



Federal Trade Commission

**American Teleservices Association
Washington Summit
Washington, DC**

**Remarks of David C. Vladeck¹
Director, FTC Bureau of Consumer Protection
April 27, 2010**

Good morning. I want to thank the American Teleservices Association (ATA) for inviting me to speak at your Washington Summit. I appreciate having the opportunity to address so many members of the telemarketing industry. We've enjoyed working closely with ATA over the past several years. As in the past, we are going to disagree on some approaches and outcomes. But, our discussions have gotten richer and more candid, which has been helpful and rewarding. I value your input on what we do.

Robocall Regulations

Let me start today by going through some details about the new regulations regarding robocalls – outbound telemarketing calls that deliver a prerecorded message. What we heard loud and clear throughout the rule making process was that consumers really dislike robocalls. And as you know, in August 2008, the Commission issued amendments to the Telemarketing

¹The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

Sales Rule (TSR) that include provisions focused on robocalls.² Some of these provisions went into effect in December 2008, and others, in September 2009.

The provisions form what I consider a balanced, comprehensive regulatory framework. The new rules – now in effect – expressly prohibit all telemarketing robocalls unless the seller has obtained the call recipient’s prior signed, written agreement to receive such calls from that seller. No longer does an “established business relationship” provide a basis for placing any call that delivers a prerecorded message. A few more things you should know: the written agreement is required regardless of whether the number called is on the National Do Not Call Registry. It also does not matter whether the call delivering a prerecorded message is answered “live” by a person or by an answering machine or voicemail service. Violators of the robocall provisions face penalties of up to \$16,000 per call.

Further, even if the telemarketers and sellers have written permission, the prerecorded message must provide an automated mechanism enabling the recipients to opt out of further calls. If the call could be answered by a person, the recipient of the call must be given the opportunity to make a do-not-call request through an automated interactive voice or keypad-activated opt-out mechanism. If the call could be answered by an answering machine or voicemail service, the message must provide a toll-free number at which the recipient of the call can make a do-not-call request through such an automated mechanism. In a nutshell, all prerecorded messages delivered must disclose that the recipient may assert a do-not-call request in this manner.

²See 73 Fed. Reg. 51,163 (2008).

The amendments specify that the opt-out mechanism must be disclosed “immediately” following disclosure of the name of the seller, the purpose of the call, and the nature of the goods or services being sold.³ Moreover, if the recipient invokes the opt-out mechanism, that mechanism must automatically add the number to the seller’s do not call list, and then “immediately” disconnect the call. We want to ensure that the ability of consumers to assert a do-not-call request in response to a prerecorded message is comparable to what happens in a live call. Just as a person who receives a call from a live sales representative may “interrupt the sales pitch immediately to make a do-not-call request, and the sales representative must take that request without delay,” the Rule requires that prerecorded calls give the recipient of the call the opportunity to cut off the sales pitch, assert a do-not-call request, and end the call.⁴

Enforcement of Robocall Regulations and Do Not Call Provisions

The Commission will enforce these provisions fully and already has brought actions alleging violations of the new provisions.

In fact, just this morning and perhaps not coincidentally, the Commission announced settlements with The Talbots, Inc., and its telemarketer, SmartReply, Inc., resolving two cases challenging robocalls that targeted consumers who had recently made purchases from Talbots. When these calls were made last year, delivering recordings to such customers was permissible, although the TSR now requires written authorization. The Commission alleges, however, that these prerecorded messages were unlawful because they failed to promptly and properly disclose how the consumers could request that Talbots take them off the list of customers receiving such

³See 71 Fed. Reg. 58,715, 58,718 (2006).

⁴See 69 Fed. Reg. 67,287, 67,288-89 (2004).

messages. The Commission's investigation found that the messages did not include an opt-out automated key-pad mechanism or toll free number until after thirty or more seconds into the prerecorded message. Indeed, some of the messages did not describe an opt-out at all. The prerecorded message also did not disconnect the calls immediately when a consumer pressed the key-pad prompt to assert a do-not-call request. Instead, consumers were connected to additional recordings and advertising.

To settle the Commission's allegations that this campaign violated the TSR's requirements for prerecorded messages, Talbots and SmartReply agreed to injunctions and judgments for \$112,000 in civil penalties.

These settlements also illustrate that limiting the delivery of prerecorded messages to persons who have given written authorization or are previous donors to a charity is not sufficient, by itself, to satisfy the new provisions. The messages must promptly disclose how the recipient can easily opt out of listening to these recorded solicitations, and the telemarketer must immediately disconnects the call when the recipient registers a do-not-call request in this way.

The FTC continues to hold violators of the Do Not Call provisions accountable. In April, Direct TV and Comcast settled charges that the Department of Justice (DOJ) had brought on behalf of the FTC. The FTC charged Direct TV with violating the TSR's Do Not Call provisions and violating a federal court order entered against the company in 2005 for related conduct. Direct TV agreed to pay \$2.31 million in civil penalties. Comcast, which the FTC alleged also violated Do Not Call provisions, paid \$900,000 in civil penalties.⁵

⁵ See Press Release, DIRECTTV, Comcast to Pay Total of \$3.21 Million for Entity-Specific Do Not Call Violations (April 16, 2009), *available at* <http://www.ftc.gov/opa/2009/04/directv.shtm>.

In the Dish Network case, on referral from the FTC, the DOJ and the States of California, Illinois, North Carolina and Ohio filed suit in March 2009 against one of the country's largest satellite-television companies for calls that it and its authorized dealers made to consumers on the Do Not Call Registry. As the FTC's press release noted:

“If you call consumers whose numbers are on the Do Not Call Registry, you're breaking the law. If your authorized dealers call consumers whose numbers are on the Registry, you're breaking the law.”⁶

Dish Network filed a motion to dismiss the complaint, arguing that it was not liable for the actions of its dealers. The Court denied Dish Network's motion, and then denied a second motion in which Dish Network asked the Court to reconsider its decision. Together with DOJ and the State Attorneys' General offices, the FTC is continuing to prosecute this case vigorously. The bottom line remains the same as it always has -- sellers are on the hook for their own calls as well as for calls placed by their dealers.

Enforcement of the TSR and Fraud Violations Combined

I'm sure that you won't be surprised that much of our robocall and Do Not Call enforcement also has targeted fraud. For example, last month, the Commission settled its suit against two of the defendants in *FTC v. Voice Touch*. The Commission obtained a restraining order against Voice Touch last May after showing that Voice Touch arranged robocalling services to deliver millions of illegal prerecorded pitches that misled consumers into thinking that the callers were affiliated with consumers' car dealership or manufacturer, and that their

⁶ See Press Release, FTC Charges Dish Network, Formerly Known as EchoStar, with Multiple Do Not Call Violations (March 25, 2009), available at <http://www.ftc.gov/opa/2009/03/echostar.shtm>.

auto warranty was expiring or about to expire.⁷ The complaints also alleged that the defendants violated the robocall provisions. The Defendants agreed to a complete ban on future telemarketing and to pay more than \$650,000 for consumer redress.

And in December 2009, the Commission announced cases against three companies allegedly making millions of robocalls to sell worthless credit-card interest-rate reduction programs for large up-front fees. The court issued an order temporarily halting these companies from making any further robocalls pending trial.⁸

In the past year, the FTC also has sued a variety of companies that have allegedly violated the TSR while conducting calling campaigns delivering bogus charitable solicitations⁹

⁷ See Press Release, Auto Warranty Robocallers To Pay \$655,000 and Sell Assets For Consumer Redress (March 25, 2010), *available at* <http://www.ftc.gov/opa/2010/03/voicetouch.shtm>.

⁸ See Press Release, FTC Sues to Stop Robocalls With Deceptive Credit Card Interest-Rate Reduction Claims (December 8, 2009), *available at* <http://www.ftc.gov/opa/2009/12/robocall.shtm>.

⁹ See Press Release, New Jersey-Based Telephone Fundraisers Banned from Soliciting Donations; Will Pay \$18.8 Million for Violating FTC Order (March 31, 2010), *available at* <http://www.ftc.gov/opa/2010/03/cdg.shtm>; Press Release, Telemarketers Barred from Falsely Telling Consumers that Proceeds from the Sale of Household Goods Will Benefit Charities or the Disabled (April 8, 2010), *available at* <http://www.ftc.gov/opa/2010/04/helphands.shtm>.

or making fraudulent offers of grant money,¹⁰ health care services,¹¹ or foreclosure-rescue relief.¹²

Frauds are often perpetrated through the use of telemarketing campaigns that violate the TSR, and the robocall provisions in particular. Although none of the robocall cases brought so far has alleged that a company lacked written consent, we are closely monitoring the market for such cases. And, as always, we welcome complaints in this area.

Industry Self-Regulation

Turning to the industry's self-regulation efforts, my staff and I have had many conversations with Tim Searcy and others about ATA's Self-Regulatory Organization and about the possibility of incorporating this training and auditing initiative as part of the FTC's telemarketing enforcement program, with a focus on Do Not Call issues.

First and foremost, I'm a big advocate of self-regulation, provided that self-regulation is based on clear guidelines that are subject to rigorous and meaningful enforcement. In short, a self-regulatory program must have teeth. There are many solid models out there that benefit consumers and industry. ATA's SRO program has made substantial strides and, I understand, already provides a valuable tool for many of you. Real training, independent auditing, and

¹⁰ See Press Release, FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009), *available at* <http://www.ftc.gov/opa/2009/07/shortchange.shtm>.

¹¹ See Press Release, FTC Actions Stop Deceptive Schemes in "Operation Tele-PHONEY" Cases (August 25, 2009), *available at* <http://www.ftc.gov/opa/2009/08/telephony.shtm>.

¹² See Press Release, Defendants Banned from Mortgage Foreclosure 'Rescue' Business (March 22, 2010), *available at* <http://www.ftc.gov/opa/2010/03/foreclosure.shtm>.

certification in TSR compliance are the right goals, and the SRO program looks by all accounts to be a great way to achieve those goals.

I fully support your hard work on the SRO program. I am pleased with its progress and look forward to continued discussions with you about it.

Two Areas of Interest

Negative Options: I would now like to discuss two areas that have been ripe for fraud, and where we can do more: negative option marketing and remotely administered checks.

I am sure you are familiar with negative option marketing: it occurs when a marketer takes a consumer's silence as agreement to continue a transaction, such as monthly billing for membership in a discount buying club. While these offers can provide benefits to consumers, they also pose a high risk of deception. Unscrupulous marketers use negative options to trap consumers in a cycle of recurring charges for goods or services they do not want and never knew they purchased.

The FTC and its state law enforcement partners have taken aggressive action against abusive negative option marketing. Indeed, in the past 10 years, the Commission has brought 60 cases against negative option marketers hawking everything from dietary supplements to buyers' clubs. Most recently, we brought a case against a massive get-rich-quick scheme perpetrated by John Beck and several co-defendants, which included telemarketers.

The Defendants in this case allegedly made false and unsubstantiated claims about potential earnings for users of their money-making systems. Through infomercials, they sold the systems for \$39.95 and then contacted the purchasers via telemarketing to offer "personal coaching services," which cost several thousand dollars and purportedly enhanced the purchaser's ability to earn money quickly and easily. In addition, all purchasers were signed up

for continuity programs that cost almost \$40 per month, but which were not adequately disclosed to consumers. We believe that consumers likely lost more than \$300 million in this scheme.¹³

The Beck case involves infomercials and telemarketing, but we have seen lots of problems with negative option marketing online, in connection with, for example, “free” trial offers or “teaser” rates for teeth whitening and various dietary supplements, as well as other “get-rich-quick” opportunities. Also, among my favorites, are the offers to purchase information on how to obtain a government grant in connection with the economic stimulus plan, to help you pay off your debts and remodel your kitchen. Disclosed cost: just \$1.99. Surreptitiously and, as the FTC alleged, illegally, defendants debited consumers’ accounts nearly \$100 every month because they enrolled people in a membership club.

Remotely Administered Checks: The second troubling area is remotely created checks, often called demand drafts. In early 2009, FTC staff held a Fraud Forum to examine how the FTC can more effectively protect consumers from fraudulent schemes. Participants of the Forum emphasized the tremendous risk posed by remotely created checks, which are largely unregulated and are the source of significant fraud.¹⁴

We know too well from our law enforcement experience that fraudulent telemarketers may prefer to process payments by demand drafts, because of the limited regulatory oversight. This is a real problem. As a result, in the Fraud Forum Report, the staff recommended that the Commission initiate a rule making under the TSR to determine whether to prohibit the use of

¹³ See Press Release, FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009), available at <http://www.ftc.gov/opa/2009/07/shortchange.shtm>.

¹⁴ See Press Release, FTC Issues Staff Report on Agency’s Fraud Forum (December 29, 2009), available at <http://www.ftc.gov/opa/2009/12/fraud.shtm>.

remotely created checks in telemarketing. If we go down this path, I hope you will weigh in on the proposal. As in past TSR proceedings, your input is quite valuable.

Another “Hot” Area:

Let me now move away from issues that clearly and directly impact your industry to a “hot” area that, at a minimum, may have ripple effects on what you do—consumer privacy and, more specifically, the privacy concerns related to behavioral advertising. Ensuring the privacy of consumers’ personal information has been one of the FTC’s top consumer protection priorities for more than a decade.

Over the past several months, we’ve held a series of roundtables to get a current and fuller sense of what consumer privacy is about today. To date, we’ve learned a good deal. First, that consumers have little understanding of commercial information-collection practices. They do not really understand what data is collected about them, how the data is used and shared, and whether and how they can exercise control over their data.

A second and related point is that, although traditional, lengthy privacy notices are not effective, there continues to be an important role for privacy disclosures. Industry is coming up with interesting innovations in this area.

Third, we learned that consumers **DO** care about privacy. One area in particular has garnered lots of attention, namely behavioral targeting.

Target marketing based upon online behavior directly raises thorny privacy issues. In behavioral advertising, companies track consumers’ online activities in order to deliver advertising tailored to the consumers’ interests. For instance, a consumer who lives in Washington, D.C. and searches online for information on the Seattle Mariners might be served ads for airfare sales to Seattle, Seattle hotels, or perhaps Nationals games in the D.C. area.

Often, the companies involved in behavioral advertising are “network advertisers,” who select and deliver advertisements to multiple websites that participate in their networks. They commonly track consumer behavior by placing a file called a “cookie” on a consumer’s computer that tracks which web pages have been visited, what content was viewed, what queries were typed into search engines, and whether the user has clicked on particular advertisements. In many cases, the information collected through the use of cookies is not personally identifiable in the traditional sense of including a consumer’s name and address, but is instead identified with a particular computer or IP address. However, in some cases sufficient amounts of data may be collected that in the aggregate could be analyzed and used to identify a specific person.

Behavioral advertising offers potential benefits for consumers. Online advertising in general helps support free Internet content that many consumers value, and the targeted nature of behavioral advertising makes online advertising more efficient and attractive to advertisers. The practice may also potentially reduce unwanted advertising and increase the amount of advertising that a particular consumer finds relevant and useful. The Commission makes an effort not to stifle innovation and to allow responsible business practices to develop and flourish.

However, behavioral advertising also raises serious privacy concerns. These include the invisibility of the practice to consumers, the lack of effective disclosures about the practice, the potential to develop and store detailed profiles about consumers, and the risk that the data collected for behavioral advertising – including sensitive data regarding health, finance, or children – could fall into the wrong hands or be used for unanticipated purposes.

One year ago, the Commission staff issued a set of revised behavioral advertising self-regulatory principles to encourage the industry to provide more comprehensive and accessible protections to consumers. We did this after holding a workshop on the issue and reviewing

comments from industry members, privacy advocates, and other stakeholders. I urge you to review those principles, which are available on the FTC website.¹⁵

As I mentioned earlier, there are many intertwined pieces in the privacy dialog, beyond the behavioral marketing pieces. Many are asking about our next steps: We intend to continue the collaborative process we started with the roundtables. Given the challenges involved, we aren't about to just pop out a "New Framework" on our own, fully formed and ready for implementation. Instead, we're going to take a little time to put our thoughts together and then likely put them out for public comment – just as we have in prior efforts such as those involving behavioral advertising.

Conclusion–Do Not Call Registry

As I close, let me make a few points about the Do Not Call Registry. I hope you agree with me that the Do Not Call Registry is a huge success. The Registry has been enthusiastically embraced by consumers since it was introduced in 2003, and there are currently over 191 million telephone numbers on the Registry.¹⁶ And, as my colleagues and I have said on many occasions, the success of the DNC Program is, in no small part, a reflection on your members' substantial compliance efforts.

As you probably know, when the Do Not Call Registry was established, registrations were set to expire after five years. However, due to changes implemented by the Do No Call Improvement Act of 2007, registrations are now permanent and do not expire after any particular length of time. In light of this change, the Commission is taking steps to ensure the continued

¹⁵See <http://www.ftc.gov/opa/2007/12/principles.shtm>

¹⁶ See Press Release, FTC Approves Two Reports to Congress on the National Do Not Call Registry (Jan 4, 2010), *available at* <http://www.ftc.gov/opa/2010/01/donotcall.shtm>.

accuracy of the Registry. We are making efforts to keep up with technology and ensure that abandoned numbers are eliminated from the Registry, while ported numbers – including cell phone numbers, and Voice over Internet Protocol (VoIP) numbers – are not.

In short, the Commission tries to stay on the leading edge of technological and industry developments to make sure that our enforcement efforts remain effective and relevant. I look forward to working with you as our regulatory and enforcement programs continue to evolve. We want to hear from you.