a state like Iowa, dealing with international boundaries, is again to turn our attention to the U.S.-based facilitators to try to make a difference there.

Senator KLOBUCHAR. Thank you.

I know one of the things we would always recommend for victims of identity theft is that they check with the credit bureaus. So, I am concerned about what I hear about them being overburdened and not being able to get at some of the major issues here because I always thought of identity theft as the crime that keeps on giving. Once your identity's stolen, because you've given the Social Security number out to someone, it takes you, sometimes years, to get it back, and to correct your credit rating.

And so I was listening to Ms. Faulkner, and my question for you, Ms. Holland, is about what this difference is, between the free credit reports that you're required to provide and the company's paid monitoring service?

Ms. HOLLAND. The free credit report, which is available through *annualcreditreport.com*, is simply a copy of their report that outlines all of the items in their credit report.

A credit monitoring service, or credit monitoring product, is a bit different. The credit monitoring product sends them alerts as soon as there's a change in their credit report.

So, for example, you obtain your credit report, the free report from *annualcreditreport.com*, and that's just a one-time snapshot based upon the time you picked it up. When you subscribe to a monitoring service, you're going to be alerted every single time that there is a change to your credit report, and that has proven to be beneficial to detect and guard against identity theft.

So, what would happen is, if there's a change in my file, I would be alerted—depending upon the service or the product that I purchased. And it would say that there has been a change in my report, and then I would be able to investigate what that change is. So, there is a clear distinction between just getting a free report, at that one period in time, versus having a monitoring service that's going to look at that report, and notify you every time there's a change.

Senator KLOBUCHAR. And again, my interest is making sure that consumers have easy access to these credit reports since we kept telling them you can just easily use one of these credit agencies. If I were to access your website right now, would it be easy for me to see where I could access my credit report for free without a fee? Or would I be directed directly to your company's fee-based credit monitoring?

Ms. HOLLAND. You would be—it would, it would—up front, you would know that you could get a free report, because it states it there, and we actually link you to the free credit report site, at *annualcreditreport.com*. So you are keenly aware that you can get the free report. And in our educational portion of our website, we talk a lot about being able to obtain that free credit report.

Senator KLOBUCHAR. Ms. Faulkner, do you want to add anything to this?

Ms. FAULKNER. I disagree that the credit monitoring service is useful to consumers. And, basically it's because credit reports change almost every day, as creditors report. So, I had one client with, actually, Equifax's credit monitoring service, and she was a nervous wreck, because every third day, she would get a notice that something had changed on her credit report. And she was making me a nervous wreck, because I had to tell her, "Well, this is just a creditor updating something, nobody is stealing your credit, there's no more adverse information than there was before in it.

So, I think that the consumers are, perhaps, overwhelmed by the credit monitoring services, and I think checking once or twice a year is sufficient. Particularly when, in Connecticut, you can get a copy of your credit report for \$7.00. Whereas, if you're paying nine or ten dollars a month for your credit monitoring service, that's costing a lot more.

Senator KLOBUCHAR. Ms. Holland?

Ms. HOLLAND. Yes, I'd just like to state, in my role at Equifax, I talk to consumers every single day. That's my job, and I'm very passionate about making sure consumers are aware of what they can do to protect themselves. And I would simply say to you that I—we see, we get numerous accolades about consumers thanking us for being vigilant, alerting them when they subscribe to those services. They're very thankful that they were alerted, because they realize by being notified early that there has been a change. And remember—they can look at that change. If that change is simply an update to their balance, there's no problem there, and they close—they log off, and they go on about their business. So, I don't know that I—I don't agree with Ms. Faulkner's characterization, because we have consumers—and I talk to them—and they say that the credit monitoring product has been very, very helpful to them.

Senator KLOBUCHAR. All right. Thank you very much. Does anyone want to add anything to that discussion?

[No response.]

Senator KLOBUCHAR. All right, well thank you. We look forward to working with you as we go ahead with both of these areas, in terms of perfecting the legislation, and making it easier for consumers to access their information.

Senator PRYOR. Thank you, Senator Klobuchar.

Let me go ahead and ask you a few more questions, if I may.

Mr. Cerasale, are there any changes out there in the marketplace, or changes occurring in your industry that we need to know about as we're crafting a new Do Not Call law? In other words, we talked a little bit about Voice-over-Internet Protocol phones, we talked a little bit about cellular phones. Are there changes in the industry or changes in the marketplace that we need to take into consideration?

Mr. CERASALE. Well, I think that the first one, of course, is that one-eighth of the American public does not have a landline that they—their only form of telephone is a cell phone. The FCC—the Federal Communications Commission, under the Telephone Consumer Protection Act—it is, you cannot use those predictive dialers to make any solicitation call to them, unless you have express permission. So that, I think, if you look at the Do Not Call Registry, and the idea of having cell numbers on it, that's a repeat. That's a cost to the Government, and eventually a cost to the marketer that's already covered through another—even greater than the Do Not Call Registry, through the Telephone Consumer Protection Act. Because, even if you have an established business relationship, you cannot call someone on a cell phone, unless you get their permission.

Looking at—I think the idea of being able to contact your customers is an important one to preserve. And, so the established business relationship has worked, and works well. And there is a difference between someone who has purchased something, or someone who has made an inquiry. Even under the current law, an inquiry—you have 3 months to try and contact someone, and then that business relationship expires, whereas you have 18 months from the time that you completed the transaction, if you have a subscription to *Sports Illustrated*, for example, when the subscription ended is when the 18 months clock starts. That is a difference between a customer, and someone who has made an inquiry, and that has worked. I mean, overwhelmingly, the Federal Trade Commission thinks that this is a product that has worked well.

Senator PRYOR. Thank you.

Let me move, if I may, very quickly. I want to acknowledge Senator Thune here, in just one moment, but let me move, if I can, to Mr. St. Clair. First I want you to please tell your boss I said hello. I served with him as Attorney General, and he's great. Tell him I said hello.

But second, let me ask about something you said in your opening statement about list builders. Can you explain to the Committee what they do, who they are, how the lists are built, and how they're used?

Mr. ST. CLAIR. Well, perhaps—perhaps one of the better ways to do that would be an example. In Iowa, we discovered that a local commercial mail drop was receiving about, ultimately, it was about 20,000 pieces of mail, all addressed to different—some nine different businesses. And we ultimately seized the mail, and upon examining it, we determined that it was coming all from a place in South Carolina, and what they were doing, basically, is mass-mailing to a very extensive list, mailers that were on their, on their face—in our view—on their face, deceptive, and they were focused on winning prizes, winning sweepstakes, and so forth. And, they asked the person to send a small check, as small as, say, sometimes, \$10, or \$20. And, what this permitted the recipient, in South Carolina—of course all of the mail was ultimately just to be forwarded to South Carolina—what this would have permitted the recipient of all of the mail to do, is—in addition to receiving the modest checks, which was undoubtedly welcome, and helped pay for the mailing—is to create a very hot list of highly vulnerable people. The people we checked with that were responding to these mailings were predominantly elderly. And again, they were self-selecting for their vulnerability, in effect, as willing to send off money at a distance, to a stranger in response to vague representations about winning prizes.

And, we ultimately determined, in that case, that some of the same mailings were later followed by telemarketing calls that referred back to the mailings. And, so some of the same people who had responded, you know, sent off only \$10 or \$20, you know, not a great loss, had, in effect, put themselves on the list, and then that list was made available to predatory telemarketers, who were after thousands of dollars.

So, that's what we mean by list builders, and there are a lot of enterprises out there, right now, that appear to be engaged in those sorts of activities.

Senator PRYOR. Senator Thune?

**STATEMENT OF HON. JOHN THUNE,  
U.S. SENATOR FROM SOUTH DAKOTA**

Senator THUNE. Thank you, Mr. Chairman. And I want to thank the witnesses for being here today, and sharing your insights.

We've got 146 million telephone numbers that were registered with the Do Not Call list which has been, I think, by and large a win for consumers. Families now can choose to rid themselves of many of those calls that all seem to come during dinnertime, but there are, of course, still millions of Americans who are not listed, and still receive telemarketing calls for one reason or another, and as some have already pointed out—often lonely, elderly Americans enjoy receiving telemarketing phone calls during the day. It's important, Mr. Chairman, that this Committee continue in its oversight duties to ensure that telemarketing regulations and policies we have in place are effective.

I just have a couple of, I guess, quick questions, if I might, for Mr. Cerasale, is that—did I say that correctly?

Mr. CERASALE. You said it correctly, Senator.

Senator THUNE. All right. It's my understanding that list brokers—those companies who collect and sell lists of names and

phone numbers, that are members of the Direct Marketing Association are required by DMA to screen list buyers for suspicious activity. And, I guess I'm just—maybe if you could explain to us what that entails, and if you think there is more that could be done to stop bad actors from getting these lists to begin with?

Mr. CERASALE. The—the members of DMA—the list builders that Mr. St. Clair talked about, that's illegal from the start. I mean, these are people getting names, and with that mailing, and asking for a check on a sweepstakes, which is illegal under postal regs, and I'm sure illegal under most State regulations, making it a lottery, as opposed to a sweepstakes—anyway. So, that's illegal activity. So, I want to just make a change, a switch from that, from a list broker, someone who obtains information from public records, from purchased records, and compiles those lists. Or even the list of—I subscribe to one magazine, and therefore I exchange or share my list with another magazine. Or, for example, a maker of a golf ball, who's trying to get the list of subscribers to *Golf Magazine* to try and send out an offer.

If our—we've clarified our guidelines in the testimony. If you're a list compiler—someone who gathers the list together, you have sensitive information—that would be financial information, also defined as seniors. You have to screen the—as a compiler—screen the promotion that the list is going to be used for, for appropriateness.

For example, let's use the example that Mr. St. Clair raised. If you get the script of the telemarketing, or the piece that was sent through the mail that says, "Here's a chance to win some money, and please send us a \$10 check." Well, you don't do that, that's illegal. So, that kind of obligation is now upon those list compilers, to know with whom they are dealing. And, I think that's the important part in making—it's a stronger guideline, is to ensure that our members know with whom they're dealing. In other words, know the reputation of those with whom you're dealing. And, if it's sensitive information, absolutely ensure that you've seen the script. You see the piece of mail, you see the e-mail.

Senator THUNE. Mr. Johnson?

Mr. JOHNSON. The only information I have about list builders is the article in *The New York Times* which referred to infoUSA. And some of the things that they've cited were that these lists are comprised of names that they've obtained—as Mr. Cerasale has said—by various means, magazine subscriptions, or whatever. But they've compiled these, and put them into categories, which are particularly aimed at seniors. And, not only seniors, but groups. There's a listing that is headed as "oldies but goodies." And these are folks that they found were gamblers, and that they would send them out, to people with the recommendation that "these folks are gullible."

Now, I think that it's something that must be done to say that these list compilers, who put this kind of a caveat, it's almost targeting the seniors, who have already been found that 50 percent of the folks that are subject to this kind of fraud, are over 50 years of age.

Senator THUNE. Just as a followup, if I might, Mr. Johnson, we've got a high percentage of elderly citizens in South Dakota, many of whom live in rural parts of the state, and may enjoy re-

ceiving calls from telemarketers, and therefore not want to put their name or their number on a Do Not Call list. Do you have any suggestions for what we can do to help protect these elderly Americans who want to continue receiving telemarketing calls?

Mr. JOHNSON. I think the only thing we can do is try to educate them that this is not a friendly call. We've had reverse border rooms, when we've tried to put these things in evidence, and that gives a "chump list" that we receive from the Attorney General's office. And we call those folks to alert them that they're on a list of folks that have been designated to receive telemarketing calls—and principally, telemarketing fraudulent calls.

So, the only thing I can suggest, is what we used to do. We would make a lot of effort to tell the folks that, just hang up when you get this. It's not a person on the other end that's trying to be your friend, it's someone that's trying to take your livelihood.

Mr. CERASALE. Enforcement. Most of this stuff is illegal. As a senior, many times you are more of a shut-in, can't get out as much, so that there, these are means to keep you in touch with commerce, in part too. So, it's not all—I think the impression here might be that every call to a senior, every piece of mail that comes to a senior is fraudulent—there are many, many legitimate marketers out there, and this is the, the touch for many seniors to reach commerce in the United States.

The key is to go after enforcement. The fraud—it's illegal already. And we need more enforcement—both on the State level, the local level, the Federal level, to go after and protect. I think the laws are there, and the choices are there, I mean, even on the Do Not Call Registry, as seniors go further and further—I mean, I'm one of them. As they say, as you go further and further down the way, maybe my children can come in and take over, too. And there are means for that, there's—to try and keep my dignity, but also allow children guardians to try and come in and protect, if that's necessary.

And, so I think the key is, is laws—not the laws, but the enforcement of current laws. And, we're—we encourage that.

Senator THUNE. Is that primarily a State function, law enforcement—we've got a former Attorney General here?

Senator PRYOR. I think to a large extent it is. We have an Assistant Attorney General here who might want to take a stab at that. But I think States generally will enforce those types of laws.

Mr. ST. CLAIR. Yes, I believe—well, as I think was mentioned, postal authorities have a lottery prohibition, but I think each State has some version of a lottery prohibition. Sometimes the sort of mail building efforts, or list building efforts we were talking about are not clear lottery cases. It's not a matter, always, of just sending \$10 in order to be buying the equivalent of a ticket in a lottery. If it were, that would be a fairly straightforward lottery violation.

But, sometimes what they are selling are, for example, sweepstakes reports. So that, that permits the mailer to talk heavily about sweepstakes, and prizes, and large amounts of money, in a confusing fashion, and then ask for an administrative, or a transfer fee. But the fee, in fact, is just—they would say, the mailer would say—is just a payment, a straight-up payment for a sweepstakes

report, that they then send out, and the sweepstakes report just identifies different publicly accessible sweepstakes.

And so, so it wouldn't be so easy to just simply go after them as a lottery. But, it still has the intended list building function, and some of the deceptive aspects are fairly subtle.

But yes, it's often a State function.

Senator THUNE. Thank you, Mr. Chairman.

Thank you all very much.

Senator PRYOR. Thank you.

And to follow up on that, the Arkansas law is called the Deceptive Trade Practices Act, which is just a big umbrella law that we use. We had other, more specific, acts, but it seems like you could always plug something into the Deceptive Trade Practices Act.

Let me ask, if I may, Ms. Holland, about CROA. I understand that you and Ms. Faulkner disagree, or your organizations disagree on some of this.

But, for clarification, Ms. Holland from your standpoint, how does credit monitoring safeguard against identify theft, or mitigate the impact of identity theft?

Ms. HOLLAND. Well, credit monitoring products provide consumers with a proactive first line of defense against identity theft. And so, depending on the product, notices and alerts can be sent directly to that consumer, whenever changes are made to the consumer's credit report. So, this early detection of a problem through credit monitoring can save a consumer the time and expense that otherwise is spent trying to correct fraudulent activity after the fact, or fraudulent credit reporting information. So, what it does is that, instead of you checking your credit report annually, at Equifax, we recommend you check your credit report three or four time a year. But at the end of the day, fraudsters are always looking to commit fraud. So, a consumer who has a monitoring service that's going to alert them every time that change comes, they're going to be more aware of a change versus someone who gets a report three or four times a year.

And so, we believe that's the biggest distinction, in that you are notified every time there's a change to the report, a relevant change.

Senator PRYOR. Right, again, for clarification, we've talked about repair services and monitoring products, which are two distinct products, or two distinct services, I guess you might say,—

Ms. HOLLAND. Correct.

Senator PRYOR.—that can be offered to consumers. Do you think that these should be treated differently under the law? Or should they both be under CROA?

Ms. HOLLAND. Well, I think if you behave like a credit repair organization, then you should be subject to CROA. The heart of a credit repair scam, Chairman Pryor, is to remove accurate and timely—but adverse—credit information from a credit report. Well, that not only harms the individual integrity of the credit report, but it has the potential to undermine the entire credit reporting system.

So, if you're going out as a credit repair organization, making promises about how you're going to have accurate information removed, then you should be subject to CROA. A credit monitoring

service is a benefit to a consumer, as it helps them not only have a defense against identity theft, but it also gives them the tools and gives them the ability to manage their credit report themselves, and helps them learn and change behaviors about improving their credit score through personal management of their financial health. And that's the key about empowering, enlightening, and enabling consumers, to take control of their credit. A credit repair organization simply behaves and tells consumers untruths about being able to remove information, and they should obviously be subject to the harsh penalties of CROA.

Senator PRYOR. Let me ask you another question, Ms. Holland. It's my understanding that the credit bureaus, the consumer groups and the Federal Trade Commission have been working together for some time to address this issue. And, it seems that, as much as you've tried, recent efforts have not been able to create a legislative product that everybody is happy with. Is that a fair assessment?

Ms. HOLLAND. I believe that is a fair assessment, Chairman.

Senator PRYOR. And does your organization have language that you would like to see in legislation? Have you all—has your organization gotten that far?

Ms. HOLLAND. Well, I think we've worked very closely—and I think that's an important question, and rather than speculate, I'd like to get back to you and give you that in writing.

Senator PRYOR. Great, I appreciate that.

Ms. Faulkner, I know that, again, you disagree with some of the answers you just heard just a moment ago, but have either you personally, or your organization, been part of these discussions to try to find language that we can put in a bill that will satisfy all of the parties? Have you been part of that?

Ms. FAULKNER. I have. And we have been literally wracking our brains, and we have not been able to come up with something that would exempt just credit monitoring, without making a loophole for credit repair.

I can tell you there has been case law recently, in particular, the *Hillis* case, where one of the Federal judges made a really good distinction between credit improvement—credit monitoring, and credit repair organizations, just based on the language of the statute. So, it may be that no amendment is needed for the distinction to be made between credit monitoring and credit repair. But, we would just hate to see anything done that gives the credit clinics one more way to scam consumers.

Senator PRYOR. OK.

Ms. Faulkner, let me ask you another last question, and that is something that you mentioned in your opening statement, but you didn't really dwell on it, and it's not the subject of this hearing, but you mentioned arbitration clauses—

Ms. FAULKNER. I did.

Senator PRYOR. and distant forum clauses. Is it your experience that you see arbitration clauses, and distant forum clauses in—what did you say—in credit monitoring?

Ms. FAULKNER. In the credit clinics.

Senator PRYOR. OK.

Ms. FAULKNER. In the credit clinics, yes.

Senator PRYOR. And from your standpoint, how do those disadvantage consumers?

Ms. FAULKNER. With arbitration clauses, it means the consumer cannot go to court to get his or her rights, and to enforce his rights under the CROA. It means they have to go to a private arbitration organization. It means that the hearing is secret. It means that the wrongdoing never gets publicized. So, the wrongdoing is swept under the rug in a private manner.

And, the distant forum clauses are just to make it more expensive for the consumer to do anything at all. If you have to go from Connecticut to California, in other words, even for arbitration, it's cost-prohibitive. So, essentially what these two clauses do is evade liability completely, because no consumer can afford either arbitration, or going to a distance forum. We would like to see a local, Federal—right to go to your local Federal court.

Senator PRYOR. All right, now, I know this is a little bit beyond the scope of the hearing, but while we're on that subject, are you seeing these type of clauses in other consumer contracts?

Ms. FAULKNER. Yes. Yes, they are spreading like the plague.

Senator PRYOR. Then, from your standpoint, they're increasing out there in the—

Ms. FAULKNER. Yes, definitely.

Senator PRYOR. With that, hold on, let me ask the staff if I missed anything. Are we square?

What we'll do is, we'll keep the record open for 14 days, for 2 weeks. And I just want to thank everybody for being here. Your testimony was appreciated and very helpful.

And with that, like I said, we'll leave the record open for Senators, if they choose, to submit questions in writing, and the Commerce Committee staff will forward them to you. And, if you all have opening statements, et cetera, that you want to submit for the record, we'll take care of that, just let us know.

But again, thank you all for being here, and thank you for being involved in the process.

The hearing is adjourned.

[Whereupon, at 4 p.m., the hearing was adjourned.]



# A P P E N D I X

SUPPLEMENTAL STATEMENT OF ROBIN HOLLAND, SENIOR VICE PRESIDENT,  
GLOBAL OPERATIONS, EQUIFAX INC.

## Introduction

I want to thank you for this opportunity to respond to a question raised by Chairman Pryor during the recent hearing on the Credit Repair Organizations Act (CROA) reform. Specifically, this Supplemental Statement will address the type of CROA reform necessary to combat credit repair organizations, while protecting legitimate credit monitoring products and services.

Subsequent to the enactment of CROA, credit monitoring has been developed to give consumers a first line of defense against identity theft and to increase consumer literacy regarding credit matters. The credit bureaus seek statutory reforms that conclusively establish that credit monitoring and similar credit information products and services are not subject to CROA. As indicated by Joanne Faulkner's testimony at the hearing, consumer groups fear that such reforms would open the door for credit repair organizations (CROs) to evade the requirements of CROA. For the reasons set forth below, Equifax believes that such fears are unfounded.

## Defining Credit Repair

CROs are defined as entities that use any instrumentality of interstate commerce to sell, provide, or perform (or represent that they can perform) services or advice for the express or implied purpose of improving a consumer's credit record, credit history, or credit rating in return for a fee.<sup>1</sup> As noted by Ms. Faulkner in her written statement, CROs intentionally and systematically deceive not only consumers, but the credit bureaus. In contrast, credit monitoring and similar credit information products and services were developed to help improve consumer understanding about their credit history.

CROA was originally enacted to stop CROs from harming consumers and the credit reporting system through credit repair activities. Looking to the legislative history,<sup>2</sup> Congress did not seek to place limitations on all products and services that pertain to credit, but instead sought to target narrowly those specific harmful activities performed by CROs. Congress did not intend for the definition of a CRO to sweep in products that offer only prospective credit advice to consumers or provide information to consumers so that the consumers can take steps on their own to improve their credit in the future. Credit monitoring and similar credit information products and services should not be swept into the definition of CRO, because such products provide information that empowers rather than harms consumers.

CROA is enforced by the Federal Trade Commission (FTC). The FTC staff has stated that there is no basis to subject the sale of credit monitoring and similar educational products to CROA's specific prohibitions and requirements, which were intended to rein in fraudulent credit repair. The FTC staff has even commended credit monitoring products—if promoted and sold in a truthful manner—as a way to help consumers maintain an accurate credit file and provide them with valuable information for combating identity theft.

## A Behavior-based Solution

CROA can be amended to prevent the type of abusive practices that Congress originally intended to address by taking a behavior-based approach to the application of CROA's requirements. By applying CROA to only those entities engaged in the potentially fraudulent activities known as credit repair, CROA can be reformed in a way that continues to protect consumers from those activities and permits the

<sup>1</sup>Sec. 403(3) of the Credit Repair Organizations Act, Public Law 90-321, 82 Stat. 164, 15 U.S.C. S. § 1679a (2006).

<sup>2</sup>See H.R. Rep. No. 103-486, at 57 (Apr. 28, 1994), and see also *Hearing on the Credit Repair Organizations Act (H.R. 458) Before the Subcommittee on Consumer Affairs and Coinage of the House Committee on Banking, Finance, and Urban Affairs*, 100th Congress (Sept. 15, 1988).

provision of legitimate credit monitoring products and similar credit information products and services outside of the technical provisions of CROA. The nature of the activity performed by the entity would trigger application of CROA, rather than the characterization those entities assign to their products and services. An example of this approach can be seen in a House bill (H.R. 2885), introduced by Rep. Paul Kanjorski, which sets out in detail the type of credit monitoring activities that would not be covered by CROA.

Through this behavior-based approach, CROA would be able to reach credit repair services regardless of whether the entity claims to be a CRO or a provider of credit monitoring. Improperly characterizing either the product being sold or the entity making the offer will not achieve the purpose of evading CROA. Credit repair organizations that purport to offer legitimate services, but actually engage in credit repair operations will still be subject to CROA. Conversely, if an entity offers legitimate and beneficial products, such as credit monitoring, then the activity-based approach to CROA enforcement would permit such activities to continue without being subject to CROA. Through such reforms, no entity could escape the consumer protection requirements of CROA, but consumers would benefit from the increased availability of other legitimate products, such as credit monitoring.

To the benefit of consumers, the FTC has developed extensive expertise in investigating entities engaged in unfair or deceptive trade practices through Section 5 of the FTC Act. *See* 15 U.S.C. § 45(a). The FTC specializes in distinguishing between what companies say they do and what those companies actually do. Given a clearly established definition of credit repair activity, with specific exceptions in place for credit information products and services such as credit monitoring products, and the FTC's expertise with respect to deceptive practices, the FTC should easily be able to recognize any attempt to mischaracterize an illegal credit repair service as a legitimate credit monitoring product. To the extent a credit repair organization falsely purported to offer CROA-exempt products or services to evade CROA coverage, they could be in violation of both CROA and Section 5 of the FTC Act.

#### **The *Hillis* Case**

Ms. Faulkner suggested during the hearing that reforms to CROA are unnecessary because a judge in a recent case, *Hillis v. Equifax Consumer Services, Inc.*, 237 F.R.D. 491 (N.D. Ga. 2006), was able to distinguish between credit repair and credit monitoring under existing law. The judge in the *Hillis* case rejected a broad interpretation of the definition of CRO, and concluded that "Congress could not have intended these terms to encompass all credit-related advice." *Hillis*, p. 512.

However, Ms. Faulkner's argument that taking no legislation action is the proper solution in light of this decision misses the mark. The court in *Hillis* recognized that if providers of credit monitoring are considered CROs, it will be highly impractical for those entities to comply with the technical provisions of the CROA and still provide the type of credit information being sought by consumers. Not every court is the same, and not all judges will necessarily have the wisdom of the *Hillis* judge. Without reforming CROA to definitively establish that credit monitoring and similar credit information products and services are not credit repair activities, similar litigation could result in significant harm to companies that offer credit monitoring.

The total cost of the *Hillis* settlement will be well over \$4 million. Equifax and Fair Isaac will pay up to \$4 million in attorney's fees and costs to the *Hillis* class counsel, and the two named plaintiffs will each receive up to \$7,500. Additionally, the more than 6 million putative members of the *Hillis* class are eligible to receive either three or six free months of Score Watch™ (depending on whether they purchased an eligible product from only one or both of Equifax and Fair Isaac), a product which provides monitoring of the consumer's FICO® Credit Score and two free Score Power® reports. The retail value to each putative class member of this free product benefit is at least \$24 (for 3 months) or \$48 (for 6 months). Equifax and Fair Isaac also agreed to pay for the costs of printing and mailing postcard notices to class members, a settlement website with the terms of the agreement, a telephone assistance program, as well as other settlement administrative expenses. Without CROA reform, new lawsuits could be brought which would push litigation costs even higher.

Ironically, the *Hillis* court approved the settlement in part because Equifax and Fair Isaac agreed to provide a disclaimer stating that it is not a credit repair organization and that Equifax does not offer credit repair advice to consumers. This has always been the position of Equifax, a position we seek to have established conclusively through reform of the CROA statute.

### Conclusion

CROA should be reformed so that it is clear that entities that offer credit monitoring and similar credit information products and services are not subject to the requirements and restrictions placed on CROs. These products and services benefit consumers in a way that can be easily distinguished from the harmful credit repair activities performed by CROs. By reforming the CROA statute to take a behavior-based look at an entity's activities, credit monitoring and similar credit information products and services can remain available to consumers without throwing open the door for CROs to evade the consumer protections put into place by CROA.

---

#### SUPPLEMENTAL STATEMENT OF JOANNE S. FAULKNER, ATTORNEY, ON BEHALF OF THE NATIONAL ASSOCIATION OF CONSUMER ADVOCATES

Senator Pryor left the record open for 2 weeks. At the end of the hearing, he asked whether I had seen mandatory predispute arbitration clauses and distant forum clauses in credit monitoring services. I now have.

My own bank, Bank of America, offered Bank of America Privacy Assist Premier™ (Trademark of FIA, Inc.). The service includes “automatic alerts when certain changes occur in your credit files from 3 major credit reporting agencies; unlimited online access to your 3 credit reports; ID theft recovery assistance from trained specialists, and identity theft insurance.”

The agreement also includes binding arbitration before the American Arbitration Association in Washington, DC, together with other clauses limiting consumer remedies.

The Equifax website would not reveal the terms of the contract until after I filled out an enrollment form including much personal information (which I would not do). However, a report on the Internet reveals that an Equifax credit monitoring service “agreement also specifies that users are forced into binding arbitration if they have any disputes with the service, rather than pursue litigation, except in small claims court.” [http://www.consumeraffairs.com/news04/2006/05/paypal\\_equifax.html](http://www.consumeraffairs.com/news04/2006/05/paypal_equifax.html).

Contrary to the testimony of Ms. Holland, the website for Equifax Personal Solutions does not mention the free credit report. It may be found by typing Equifax Credit Monitoring into a search engine and selecting Personal Solutions, or at <http://www.equifax.com/cs>

---

#### RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO LYDIA B. PARNES

*Question 1.* Do Not Call telephone number registrations will expire during the summer of 2008 for all consumers who registered their telephone numbers in 2003. At the hearing, you indicated that the Commission will conduct a consumer education campaign to inform consumers of the need to re-register. Can you please provide more details about the Commission's plans for educating consumers about the need to re-register and how to do so?

*Answer.* The FTC will conduct a consumer education campaign beginning in early 2008 to explain the registry and that some numbers will need to be re-registered. The campaign will be modeled on the highly successful, award-winning marketing campaign for the registry in 2003. The FTC will provide focused messages for consumers and the media, as well as products such as web buttons and banners, articles, and short videos that can be disseminated by the agency's communications partners—including industry associations, non-profit groups, government agencies, and congressional offices. There is a high level of interest in the registry among consumers and the media, and the FTC will provide plain-language information for consumers about how to take advantage of the registry.

*Question 2.* The need to re-register could lead to confusion among consumers who do not know when they registered for the Do Not Call list, and, as a result, will not know whether they need to re-register in 2008 or at some later date. How can consumers determine when they need to re-register?

*Answer.* Consumers can access the National Registry at any time to confirm that their telephone numbers are registered and when the registrations will expire by visiting our website at [www.donotcall.gov](http://www.donotcall.gov) or calling our toll-free numbers 888-382-1222 (TTY 866-290-4236). Consumers also can re-register their telephone numbers at any time through the same website or toll-free numbers. They do not need to wait until their registration expires. Telephone numbers remain on the registry for 5 years from the date of the most recent registration. We will include this information in our consumer education campaign planned for early 2008.

*Question 3.* Some credit monitoring companies advertise “free credit reports” to consumers who subscribe to their pay credit monitoring services. Often, these companies’ websites have only a small-print link to information about receiving the free annual credit report to which every consumer is entitled by law. Has the FTC received complaints from consumers who unwittingly subscribed to pay credit monitoring services when all they wanted was to get their free credit report?

Answer. Since the annual free credit report program went into effect in September 2004, the FTC has received a number of complaints from consumers about “imposter” free report websites that mimic the FACT Act-required website, *www.annualcreditreport.com*. These sites typically use URLs that are common misspellings of *annualcreditreport.com* or are sound-alike names. In many cases, the imposter sites offer free reports in conjunction with the purchase of a credit monitoring service. The credit monitoring typically is sold on a “free-to-pay conversion” basis, *i.e.*, the service is free for a short period, but converts to an automatically-renewing paid service unless the consumer affirmatively cancels within the free period. This type of promotion is a variation on the more general category of “continuity” or “negative option” plans, whereby consumers are automatically sent products and billed on a periodic basis until they cancel.

The FTC carefully monitors imposter sites and has sent warning letters to operators of more than 130 such sites explaining that attempts to mislead consumers are illegal.<sup>1</sup> Most of these sites have been taken down. The FTC also takes enforcement action in appropriate cases.

For example, in 2005, the Commission charged *Consumerinfo.com*, a subsidiary of Experian and the operator of the “freecreditreport.com” site, with deceptively marketing “free credit reports.”<sup>2</sup> The Commission alleged that Consumerinfo deceived consumers by not adequately disclosing that consumers who took advantage of the free credit report offer automatically would be signed up for a credit monitoring service and charged \$79.95 if they did not cancel within 30 days. The Commission’s complaint further alleged that Consumerinfo misled consumers by promoting its “free reports” without disclosing that it was not associated with the official annual free credit report program. In settlement of those charges, the FTC required Consumerinfo to pay redress to deceived consumers, barred deceptive and misleading claims about “free” offers, required clear and prominent disclosures of the terms and conditions of any “free” offers, required clear and prominent disclosures that its promotion is not affiliated with the FACT Act free report program, and required the defendant to disgorge \$950,000.

Earlier this year, the FTC charged Consumerinfo with disseminating advertisements after entry of the settlement that violated the disclosure requirements.<sup>3</sup> Consumerinfo was required to pay \$300,000 in additional ill-gotten gains.

The FTC also has engaged in extensive outreach efforts to warn consumers about imposter free credit report promotions. The Commission maintains a micro-site on its website devoted to the free annual credit report program.<sup>4</sup> The micro-site links directly to *annualcreditreport.com* so that consumers can be sure they are not misdirected to an imposter site. The micro-site also links to educational materials for consumers about the free annual report program and how to avoid imposters.<sup>5</sup> Additional materials available through the micro-site advise consumers about avoiding deceptive “trial offers” and other types of continuity promotions.<sup>6</sup> The FTC also has produced radio public service announcements warning about imposter free report sites.<sup>7</sup> In addition, the FTC mails copies of its education materials to consumers who call the FTC’s toll-free complaint hotline.

<sup>1</sup> Press Release, Federal Trade Commission, Marketer of “Free Credit Reports” Settles FTC Charges (Aug. 16, 2005), available at <http://www.ftc.gov/opa/2005/08/consumerinfo.shtm>.

<sup>2</sup> *Id.*

<sup>3</sup> Press Release, Federal Trade Commission, *Consumerinfo.com* Settles FTC Charges (Feb. 21, 2007), available at <http://www.ftc.gov/opa/2007/02/cic.shtm>.

<sup>4</sup> Free Annual Credit Reports, <http://www.ftc.gov/bcp/online/edcams/freereports/index.html>.

<sup>5</sup> FTC Consumer Alert, Want a Free Annual Credit Report? (May 2006), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt156.shtm>; Facts for Consumers, Your Access to Free Credit Reports (Sept. 2005), available at <http://www.ftc.gov/bcp/online/pubs/credit/freereports.shtm>.

<sup>6</sup> Facts for Consumers, Trial Offers: The Deal is in the Details (June 2001) available at <http://www.ftc.gov/bcp/online/pubs/products/trialoffers.shtm>.

<sup>7</sup> Free Annual Credit Reports, Radio PSAs, available at <http://www.ftc.gov/bcp/online/edcams/freereports/psa.html#onesource>; Free Annual Credit Reports, Radio PSAs, available at <http://www.ftc.gov/bcp/online/edcams/freereports/psa.html#solicitations>.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO  
RICHARD JOHNSON

*Question.* Next summer, every consumer who registered on the Do Not Call list in 2003 will have to re-register. What is your organization doing to prepare for the re-registration?

*Answer.* AARP shares the concern of Members of Congress regarding consumers' need to re-register for the Do Not Call Registry next year. The DNCR is one of the most successful consumer programs initiated by the government. With over 140 million telephone numbers registered on the list, consumers have realized a substantial decrease in the number of unwanted telemarketing calls they receive in their homes. Consumers will most certainly want to continue to participate in this valuable program.

AARP will use its resources to inform its 39 million members about the re-registration process through a number of communication avenues that could include AARP publications, outreach materials, the Web, our call center, and AARP's state offices and volunteer network. AARP will work closely with the Federal Trade Commission and the Federal Communications Commission to ensure that consumer information about this process is clear and non-misleading.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO  
JERRY CERASALE

*Question.* Next summer, every consumer who registered on the Do Not Call list in 2003 will have to re-register. What is your organization doing to prepare for the re-registration?

*Answer.* Approximately one third of the numbers on the National Do Not Call Registry will need to be re-registered by October 2008. The remaining two thirds of the numbers will need to re-register over the course of the next 5 years. As in 2003, the Federal Trade Commission will be using publicity, mainly through the press, but also on its publications, on its website and in its announcements, to promote the need for citizens to re-register their telephone numbers after 5 years. Since the initial publicity in 2003 was very successful, the DMA expects the 2008 campaign to meet similar success.

As I testified, 30 percent to 40 percent of the telephone numbers on the Registry are not useful for marketers following either the Federal Trade Commission or Federal Communications Commission regulations. They are abandoned numbers, business numbers, cell numbers and fax numbers that clutter the registry increasing costs to all. We hope that the new contractor for the Do Not Call Registry will take advantage of the 5 year timing to improve the hygiene of the list—making it more effective and less costly.

DMA is telling its members to be mindful that the telephone numbers placed on the Registry in 2003 were done so by consumers wanting to limit telephone solicitations. Therefore, after the 5-year period ends, many of those consumers may want to re-register their telephone numbers, and marketers should provide them the time to do so before presenting any marketing offers via telephone.