

**BEFORE THE**  
**SENATE COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION**

**HEARING ON**  
**S. 704, THE TRUTH IN CALLER ID ACT**

**JUNE 21, 2007**

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

Jerry Cerasale  
Senior Vice President, Government Affairs  
Direct Marketing Association, Inc.  
1615 L Street, NW Suite 1100  
Washington, DC 20036  
202/955-5030

## **I. Introduction & 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 as it examines S. 704 and the caller ID spoofing issue in general.

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 Committee’s continued outreach to the business community on important issues such as caller ID spoofing. DMA fully supports the efforts of Senators Nelson, McCaskill, and Snowe, and the Committee, to enact legislation prohibiting caller ID spoofing. Spoofing is a malicious practice that undermines caller ID as a useful verification device, and can cause harm to both consumers and business. DMA has long recognized caller ID as an important enhancer to two-way communication between people making and receiving calls, especially in the context of business and customer relations. Caller ID provides consumers with choice and control over their telephones. It alerts a consumer as to the identity of a caller and allows the consumer to choose whether to answer a call from a marketer offering a product or service of interest.

Caller ID, when used for illegitimate purposes, can have a harmful effect on consumers and legitimate marketers and other businesses. Bad actors use caller ID spoofing to damage a competitor's reputation, to gain unauthorized access to a consumer's personal information, and to commit illicit practices such as phishing and pretexting. The cumulative effect is consumer confusion, possible identity theft, and the transfer of ill will to legitimate businesses and marketers. We believe that spoofing, and, in general, the manipulation of caller ID for illegitimate purposes, should be prohibited.

Understanding the importance of standards and best practices in fostering consumer choice, DMA several years ago, working with our members, developed and adopted Caller-ID Requirements as part of our Guidelines for Ethical Business Practice ("Guidelines"), to specifically discourage illegitimate telemarketing practices that threaten to undermine consumer confidence and relations with legitimate marketers.<sup>1</sup> In 2004, in response to a rise in caller ID spoofing, DMA issued an advisory detailing marketers' rights and responsibilities when using caller ID technology.<sup>2</sup> DMA requires its members, including nonprofits and other groups, to transmit caller ID information. Specifically, when DMA members make marketing calls, they are required to transmit the name of the seller and the telephone number by which a called party can call back during normal business hours to ask questions or request not to receive future calls. Under our Guidelines, DMA members must not transmit a false name or telephone number.

DMA also supports the importance of accurately disclosing identity and contact information in other forms of marketing communications. For example, in the e-mail context, our Guidelines detail responsible practices for marketers to disclose accurate identifying information. The problems caused by inaccurate e-mail headers are similar to those in the caller ID spoofing context. In 2002, in response to illegitimate actors manipulating e-mail message headers, we developed and adopted Commercial

---

<sup>1</sup> Caller-ID/Automatic Number Identification Requirements, Article #46, DMA Guidelines for Ethical Business Practice, at 23 (attached) (available at <http://www.the-dma.org/guidelines/EthicsGuidelines.pdf>).

<sup>2</sup> DMA Statement Caller-ID Falsification, September 2004 (attached) (available at <http://www.the-dma.org/guidelines/callerid/shtml>).

Solicitations Online requirements as part of our Guidelines.<sup>3</sup> Our members are required to clearly disclose the marketer’s identity and street address in e-mail solicitations. The identity of the sender of the message must be provided clearly, honestly, and not in a misleading manner. The subject lines must accurately convey the content of the message, and the header information must be accurate. These requirements are also part of the CAN-SPAM Act that emerged through this Committee.

## **II. Legislation Should Include an “Intent to Defraud or Cause Harm” Requirement**

As stated at the outset, DMA supports the purpose of S. 704, to prevent the manipulation of caller ID for fraudulent, spoofing purposes. While the practice of spoofing to defraud or cause harm to a person is unacceptable, there are legitimate reasons for transmitting caller ID information that is different from the calling party’s information that the Committee should ensure are not restricted. Blocking or modifying caller ID information is necessary in several contexts such as safety, protecting privileged communications, and in business and customer relations. Businesses rely on the practice of modifying caller ID for such purposes as to facilitate a consumer’s request to be placed on a business’s do-not-call list and to properly disclose the identity of the entity on whose behalf a third-party marketer is calling. In order to ensure that non-spoofing activities that may involve display of caller ID information that is different from that of the entity making the call are not unintentionally covered by the legislation, we suggest that the scope of conduct covered by the legislation should be narrowed to restrict only such acts committed with “intent to defraud or cause harm.”

Inclusion of such an “intent to defraud or cause harm” standard will serve the purpose of explicitly recognizing that the widely adopted business practice of transmitting a customer service telephone number in place of the calling party’s telephone number is not restricted. Without such an intent standard, telemarketers that substitute a customer service telephone number for call back purposes could be covered

---

<sup>3</sup> Commercial Solicitations Online, Article #38, DMA Guidelines for Ethical Business Practice, at 20 (attached) (available at <http://www.the-dma.org/guidelines/EthicsGuidelines.pdf>).

by the bill. This practice is, in fact, currently required under existing law whereby marketers are required to transmit a telephone number through a caller identification service by which a called party may place a return call to make inquiries or request that their telephone number be added to the calling party's do-not-call list. Often businesses provide the telephone number of their customer service department to facilitate such requests rather than the number of the calling party's line. Businesses that employ such practices are not seeking to defraud or mislead customers, but rather transmitting the most relevant information and creating processes to efficiently respond to customer requests.

In addition, we are aware of scenarios where the caller ID information transmitted from the telemarketer to a telecommunications carrier is not the same as the information provided by the carrier to the call recipient. With a strict liability standard, and with no intent standard, telemarketers could be liable for an act of the carrier over which the telemarketer has no control. Thus, the addition of an "intent to defraud or cause harm" standard also will ensure that a telemarketer is only responsible for accurately providing caller ID information to the carrier and not for incorrect transmission by the carrier.

Requiring that a calling party provide its exact name and telephone number could jeopardize legitimate practices and restrain consumer preferences. Requiring "intent to defraud or cause harm" will ensure that bad actors with ill intent are targeted by the legislation rather than legitimate practices, customer preferences, and the underlying technology used. We believe that tying the act of transmitting misleading caller ID information with an intent standard appropriately identifies the offending act while ensuring that businesses are not liable for simple mistakes or other instances where changing the caller ID information is appropriate. We note that this is the approach that is in the caller ID spoofing bills that recently passed the House of Representatives.

\* \* \*

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

## Excerpts from the DMA Guidelines for Ethical Business Practice

### COMMERCIAL SOLICITATIONS ONLINE

#### Article #38

Marketers may send commercial solicitations online under the following circumstances:

- The solicitations are sent to the marketers' own customers, or
- Individuals have given their affirmative consent to the marketer to receive solicitations online, or
- Individuals did not opt out after the marketer has given notice of the opportunity to opt out from solicitations online, or
- The marketer has received assurance from the third party list provider that the individuals whose e-mail addresses appear on that list:
  - have already provided affirmative consent to receive solicitations online, or
  - have already received notice of the opportunity to have their e-mail addresses removed and have not opted out, and
- The individual is not on the marketer's in-house suppression list

Within each e-mail solicitation, marketers should furnish individuals with a notice and an Internet-based mechanism they can use to:

- Request that the marketer not send them future e-mail solicitations and
- Request that the marketer not rent, sell, or exchange their e-mail addresses for online solicitation purposes

If individuals request that their names be removed from the marketer's in-house online suppression list, then the marketer may not rent, sell, or exchange their e-mail addresses with third parties for solicitation purposes.

The above requests should be honored within 10 business days, and the marketer's opt-out mechanism should be active for at least 30 days from the date of the e-mail solicitation.

Only those marketers that rent, sell, or exchange information need to provide notice of a mechanism to opt out of information transfer to third-party marketers.

Marketers should process commercial e-mail lists obtained from third parties using DMA's E-Mail Preference Service suppression file. E-MPS need not be used on one's own *customer* lists, or when individuals have given affirmative consent to the marketer directly.

Solicitations sent via e-mail should disclose the marketer's identity and street address. The subject and "from" lines should be clear, honest, and not misleading, and the subject line should reflect the actual content of the message so that recipients understand that the e-mail is an advertisement. The header information should be accurate. A marketer should also provide specific contact information at which the individual can obtain service or information.

\* \* \*

**CALLER-ID/AUTOMATIC NUMBER IDENTIFICATION REQUIREMENTS**  
**Article #46**

Wherever the technology is available marketers should:

- Transmit a telephone number such as the telephone number of the seller, service bureau, or customer service department that the consumer can call back during normal business hours to ask questions and/or to request not to receive future calls and
- Transmit the name of the seller or service bureau

Marketers should not block transmission of caller identification or transmit a false name or telephone number.

Telephone marketers using automatic number identification (ANI) should not rent, sell, transfer, or exchange, without customer consent, telephone numbers gained from ANI, except where a prior business relationship exists for the sale of directly related goods or services.

## DMA STATEMENT CALLER-ID FALSIFICATION

**Falsely altering Caller-ID information for marketing purposes is not only unethical, it is illegal!**

In response to recent news reports about a new Caller-ID service that would allow subscribers to transmit false Caller-ID information, The DMA has issued this statement to remind marketers about their rights and responsibilities when using Caller-ID technology.

When calling customers or prospects, it is deceptive and unlawful for a marketer to knowingly substitute and transmit a false, or 'dummy,' telephone number. Rather, wherever the technology is available, a marketer must:

- transmit the name of the seller or service bureau; and
- transmit an accurate and valid telephone number for the seller, the service bureau, or respective customer service department. A consumer should be able to call back this telephone number during normal business hours to ask questions and/or to request not to receive future calls.

Please note that a marketer MAY transmit a Caller-ID telephone number that is DIFFERENT from the number from which the call is coming AS LONG AS the number transmitted correctly identifies the name of the seller or service bureau and is a valid number that the consumer may call back during normal business hours to ask questions and/or to request not to receive future calls. For example, sometimes it may be necessary to transmit a Caller-ID number for the customer service department, instead of the number of the representative who is calling (since the representative's number will likely be busy). In this instance, substituting the customer service department number provides the consumer with a number he/she can call back for more information and/or to request to be put on the company's do-not-call list.

A marketer who intentionally creates and transmits inaccurate or false Caller-ID information is violating federal law—for starters, the Federal Trade Commission Act (which outlaws unfair and deceptive trade practices), the Federal Trade Commission's Telemarketing Sales Rule, and the Federal Communications Commission's Telephone Consumer Protection Act.

Moreover, transmitting false Caller-ID information violates the Direct Marketing Association's Guidelines for Ethical Business Practices (*Article #44* and *Article #51*). Specifically, *Article #44* (Caller-ID/Automatic Number Identification Requirements) advises: "Marketers should not block transmission of caller identification or transmit a false name or telephone number..." *Article #51* (Laws, Codes, and Regulations) calls for marketers to abide by state, federal and local laws governing marketing practices and business transactions.