PACIFIC TRIAL ATTORNEYS
A Professional Corporation
Scott J. Ferrell, Bar No. 202091
sferrell@pacifictrialattorneys.com
Victoria C. Knowles, Bar No. 277231
vknowles@pacifictrialattorneys.com
4100 Newport Place, Ste. 800
Newport Beach, CA 92660
Tel: (949) 706-6464
Fax: (949) 706-6469

Attorneys for Plaintiff and the Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JIM REIDER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ELECTROLUX HOME CARE PRODUCTS, INC.., a Delaware corporation; and DOES 1 – 10, inclusive,

Defendants.

Case No. 8:17-cv-26

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jim Reider ("Plaintiff") brings this action on behalf of himself and all others similarly situated against Electrolux Home Care Products, Inc. ("Electrolux" or "Defendant") and, based on personal knowledge as to his own actions and upon information and belief, based upon the investigation of counsel, as to the actions of Defendant, alleges as follows:

I. INTRODUCTION & OVERVIEW OF CLAIMS

1. Plaintiff bring this action on his own behalf and on behalf of similarly situated consumers who purchased items from Defendant and were charged a "Shipping/Handling" charge. These charges violated the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.* and the Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750 *et seq*. because, in contravention of established ethical principles, Defendant's shipping/handling charges were not reasonably related to Defendant's costs of delivering or shipping the items to consumers but instead greatly exceeded those costs.

2. Defendant's delivery charges also violated the above statutes' prohibitions against fraudulent and/or deceptive practices. They deceived consumers, who expect that shipping/handling charges are reasonably related to a company's actual costs of shipping and delivery.

3. Additionally, the arbitration provision contained in Defendant's website, www.eureka.com, is unenforceable because there is no mutual consent for the provision; the terms allow Defendant unilaterally to change or modify the terms at any time, and the provision requires consumers to bear their own attorneys' fees.

II. JURISDICTION AND VENUE

4. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), because members of the proposed Class are citizens of states different from Defendant's home state, there are more than 100 Class Members, and the amount-in-controversy exceeds $5,000,000 exclusive of interest and costs.

/ / /

5. This Court has jurisdiction over the Defendant named herein because Defendant has sufficient minimum contacts with California and/or otherwise intentionally avails itself of the laws and markets of California, through the promotion, sale, marketing and distribution of its goods and services in California, to render the exercise of jurisdiction by the California courts permissible.

6. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant's improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district, because Defendant has caused harm to Class Members residing in this district, and/or because the Defendant is subject to personal jurisdiction in this district.

III. PARTIES

7. Plaintiff Jim Reider is an individual adult resident and citizen of California, residing in Orange County, California.

8. Plaintiff is informed and believes, and upon such information and belief alleges, that Defendant Electrolux Home Care Products, Inc. is a Delaware corporation, with its principal place of business located at 10200 David Taylor Drive, Charlotte, NC 28262. As such, Defendant is a citizen of Delaware and North Carolina. Plaintiff is informed and believes, and upon such information and belief alleges, that at all times relevant, Defendant conducted business in the State of California and in Orange County, within the Central District of California.

9. The true names and capacities of the Defendants sued herein as DOES 1 through 10, inclusive, are currently unknown to Plaintiff, who therefore sues such Defendants by fictitious names. Each of the Defendants designated herein as a DOE is legally responsible for the unlawful acts alleged herein. Plaintiff will seek leave of Court to amend this Complaint to reflect the true names and capacities of the DOE Defendants when such identities become known.

10. At all relevant times, each and every Defendant was acting as an agent and/or employee of each of the other Defendants and was acting within the course

and/or scope of said agency and/or employment with the full knowledge and consent of each of the Defendants. Each of the acts and/or omissions complained of herein were alleged and made known to, and ratified by, each of the other Defendants (Electrolux Home Care Products, Inc., and DOE Defendants will hereafter collectively be referred to as "Defendant").

IV. FACTUAL BACKGROUND

A. Background of the Action

11. This action is brought by Plaintiff on behalf of himself and similarly situated consumers who were charged excessive, deceptive, unfair and unethical fees for delivery of products by Defendant during the period of the applicable statutes of limitations for Class members in California (the "Class Period").

12. Under the brand name "Eurkea," and through its website, www.eureka.com, Defendant markets assorted products at nominal prices, but then charges an additional fee for "Shipping/Handling" that is far in excess of the actual cost of shipping the product to consumers.

13. Specifically, customers order promotional products from Eureka, for which they are purportedly charged only a nominal amount, but are then charged "Shipping/Handling" fees many times the amount of the actual product charge. As set forth below, the "Shipping Method" portion of a charge provides for a choice of

1. Ground Service at $7.99;
2. Second Day Air Service at $15.00; and
3. Next Day Air Service at $25.00.

/ / /

/ /

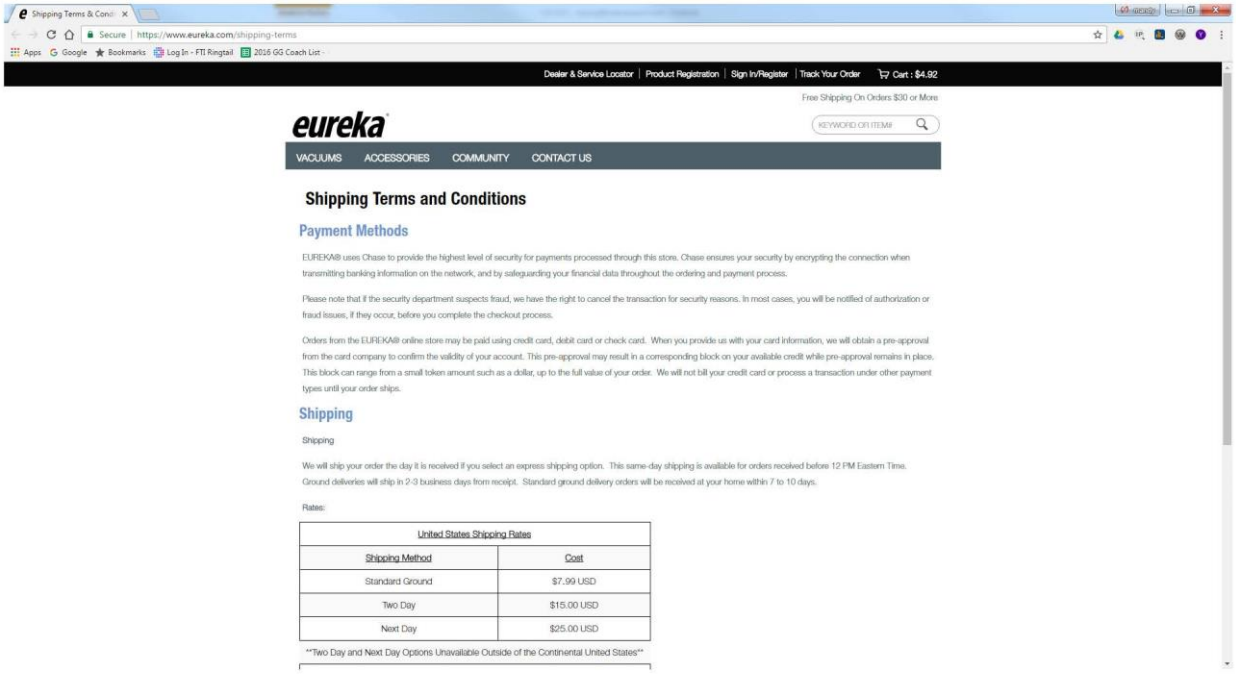
/ / /

/ / /

/ / /

/ / /

The following shows an enlarged version of what customers view on Defendant's website:



14. The prices of these delivery methods bear no reasonable relationship to and, in fact, greatly exceed Defendant's costs incurred for delivery; they, therefore, contain improper and unethical profits for Defendant.

15. These excess shipping and delivery charges are unfair, unethical and/or in violation of public policy because it violates business ethics to charge more for shipping or delivery than a company's costs of shipping, postage and handling.

16. The basis for the allegation that it is unethical to charge more for shipping or delivery than a company's costs of shipping, postage and handling comes, in part, from established ethical principles recognized by the Direct Marketing Association("DMA"), the leading industry association for companies that, like Defendant, market directly to consumers.

17. DMA has published principles of ethical business practices for such marketing activities. Direct Marketing Association's Guidelines for Ethical Business Practices, revised May 2011 ("DMA Ethical Guidelines"). A true and correct copy of

the DMA Ethical Guidelines is attached hereto as Exhibit 1. (A true and correct copy of the DMA Ethical Guideline, revised January 2014, is attached hereto as Exhibit 2.)

18. These Ethical Guidelines "are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct." *Id.* at 2. They "reflect DMA's long-standing policy of high levels of ethics and the responsibility of the Association, its members, and all marketers to maintain consumer and community relationships that are based on fair and ethical principles." *Id*. (emphasis added).

19. In addition, DMA states that the Ethical Guidelines "are intended to be honored in light of their aims and principles. All marketers should support the guidelines in spirit and not treat their provisions as obstacles to be circumvented by legal ingenuity." *Id*.

20. DMA has also published a companion volume to its Ethical Guidelines called *Do the Right Thing: A Companion to DMA's Guidelines for Ethical Business Practice* (Revised January 2009) ("*Do the Right Thing*"). A true and correct copy of this document is attached hereto as Exhibit 3. That volume is intended to "give[] direct marketers advice on how to assure their business practices comply with" the Ethical Guidelines. *Do the Right Thing* at 2.

21. As DMA recognizes, under current ethical standards, shipping and delivery charges such as those of Defendant are unethical.

22. In both the 2014 and 2011 editions of the DMA Ethical Guidelines, Article#11 states: "Postage, shipping or handling charges, if any, should bear a reasonable relationship to actual costs incurred." Ex. 1 at 1; Ex. 2 at 12.

23. With respect to Article #11, DMA's companion volume *Do the Right Thing* states: "When figuring shipping and handling fees, it is important to reflect the costs as accurately as possible so that your customers or prospects are not likely to view these fees as a company 'profit center.'" Ex 3 at 12-13.

/ / /

24. In 2003, DMA issued guidance "to assist cataloguers and other direct marketers in establishing charges for shipping, handling, and other fulfillment costs." http://www.dmaresponsibility.org/cgi/disppressrelease?article=440; a true and correct copy of this document is attached hereto as Exhibit 4. DMA stated that this new guidance "provides additional direction beyond article #11 of The DMA's Guidelines for Ethical Business Practice, which states: "Postage, shipping, or handling charges, if any, should bear a reasonable relationship to actual costs incurred." *Id.*

25. This guidance stated, "Companies should determine what costs will be covered, and substantiate their method …. Ideally, a fulfillment cost study should be done with the assistance of an impartial outside expert." *Id.*

26. The guidance also stated, "Exact charges should be disclosed clearly and conspicuously in advance of the order. … When ordering online, shoppers should receive shipping information early in the order path." *Id.*

27. The current version of DMA's ethical guidance on shipping charges is displayed on its web page entitled, "Guidance for Establishing and Substantiating Shipping and Handling Charges," (a true and correct copy of this document is attached hereto as Exhibit 5), where it states:

> Some marketers take the position that so long as there is clear disclosure on how much the consumer pays in total for the shipped product, the amount the marketer charges for shipping and handling should not matter. There appears to be a trend by law enforcement agencies, however, to insist that a consumer who is charged shipping and handling costs should be paying a fee reasonably based on the marketer's cost. The latter position is consistent with existing DMA guidelines. …. Your goal should be not to charge consumers as a whole more than you pay in total.

28. Defendant's delivery charges for products violate the ethical principle described above because they are not reasonably related to Defendant's costs; to the contrary, they include profit and make shipping and handling a profit center.

29. The statement by DMA regarding the trend among law enforcement agencies to insist that a consumer who is charged shipping and handling costs should be paying a fee reasonably based on the marketer's cost shows that the practice of charging more for shipping than a marketer's costs violates public policy.

30. Moreover, as DMA recognizes, charging a delivery charge that exceeds a company's delivery costs is deceptive because consumers expect that delivery charges are calculated based on a company's costs. In its "Guidance for Establishing and Substantiating Shipping and Handling Charges," Ex. 5, DMA states:

> Most direct marketers charge consumers for delivery of products. What the actual charges are and how these charges are calculated are significant issues for consumers.
>
> Setting shipping and handling costs is not as easy as it might, at first, seem. In a marketplace of sophisticated consumers and close scrutiny by regulators, direct marketers must be very careful. Positive consumer perception of your charges is critical to your success.

31. In its 2003 press release announcing this guidance, DMA's president echoed this statement:

> "In a marketplace of sophisticated consumers and close scrutiny by regulators, direct marketers must be very careful. Positive consumer perception of all charges, especially shipping and handling, is critical to the continued success and growth of the industry," said H. Robert Wientzen, president & CEO, The DMA.
>
> "In short, shipping and handling costs should be fair, reasonable, clear, and justifiable," said Wientzen.

32. By not informing consumers that its delivery charges greatly exceeded its costs, Defendant engaged in deception by means of the concealment, suppression or omission of material facts.

33. For these reasons, Defendant's delivery charges are deceptive, unethical and/or unfair.

B. Facts of Plaintiff's Claims Against Defendant

34. Plaintiff purchased a product from Defendant and was unfairly, unethically, deceptively and illegally charged for shipping and handling in amounts that exceeded Defendant's costs of shipping and delivery.

35. Specifically, on or about December 15, 2016, Plaintiff purchased a filter from Defendant Electrolux via its website, www.eureka.com. For the product Plaintiff was charged $1.99, while he was charged $7.99 for "Shipping/Handling".

36. The amounts Plaintiff was charged for shipping and handling had no reasonable relationship to, and, in fact, greatly exceeded, Defendant's costs incurred for shipping and delivery and constituted improper and unethical profit for Defendant. In fact, according to the calculator found at https://postcalc.usps.com/mobile/default.aspx, the actual cost of shipping and delivery was less than half of the price charged by Defendant.

37. Following his purchase, Plaintiff's counsel reviewed Defendant's website and further reviewed its Terms and Conditions. The arbitration provision contained in the website is unenforceable because there is no mutual consent for the provision; the terms allow Defendant unilaterally to change or modify the terms at any time, and the provision requires consumers to bear their own attorneys' fees.

V. CLASS ACTION ALLEGATIONS

38. Plaintiff brings this class action pursuant to Rules 23 of the Federal Rules of Civil Procedure on behalf of himself and all members of the following Class:

> "**All persons in the State of California who purchased products from www.eureka.com and were charged a fee for shipping, handling, and/or delivery within the period of the applicable statutes of limitations up to the date of trial (the "Class").**

39. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment.

40. Specifically excluded from the proposed Class is Defendant, its officers, directors, and employees. Also excluded from the proposed Class is the Court, the Court's immediate family and Court staff.

41. **Numerosity.** Membership in the Class is so numerous that separate joinder of each member is impracticable. The precise number of Class Members is unknown at this time but can be readily determined from Defendant's records. Plaintiff reasonably estimates that there are thousands of persons in the Class.

42. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff has retained counsel highly experienced in complex consumer class action litigation and intends to prosecute this action vigorously. Plaintiff is a member of the Class described herein and does not have interests antagonistic to, or in conflict with, the other members of the Class.

43. **Typicality.** Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all members of the Class purchased products from Defendant's website, www.eureka.com, were charged the "Shipping/Handling" charges for purchases from that website, and were subject to the arbitration provisions contained in the Terms and Conditions on that website.

44. **Existence and Predominance of Common Questions of Law and Fact.** There are central and substantial questions of law and fact common to all Class Members that control this litigation and predominate over any individual issues. Included within the common questions are the following:

i) Whether Defendant charged consumers an amount for shipping/handling for delivery of products;

ii) Whether the amount Defendant charged consumers for shipping/handling exceeded Defendant's actual costs for shipping or delivering the products to consumers;

/ / /

iii) Whether Defendant charged consumers for shipping/handling of product more than it paid for such shipping or delivery;

iv) Whether Defendant's actions in charging more for shipping/handling than its costs were unethical;

v) Whether Defendant's actions in charging more for shipping/handling than its costs violated the unfairness provisions of the UCL;

vi) Whether Defendant's actions in charging more for shipping/handling than its costs violated the fraudulent and unfairness provisions of the UCL;

vii) Whether Defendant's actions in charging more for shipping/handling than its costs violated provisions of the CLRA; and

viii) Whether Defendant should be required to pay Plaintiff's attorneys' fees.

45. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy for at least the following reasons:

i) Given the size of the claims of individual Class Members, as well as the resources of Defendant, few, if any, could afford to seek legal redress individually for the wrongs alleged herein;

ii) This action will permit an orderly and expeditious administration of the claims of Class Members, will foster economies of time, effort and expense, and will ensure uniformity of decisions;

iii) Any interest of Class Members in individually controlling the prosecution of separate actions is not practical, creates the potential for inconsistent or contradictory judgments, and would create a burden on the court system;

/ / /

iv) Without a class action, Class Members will continue to suffer as a consequence of Defendant's illegal and predatory conduct, Defendant's violations of law will proceed without remedy, and Defendant will continue to reap and retain the substantial proceeds derived from its wrongful and unlawful conduct. Plaintiff and the Classes are entitled to appropriate civil penalties. This action presents no difficulties that will impede its management by the Court as a class action.

46. For the above reasons, this action is maintainable as a class action pursuant to Fed. R. Civ. P. 23.

VI. DEFENDANT'S VIOLATIONS OF THE UCL, CLRA, AND LAW APPLICABLE TO ARBITRATION PROVISIONS

A. Violations of the UCL

47. The UCL outlaws "any unlawful, unfair or fraudulent business act or practice …." (Business & Prof. Code § 17200.)

48. An unfair business practice under the UCL "is one that either 'offends an established public policy' or is 'immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.'" (*Evenchik v. Avis Rent A Car Sys., LLC*, 2012 WL 4111382, at *8 (S.D. Cal. Sept. 17, 2012) *(quoting McDonald v. Coldwell Banker*, 543 F.3d 498, 506 (9th Cir.2008) (in turn quoting *People v. Casa Blanca Convalescent Homes, Inc.*, 159 Cal.App.3d 509, 530, 206 Cal.Rptr. 164 (1984)).)

49. Defendant's conduct as alleged herein has violated the unfairness prong of the UCL because it is unethical. In addition, it violates established public policy as recognized by DMA in citing law enforcement authorities in support of its ethical guideline against excessive delivery charges. It also violates public policy as recognized by the Federal Trade Commission in enforcing Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a). In *In the Matter of Bill Crouch Foreign, Inc., d/b/a Bill Crouch Imports, Inc. (Formerly Mazda of Boulder, Inc.)*, 96 F.T.C. 111,

1980 WL 339028, the FTC entered into a consent order that prohibited a car dealer from violating the FTC Act by charging an amount for "Freight" that "exceeded respondent's actual outlays to third parties for the transportation of new automobiles." *Id.* at *2. By bringing that proceeding under Section 5(a) and entering into a consent order, the FTC showed that its interpretation of Section 5(a) is that such charges violate the Act.

50. Additionally, the Ninth Circuit has ruled that courts are warranted in applying a test for unfairness that "involves balancing the harm to the consumer against the utility of the defendant's practice." (*Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 735 (9th Cir. 2007).) Under this test, Defendant's shipping/handling charges violate the UCL because the harm to the consumer outweighs the utility of Defendant's practice, which has no utility.

51. In addition, Defendants's shipping/handling charges violate the "fraudulent" prong of the UCL in that they are likely to deceive reasonable consumers who expect that delivery charges bear a reasonable relationship to a company's costs of delivery.

B. Violations of the CLRA

52. The CLRA, Civil Code Section 1770, provides, in pertinent part:

(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful: ….

(9) Advertising goods or services with intent not to sell them as advertised. …..

(14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law. ….

(19) Inserting an unconscionable provision in the contract.

53. Defendant's practices violate subparagraph (9) because Defendant represents that its shipping/handling charges have the characteristics that consumers

expect, namely, that they are reasonably related to Defendant's actual costs of shipping.

54. Defendant's practices violate subparagraph (14) because they include practices that violate established ethical standards.

55. Defendant's practices violate subparagraph (19) because they are unconscionable in that they are contained in a contract of adhesion, which consumers cannot negotiate but may only accept or reject, and because they violate established ethical standards.

C. Violations of the Law regarding Arbitration Provisions

56. Additionally, Defendant's website, www.eureka.com, contains Terms and Conditions which purport to require mandatory arbitration of any disputes and contain a class action waiver. Those provisions are unenforceable for a number of reasons.

57. First, there is no mutual assent because the provisions are contained in a "browsewrap" contract that does not require customers to read and assent to the terms prior to making a purchase. (*See Nghiem v. Dick's Sporting Goods, Inc., et al.*, (C.D. Cal. July 5, 2016) (denying a motion to compel arbitration of similar browsewrap agreement).)

58. Second, Defendant's Terms and Conditions allow Defendant unilaterally to change or modify the terms at any time, which effectively allows Defendant to "opt-out" of any obligation to arbitrate. (*See Peleg v. Neiman Marcus Group, Inc.*, 204 Cal.App.4th 1425, 1457 (2012) (invalidating arbitration provision that authorized the drafter to "pick and choose" the claims it wanted to arbitrate).)

59. Third, the provisions require consumers to bear their own attorneys' fees in violation of California law ("All other fees, such as attorneys' fees and expenses of travel to the arbitration, will be paid in accordance with JAMS Rules."). (*See Sanchez v. Valencia Holding Co., LLC*, 61 Cal.4th 899, 919 (2015) (arbitration agreement unenforceable where it "would have a substantial deterrent effect in [the consumer's] case").)

/ / /

60. Accordingly, if and to the extent that Defendant claims that its arbitration and/or class waiver provisions are enforceable against Plaintiff and the class, Plaintiff and the class seek declaratory relief declaring such provisions unconscionable and unenforceable.

VII. CAUSES OF ACTION

FIRST CAUSE OF ACTION

UNFAIRNESS IN VIOLATION OF THE UCL

(Plaintiff and the Class Against All Defendants)

61. The foregoing paragraphs are alleged herein and are incorporated herein by reference.

62. The UCL outlaws "any unlawful, unfair or fraudulent business act or practice …." (Business & Professions Code § 17200.)

63. Pursuant to the unfairness prong of the UCL, Defendant has a duty not to engage in an unfair business act or practice.

64. Defendant breached that duty by engaging in acts or practices that are unethical.

65. Defendant breached that duty by engaging in acts or practices that violate established public policy as recognized by the FTC and by DMA.

66. Defendant breached that duty by engaging in acts or practices whose harm outweighs their utility.

67. Plaintiff and the Class purchased products from Defendant via its website, and were charged for "Shipping/Handling" fees that exceeded Defendant's costs of shipping and delivery and are thereby entitled to have restored to them the sums of money that exceeded such costs.

68. Injunctive relief is necessary and proper to compel Defendant to cease its violations of the UCL alleged herein.

/ / /

/ / /

SECOND CAUSE OF ACTION

VIOLATION OF THE CLRA

(Plaintiff and the Class Against All Defendants)

69. The foregoing paragraphs are alleged herein and are incorporated herein by reference.

70. The CLRA, Civil Code Section 1770, provides, in pertinent part:

(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful: ….

(9) Advertising goods or services with intent not to sell them as advertised. …..

(14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law. ….

(19) Inserting an unconscionable provision in the contract.

71. Defendant's practices violate subparagraph (9) because Defendant represents that its shipping/handling charges have the characteristics that consumers expect, namely, that they are reasonably related to Defendant's actual costs of shipping.

72. Defendant's practices violate subparagraph (14) because they include practices that violate established ethical standards.

73. Defendant's practices violate subparagraph (19) because they are unconscionable in that they are contained in a contract of adhesion, which consumers cannot negotiate but may only accept or reject, and because they violate established ethical standards.

74. Plaintiff and the Class purchased products from Defendant via its website, and were charged for "Shipping/Handling" fees that exceeded Defendant's costs of shipping and delivery and are thereby entitled to have restored to them the sums of money that exceeded such costs.

75. Injunctive relief is necessary and proper to compel Defendant to cease its violations of the UCL alleged herein.

THIRD CAUSE OF ACTION

DECLARATORY RELIEF

(Plaintiff and the Class Against All Defendants)

76. The foregoing paragraphs are alleged herein and are incorporated herein by reference.

77. Defendant's website, www.eureka.com, contains Terms and Conditions which purport to require mandatory arbitration of any disputes and contain a class action waiver. Those provisions are unenforceable for a number of reasons.

78. First, there is no mutual assent because the provisions are contained in a "browsewrap" contract that does not require customers to read and assent to the terms prior to making a purchase. (*See Nghiem v. Dick's Sporting Goods, Inc., et al.*, (C.D. Cal. July 5, 2016) (denying a motion to compel arbitration of similar browsewrap agreement).)

79. Second, Defendant's Terms and Conditions allow Defendant unilaterally to change or modify the terms at any time, which effectively allows Defendant to "opt-out" of any obligation to arbitrate. (*See Peleg v. Neiman Marcus Group, Inc.*, 204 Cal.App.4th 1425, 1457 (2012) (invalidating arbitration provision that authorized the drafter to "pick and choose" the claims it wanted to arbitrate).)

80. Third, the provisions require consumers to bear their own attorneys' fees in violation of California law ("All other fees, such as attorneys' fees and expenses of travel to the arbitration, will be paid in accordance with JAMS Rules."). (*See Sanchez v. Valencia Holding Co., LLC*, 61 Cal.4th 899, 919 (2015) (arbitration agreement unenforceable where it "would have a substantial deterrent effect in [the consumer's] case").)

81. An actual controversy has arisen and now exists between Plaintiff and the Class, on the one hand, and Defendants, on the other hand, concerning their respective

rights and duties under the arbitration provisions of the Terms and Conditions contained on Defendant's website. Plaintiff and the Class contend that the arbitration provisions are invalid and unenforceable for the reasons set forth above. Plaintiff is informed and believes, and upon such information and belief alleges that Defendant believes and contends that the arbitration provisions of the Terms and Conditions contained on Defendant's website are valid and enforceable. Plaintiff and the Class desire a determination of their rights and duties under the arbitration provisions of the Terms and Conditions, and a declaration that those provisions are invalid and unenforceable as to Plaintiff and the Class.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the putative Class request the following relief:

1. An order for certification of the putative Class;

2. Judgment awarding Plaintiff and the Class compensatory damages, including a full refund of the amount of shipping and delivery charges they paid in excess of Defendant's actual costs of shipping and delivery;

3. Judgment awarding restitution to Plaintiffs and the Class;

4. Judgment entering preliminary and permanent injunctive relief barring Defendants from continuing the unfair and unethical practices alleged herein;

5. For a declaratory judgment determining the rights and obligations between Plaintiff and the Class, on the one hand, and Defendants, on the other hand, concerning their respective rights and duties under the arbitration provisions of the Terms and Conditions contained on Defendant's website, including a declaration that the arbitration provisions are invalid and unenforceable;

/ / /

/ /

/ / /

/ / /

/ / /

6. Reasonable attorneys' fees and costs; and

7. Such other and further relief as this Court may deem appropriate.

Dated: January 8, 2017

PACIFIC TRIAL ATTORNEYS, APC

By: */s/ Scott J. Ferrell*
Scott. J. Ferrell
Attorneys for Plaintiff and the Class

JURY DEMAND

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff and Class Members hereby demand trial by jury.

Dated: January 8, 2017

PACIFIC TRIAL ATTORNEYS, APC

By: */s/ Scott J. Ferrell*
Scott. J. Ferrell
Attorneys for Plaintiff and the Class

EXHIBIT 1

DMA

Advancing and Protecting Responsible Data-Driven Marketing

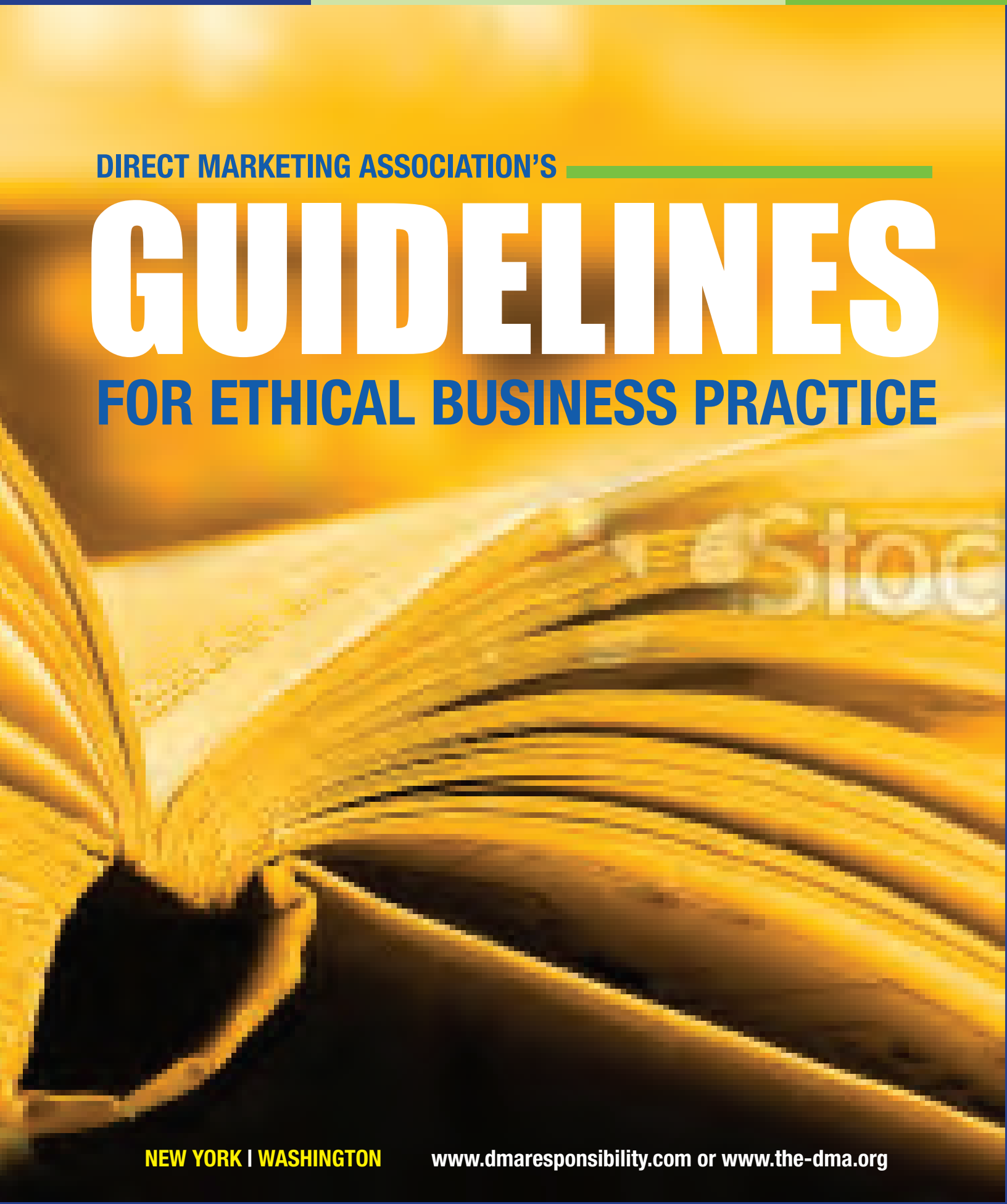
ETHICS

Revised May 2011

DIRECT MARKETING ASSOCIATION'S

GUIDELINES

FOR ETHICAL BUSINESS PRACTICE



NEW YORK | WASHINGTON

www.dmaresponsibility.com or www.the-dma.org

Direct Marketing Association Guidelines for Ethical Business Practice

The Direct Marketing Association's Guidelines for Ethical Business Practice are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct. These guidelines reflect DMA's long-standing policy of high levels of ethics and the responsibility of the Association, its members, and all marketers to maintain consumer and community relationships that are based on fair and ethical principles. In addition to providing general guidance to the industry, the Guidelines for Ethical Business Practice are used by DMA's Committee on Ethical Business Practice, an industry peer review committee, as the standard to which direct marketing promotions that are the subject of complaint to DMA are compared.

These self-regulatory guidelines are intended to be honored in light of their aims and principles. All marketers should support the guidelines in spirit and not treat their provisions as obstacles to be circumvented by legal ingenuity.

These guidelines also represent DMA's general philosophy that self-regulatory measures are preferable to governmental mandates. Self-regulatory actions are more readily adaptable to changing techniques and economic and social conditions. They encourage widespread use of sound business practices.

Because dishonest, misleading or offensive communications discredit all means of advertising and marketing, including direct marketing, observance of these guidelines by all concerned is expected. All persons involved in direct marketing should take reasonable steps to encourage other industry members to follow these guidelines as well.

Revised May 2011

DMA Member Principles

DMA Member Principles are the underlying framework for the Guidelines for Ethical Business Practice as detailed herein, and for Guidelines that will be drafted in the future. These Principles apply to DMA members' relationships with current and prospective customers, donors, and members, and are the grounding for all DMA members, which includes those who market directly not only to consumers, but also to businesses, government agencies, and "SOHO" (small-office/home-office) entities. The Principles provide a general statement to the public of the expectations they can have when dealing with DMA members.

A DMA Member:

1. Is committed to customer satisfaction, good corporate citizenship, and responsible environmental, community and financial stewardship
2. Clearly, honestly, and accurately represents its products, services, terms and conditions
3. Delivers its products and services as represented
4. Communicates in a respectful and courteous manner
5. Responds to inquiries and complaints in a constructive, timely way
6. Maintains appropriate security policies and practices to safeguard information
7. Provides information on its policies about the transfer of personally identifiable information for marketing purposes
8. Honors requests not to have personally identifiable information transferred for marketing purposes
9. Honors requests not to receive future solicitations from its organization
10. Follows the spirit and letter of the law as well as DMA's Guidelines for Ethical Business Practice

Table of Contents

The Terms of the Offer

HONESTY AND CLARITY OF OFFER

Article #1

All offers should be clear, honest, and complete so that the consumer may know the exact nature of what is being offered, the price, the terms of payment (including all extra charges) and the commitment involved in the placing of an order. Before publication of an offer, marketers should be prepared to substantiate any claims or offers made. Advertisements or specific claims that are untrue, misleading, deceptive, or fraudulent should not be used.

ACCURACY AND CONSISTENCY

Article #2

Simple and consistent statements or representations of all the essential points of the offer should appear in the promotional material. The overall impression of an offer should not be contradicted by individual statements, representations, or disclaimers.

CLARITY OF REPRESENTATIONS

Article #3

Representations which, by their size, placement, duration, or other characteristics are unlikely to be noticed or are difficult to understand should not be used if they are material to the offer.

ACTUAL CONDITIONS

Article #4

All descriptions, promises, and claims of limitation should be in accordance with actual conditions, situations, and circumstances existing at the time of the promotion.

DISPARAGEMENT

Article #5

Disparagement of any person or group on grounds addressed by federal or state laws that prohibit discrimination is unacceptable.

DECENCY

Article #6

Solicitations should not be sent to consumers who have indicated to the marketer that they consider those solicitations to be vulgar, immoral, profane, pornographic, or offensive in any way and who do not want to receive them.

PHOTOGRAPHS AND ART WORK

Article #7

Photographs, illustrations, artwork, and the situations they describe should be accurate portrayals and current reproductions of the products, services, or other subjects they represent.

DISCLOSURE OF SPONSOR AND INTENT

Article #8

All marketing contacts should disclose the name of the sponsor and each purpose of the contact. No one should make offers or solicitations in the guise of one purpose when the intent is a different purpose regardless of the marketing channel used.

ACCESSIBILITY

Article #9

Every offer should clearly identify the marketer's name and street address or telephone number, or both, at which the individual may obtain service and exercise their marketing preferences. If an offer is made online, the marketer should provide its name, an Internet-based contact mechanism, and a street address. For e-mail solicitations, marketers should comply with Article #40 (Commercial Solicitations Online). For mobile marketing solicitations, marketers should comply with Articles #54-56 to provide adequate notice to consumers to allow them to exercise their marketing preferences.

SOLICITATION IN THE GUISE OF AN INVOICE OR GOVERNMENTAL NOTIFICATION

Article #10

Offers that are likely to be mistaken for bills, invoices, or notices from public utilities or governmental agencies should not be used.

POSTAGE, SHIPPING, OR HANDLING CHARGES

Article #11

Postage, shipping, or handling charges, if any, should bear a reasonable relationship to actual costs incurred.

ADVANCE CONSENT/NEGATIVE OPTION MARKETING

Article #12

These guidelines apply to all media and address marketing plans where the consumer gives consent to receive and pay for goods or services in the future on a continuing or periodic basis, unless and until the consumer cancels the plan.

The following should apply to all advance consent or negative option marketing plans:

1. Initial Offer:

   CONSENT:
   Regardless of channel, marketers should have the consumer's express informed consent to participate in any advance consent or negative option marketing plan before the consumer is billed or charged. For example, a pre-checked box without further action, such as clicking a response button or sending back a response to confirm individual consent is not sufficient. In telephone sales where the consumer agrees to the offer in a way other than by credit or debit card payment, the consumer consent must be written or audio recorded.

   - Marketers should inform consumers in the initial offer of their right to cancel their participation in the plan
   - and any outstanding fees that may be owed.
   - Marketers should inform consumers in the initial offer of the length of any trial period, including a
   - statement that the consumer's account will be charged after the trial period (including the date of the charge) unless the consumer takes an affirmative step to cancel, providing the consumer a reasonable time period to cancel, and the steps needed to avoid charges.

MATERIAL TERMS & CONDITIONS:

Regardless of channel, marketers should clearly and conspicuously disclose all material terms and conditions before obtaining the consumer's billing information, including:

- A description of the goods or services being offered
- The identity of the marketer and contact information for service or cancellation
- The interval between shipments or services to be provided
- The price or the range of prices of the goods or services purchased by the consumer, including whether there are any additional charges should be disclosed
- Whether the consumer will be billed or automatically charged
- When and how frequently the consumer will be billed or charged
- Any terms with regards to a "free to keep" incentive as applicable
- The fact that the consumer must take affirmative action to cancel in order to avoid future billing or charges
- The specific and easy steps that consumers should follow to cancel the plan and to stop recurring charges from being placed on the consumer's account, and
- The time period within which the consumer must cancel.

When applicable, the following terms and conditions should also be clearly and conspicuously disclosed in the initial offer:

- That the current plan or renewal prices of the goods or services are subject to change
- The length of any free, trial or approval period in time or quantity
- The length of membership period, and the length of subsequent renewal or billing periods
- The fact that goods or services will continue after the free period unless the consumer cancels
- Any minimum purchase obligations, and
- The terms and conditions of any refund policy

In instances where the marketer uses pre-acquired account information under a free-to-pay conversion plan, the marketer should:

- Obtain from the consumer the complete account number to be charged within the appropriate data security protocols (such as PCI compliance)
- Obtain affirmative consent from the consumer to charge such account, and
- Provide channel specific proof (an email or hard copy confirmation, or if via telephone, audio record the entire transaction.)

In instances where the marketer uses pre-acquired account information but does not engage in a free-to-pay conversion plan, the marketer should:

- Identify with specificity the account that will be charged, and
- Obtain affirmative consent from the consumer to charge such account

2. Providing the Goods & Services to the Consumer:
   - Marketers may provide products or services and bills concurrently; however, consumers should not be obligated to pay bills prior to the expiration of any trial period.
   - Marketers should inform consumers in renewal reminders of their right to cancel their participation in the plan, and any outstanding fees owed.
   - Marketers should provide renewal reminders at the frequency specified in the initial offer.

3. Cancellation:
   - Marketers should promptly honor requests for refunds due upon consumers' cancellation of the plan.
   - Marketers should allow consumers a reasonable length of time between receipt of renewal reminders and the renewal date, after which consumers can cancel the plan.
   - Marketers should honor the time period they provided for a cancellation and should honor a cancellation after the expiration of the trial period.

4. For Internet Sales:
   The initial merchant must never disclose a credit card, debit card or other financial account number or other billing information that is used to charge the customer of the initial merchant to any post-transaction third party seller for use in an Internet-based sale of any goods or services from that post-transaction third party seller.

Post Transaction Third Party Sales:

For post-transaction third party sellers:
No charges should apply to a consumer's account before obtaining the consumer's billing information as follows:

The third party seller has first clearly and conspicuously disclosed to the purchaser a description of the goods and services being offered and all material terms of the offer including:
- The fact that the third party seller is not affiliated with the initial merchant;
- The costs of such goods or services;
- And the consumer has provided express informed consent for the charges by providing the complete account information to be charged, providing the consumer's name and address and a means to contact the consumer, and providing confirmation such as clicking a confirmation button or otherwise demonstrating consent to the charges.

All marketing partners or service providers should comply with these guidelines.

Marketing to Children

MARKETING TO CHILDREN

Article #13

Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online, via wireless devices such as a mobile phone or in any other medium, marketers should predetermine whether the use of the child's data for marketing purposes or the sending of marketing material to the child is permitted under federal law, such as the Children's Online Privacy Protection Act (COPPA), or state law. Where marketing to children is permitted by law, marketers should ensure the marketing is suitable for the child taking into account the age range, knowledge, sophistication, and maturity of their intended audience.

PARENTAL RESPONSIBILITY AND CHOICE

Article #14

Marketers should provide notice and an opportunity to opt out of the marketing process so that parents have the ability to limit the collection, use, and disclosure of their children's names, addresses, or other personally identifiable information.

INFORMATION FROM OR ABOUT CHILDREN

Article #15

Marketers should take into account the age range, knowledge, sophistication, and maturity of children when collecting information from them. Marketers should limit the collection, use, and dissemination of information collected from or about children to information required for the promotion, sale, and delivery of goods and services, provision of customer services, conducting market research, and engaging in other appropriate marketing activities.

Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected.

Upon request from a parent, marketers should promptly provide the source and general nature of information maintained about a child. Marketers should implement strict security measures to ensure against unauthorized access, alteration, or dissemination of the data collected from or about children, and should provide information regarding such measures upon request to the parent or guardian of the minor.

MARKETING ONLINE TO CHILDREN UNDER 13 YEARS OF AGE

Article #16

Marketers should not knowingly collect personally identifiable information online or via wireless handsets or devices from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of such information, and shall provide an opportunity for the parent to prevent such use and participation in the activity. Online and wireless/mobile contact information should only be used to directly respond to an activity initiated by a child and not to recontact a child for other purposes without prior parental consent. However, a marketer may contact and get information from a child for the purpose of obtaining parental consent.

Marketers should not knowingly collect, without prior parental consent, personally identifiable information online or via a wireless handset or device from children that would permit any offline contact with the child.

Marketers should not knowingly distribute to third parties, without prior parental consent, information collected from a child that would permit any contact with that child.

Marketers should take reasonable steps to prevent the online publication or posting of information that would allow a third party to contact a child offline unless the marketer has prior parental consent.

Marketers should not entice a child to divulge personally identifiable information by the prospect of a special game, prize, or other offer.

Marketers should not make a child's access to website or mobile content contingent on the collection of personally identifiable information. Only online contact information used to enhance the interactivity of the site is permitted.

The following assumptions underlie these online guidelines:

- When a marketer directs a site at a certain age group, it can expect that the visitors to that site are in that age range, and
- When a marketer asks the age of the child, the marketer can assume the answer to be truthful.

Special Offers and Claims

USE OF THE WORD "FREE" AND OTHER SIMILAR REPRESENTATIONS

Article #17

A product or service that is offered without cost or obligation to the recipient may be unqualifiedly described as "free."

If a product or service is offered as "free," all qualifications and conditions should be clearly and conspicuously disclosed, in close conjunction with the use of the term "free" or other similar phrase. When the term "free" or other similar representations are made (for example, 2-for-1, half-price, or 1-cent offers), the product or service required to be purchased should not have been increased in price or decreased in quality or quantity.

PRICE COMPARISONS

Article #18

Price comparisons, including those between a marketer's current price and a former, future, or suggested price, or between a marketer's price and the price of a competitor's comparable product, should be fair and accurate.

In each case of comparison to a former, manufacturer's suggested, or competitor's comparable product price, recent substantial sales should have been made at that price in the same trade area.

For comparisons with a future price, there should be a reasonable expectation that the new price will be charged in the foreseeable future.

GUARANTEES

Article #19

If a product or service is offered with a guarantee or a warranty, either the terms and conditions should be set forth in full in the promotion, or the promotion should state how the consumer may obtain a copy. The guarantee should clearly state the name and address of the guarantor and the duration of the guarantee.

Any requests for repair, replacement, or refund under the terms of a guarantee or warranty should be honored promptly. In an unqualified offer of refund, repair, or replacement, the customer's preference should prevail.

USE OF TEST OR SURVEY DATA

Article #20

All test or survey data referred to in advertising should be valid and reliable as to source and methodology, and should support the specific claim for which it is cited. Advertising claims should not distort test or survey results or take them out of context.

TESTIMONIALS AND ENDORSEMENTS

Article #21

Testimonials and endorsements in any media (including but not limited to such comments on a company's website and via social networking sites, online message boards, blogging and "word-of-mouth" marketing) should be used only if they:

a. Are authorized by the person quoted;
b. Are accurate, genuine and related to the experience of the person giving them, both at the time made and at the time of the promotion, and disclose the expertise of the endorser in terms of whether he or she is an expert for the purposes of the advertisement or simply a consumer endorser;
c. Are not taken out of context so as to distort the endorser's opinion or experience with the product or service;
d. Clearly and conspicuously disclose any material connections between the endorser and marketer, which the consumer would not expect. A material connection refers to a connection between the endorser and marketer that materially affects the weight or credibility of the endorsement, such as payments or free products, or an employer/employee relationship; and
e. Clearly and conspicuously disclose the generally expected, or typical, results/performance of the advertised products or services, if the claims made are not typical of what a user could expect under normal circumstances.

A marketer should be able to provide prior and adequate substantiation, including providing reliable scientific evidence, as necessary, for any claims of efficacy (i.e. whether the product/service will actually do what the marketer says it will do, typicality (i.e. whether the typical consumer will have an experience like that of the endorser), and environmental benefit. The marketer should also be able to substantiate that the endorser was a bona fide user of the product at the time of the endorsement.

Additionally, marketers should ensure that their celebrity endorsers disclose their relationships with marketers when making endorsements outside the context of traditional advertisements, such as on talk shows or in social media, and they should not knowingly make statements that are false or unsubstantiated.

For purposes of this article, the terms "testimonial" and "endorsement" refer to an advertising or marketing message made in any channel that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsor of the message, even if the views expressed by that party are identical to those of the sponsor. Testimonials and endorsements can be verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization.

Sweepstakes

USE OF THE TERM "SWEEPSTAKES"

Article #22

Sweepstakes are promotional devices by which items of value (prizes) are awarded to participants by chance without the promoter's requiring the participants to render something of value (consideration) to be eligible to participate. The co-existence of all three elements -- prize, chance and consideration -- in the same promotion constitutes a lottery. It is illegal for any private enterprise to run a lottery without specific governmental authorization.

When skill replaces chance, the promotion becomes a skill contest. When gifts (premiums or other items of value) are given to all participants independent of the element of chance, the promotion is not a sweepstakes. Promotions that are not sweepstakes should not be held out as such.

Only those promotional devices that satisfy the definition stated above should be called or held out to be a sweepstakes.

NO PURCHASE OPTION

Article #23

Promotions should clearly state that no purchase is required to win sweepstakes prizes. They should not represent that those who make a purchase or otherwise render consideration with their entry will have a better chance of winning or will be eligible to win more or larger prizes than those who do not make a purchase or otherwise render consideration. The method for entering without ordering should be easy to find, read, and understand. When response devices used only for entering the sweepstakes are provided, they should be as easy to find as those utilized for ordering the product or service.

CHANCES OF WINNING

Article #24

No sweepstakes promotion, or any of its parts, should represent that a recipient or entrant has won a prize or that any entry stands a greater chance of winning a prize than any other entry when this is not the case. Winners should be selected in a manner that ensures fair application of the laws of chance.

PRIZES

Article #25

Sweepstakes prizes should be advertised in a manner that is clear, honest, and complete so that the consumer may know the exact nature of what is being offered. For prizes paid over time, the annual payment schedule and number of years should be clearly disclosed.

Photographs, illustrations, artwork, and the situations they represent should be accurate portrayals of the prizes listed in the promotion.

No award or prize should be held forth directly or by implication as having substantial monetary value if it is of nominal worth. The value of a non-cash prize should be stated at regular retail value, whether actual cost to the sponsor is greater or less.

All prizes should be awarded and delivered without cost to the participant. If there are certain conditions under which a prize or prizes will not be awarded, that fact should be disclosed in a manner that is easy to find, read, and understand.

PREMIUMS

Article #26

Premiums should be advertised in a manner that is clear, honest, and complete so that the consumer may know the exact nature of what is being offered.

A premium, gift or item should not be called or held out to be a "prize" if it is offered to every recipient of or participant in a promotion. If all participants will receive a premium, gift, or item, that fact should be clearly disclosed.

DISCLOSURE OF RULES

Article #27

All terms and conditions of the sweepstakes, including entry procedures and rules, should be easy to find, read, and understand. Disclosures set out in the rules section concerning no purchase option, prizes, and chances of winning should not contradict the overall impression created by the promotion.

The following should be set forth clearly in the rules:

- No purchase of the advertised product or service is required in order to win a prize
- A purchase will not improve the chances of winning
- Procedures for entry
- If applicable, disclosure that a facsimile of the entry blank or other alternate means (such as a 3"x 5" card) may be used to enter the sweepstakes
- The termination date for eligibility in the sweepstakes. The termination date should specify whether it is a date of mailing or receipt of entry deadline
- The number, retail value (of non-cash prizes), and complete description of all prizes offered, and whether cash may be awarded instead of merchandise. If a cash prize is to be awarded by installment payments, that fact should be clearly disclosed, along with the nature and timing of the payments
- The estimated odds of winning each prize. If the odds depend upon the number of entries, the stated odds should be based on an estimate of the number of entries
- The method by which winners will be selected
- The geographic area covered by the sweepstakes and those areas in which the offer is void
- All eligibility requirements, if any
- Approximate dates when winners will be selected and notified
- Publicity rights regarding the use of winner's name
- Taxes are the responsibility of the winner
- Provision of a mailing address to allow consumers to receive a list of winners of prizes over $25.00 in value

Fulfillment

UNORDERED MERCHANDISE OR SERVICE

Article #28

Merchandise or services should not be provided without having first received the customer's permission. The exceptions are samples or gifts clearly marked as such, and merchandise mailed by a charitable organization soliciting contributions, as long as all items are sent with a clear and conspicuous statement informing the recipient of an unqualified right to treat the product as a gift and to do with it as the recipient sees fit, at no cost or obligation to the recipient.

PRODUCT AVAILABILITY AND SHIPMENT

Article #29

Direct marketers should offer merchandise only when it is on hand or when there is a reasonable expectation of its timely receipt.

Direct marketers should ship all orders according to the terms of the offer or within 30 days where there is no promised shipping date, unless otherwise directed by the consumer, and should promptly notify consumers of any delays.

DRY TESTING

Article #30

Direct marketers should engage in dry testing only when the special nature of the offer is made clear in the promotion.

Collection, Use, and Maintenance of Marketing Data

For purposes of the *Guidelines for Ethical Business Practice*, the following definitions are used:

Consumer refers to the subject of the data.

Marketing data means actual or inferred information consistent with a person's commercial or charitable inquiry or transaction, or market research or market survey information. Such information can be derived from either a direct contact or marketing partnership when linked to a person's name, postal or e-mail address, or telephone number, or any other personally identifiable information. When obtained from a publicly available source, information (including public record information), not combined with other information, is not marketing data.

Marketing purpose means any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to allow or induce consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers.

PROVIDING CONSUMER CHOICE & THE COLLECTION, USE, AND TRANSFER OF PERSONALLY IDENTIFIABLE DATA

Article #31
This article is applicable to all addressable media and applies to senders of marketing offers or fundraising solicitations:

A. Providing Consumer Choice and Privacy Notice Information:

- Marketers should provide consumers a point of contact where they may add, modify or eliminate direct marketing communications from a company or an organization and obtain the company or organization's privacy policy with regards to collection, use and transfer of their information. The point of contact information (such as a website, telephone number or address) should appear upon or within each written marketing offer, or upon request by the consumer.

- Online marketers should provide notice in accordance with Article #38.

- Email marketers should provide notice in accordance with Article #39 and the CAN-SPAM Act.
- Mobile marketers must obtain prior express consent and provide a notice in accordance with Articles #54 and #55.)
- The point of contact notice should: be easy for the consumer to find, read, understand, and act upon.
- A marketer periodically should provide existing customers with notice of its policy concerning the rental, sale, exchange, or transfer of data about them and of the opportunity to opt out of the marketing process. All such opt-out requests should be honored promptly.
- An in-house suppression request from a consumer should be interpreted as meaning that the consumer also wants to opt out of the transfer of his or her personal information
- Upon request by a consumer, a marketer should disclose the source from which it obtained personally identifiable information about that consumer.

B. Processing Consumer Choices:

- A consumer's request for elimination of future marketing offers should be processed:
  - within 30 days of the consumer's request or as required by law, whichever is the shorter time period
  - for a period of at least three years from the date of receipt of the request

- Where an affiliate, division, or subsidiary markets under a different company or brand name, and is perceived as separate by the consumer, each corporate entity or brand should separately honor requests received by it.

- A marketer should establish internal policies and practices that assure accountability for honoring consumer preference requests regardless of the marketing channel, in compliance with this guideline, and at no cost to consumers. Should those policies substantially change, the marketer has an obligation to inform consumers of that change prior to the rental, sale, exchange, or transfer of data, and to offer consumers an opportunity to opt out of the marketing process at that time.

C. DMAchoice and Related Consumer Choice Files:

- For each prospecting list that is rented, sold, exchanged, or transferred, the names registered on the applicable DMAchoice (DMA's consumer choice web site) name-removal lists should be removed prior to use.

- DMAchoice name-removal lists include:
  - the relevant categorical opt-out mailing lists for Catalog, Magazine, Pre-screened Credit Offers or Other categories, as well as future categories designated by the DMA; and
  - the eMail Preference Service and Telephone Preference Service, as well as future DMA preference service lists.

- The use of the DMAchoice name-removal lists and preference service lists is not required for the company's and organization's existing customer or donor lists, only for prospects.

- Members should be listed on the DMAchoice site to demonstrate their compliance with the DMA Guidelines and to provide a direct connection to consumers for further choice requests.

  - The company or organization listed must provide the correct point of contact where the consumer may exercise their marketing preferences. (See Also Article #9 Accessibility: Every offer should clearly identify the marketer's name and street address or telephone number, or both, at which the individual may obtain service and exercise their marketing preferences.)

In all instances, the most recent monthly release of the relevant DMAchoice file should be used.

In addition to adhering to these guidelines, a marketer should cooperate with DMA when requested in demonstrating its compliance with the Commitment to Consumer Choice and the marketer's own consumer preference policies.

PERSONAL DATA

Article #32

Marketers should be sensitive to the issue of consumer privacy and should only collect, combine, rent, sell, exchange, or use marketing data. Marketing data should be used only for marketing purposes.

Data and selection criteria that by reasonable standards may be considered sensitive and/or intimate should not be disclosed, be displayed, or provide the basis for lists made available for rental, sale or exchange when there is a reasonable expectation by the consumer that the information will be kept confidential.

Credit card numbers, checking account numbers, and debit account numbers are considered to be personal information and therefore should not be transferred, rented, sold, or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.

Social Security numbers are also considered to be personal information and therefore should not be transferred, rented, sold, or exchanged for use by a third party when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of Social Security numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers. Social Security numbers, however, are used by direct marketers as part of the process of extending credit to consumers or for matching or verification purposes.

COLLECTION, USE, AND TRANSFER OF HEALTH-RELATED DATA

Article #33

Health-related data constitute information related to consumers':

- Illnesses or conditions
- Treatments for those illnesses or conditions, such as prescription drugs, medical procedures, devices or supplies or
- Treatments received from doctors (or other health care providers), at hospitals, at clinics, or at other medical treatment facilities

These fair information practices and principles apply to any individual or entity that collects, maintains, uses, and/or transfers health-related data for marketing purposes, whether or not marketing is a primary purpose. These principles are applicable to nonprofit as well as for-profit entities.

1. Personally identifiable health-related data gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities should not be transferred for marketing purposes without the specific prior consent of those consumers. Health or medical care providers include licensed health care practitioners, such as doctors, nurses, psychologists, pharmacists, and counselors, and those who support health care providers and therefore have access to personally identifiable information, such as insurance companies, pharmacy benefits managers or other business partners, and businesses that sell prescription drugs.

2. Personally identifiable health-related data, including the occurrence of childbirth, gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities (as defined in #1) should not be used to contact those consumers for marketing purposes without giving consumers a clear notice of the marketer's intended uses of the data and the opportunity to request not to be so contacted.

3. Personally identifiable health-related data volunteered by consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. Such data should not be collected, maintained, used, and/or transferred for marketing purposes unless those consumers receive, at the time the data are collected, a clear notice of the marketer's intended uses of the data, whether the marketer will transfer the data to third parties for further use, the name of the collecting organization, and the opportunity to opt out of transfer of the data. Such data include, but are not limited to, data volunteered by consumers when responding to surveys and questionnaires. Clear notice should be easy to find, read, and understand.

4. Personally identifiable health-related data inferred about consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. These are data based on consumers' purchasing behavior. Such data include, but are not limited to, data captured by inquiries, donations, purchases, frequent shopper programs, advertised toll-free telephone numbers, or other consumer response devices. Any entity, including a seller of over-the-counter drugs, which uses inferred health-related data should promptly provide notice and the opportunity to opt out of any transfer of the data for marketing purposes.

5. Marketers using personally identifiable health-related data should provide both the source and the nature of the information they have about that consumer, upon request of that consumer and receipt of that consumer's proper identification.

6. Consumers should not be required to release personally identifiable health-related information about themselves to be used for marketing purposes as a condition of receiving insurance coverage, treatment or information, or otherwise completing their health care-related transaction.

7. The text, appearance, and nature of solicitations directed to consumers on the basis of health-related data should take into account the sensitive nature of such data.

8. Marketers should ensure that safeguards are built into their systems to protect personally identifiable health-related data from unauthorized access, alteration, abuse, theft, or misappropriation. Employees who have access to personally identifiable health-related data should agree in advance to use those data only in an authorized manner.

9. If personally identifiable health-related data are transferred from one direct marketer to another for a marketing purpose, the transferor should arrange strict security measures to assure that unauthorized access to the data is not likely during the transfer process. Transfers of personally identifiable health-related data should not be permitted for any marketing uses that are in violation of any of DMA's *Guidelines for Ethical Business Practice*.

Nothing in these guidelines is meant to prohibit research, marketing, or other uses of health-related data which are not personally identifiable, and which are used in the aggregate.

PROMOTION OF MARKETING LISTS

Article #34

Any advertising or promotion for marketing lists being offered for rental, sale, or exchange should reflect the fact that a marketing list is an aggregate collection of marketing data. Such promotions should also reflect a sensitivity for the consumers on those lists.

MARKETING LIST USAGE

Article #35

List owners, brokers, managers, and users of marketing lists should ascertain the nature of the list's intended usage for each materially different marketing use prior to rental, sale, exchange, transfer, or use of the list. List owners, brokers, and managers should not permit the rental, sale, exchange, or transfer of their marketing lists, nor should users use any marketing lists for an offer that is in violation of these guidelines. Mobile opt-in lists should not be rented or exchanged for the purpose of sending mobile marketing solicitations to those on the list, without obtaining prior express consent from those on the list.

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.

INFORMATION SECURITY

Article #37

The protection of personally identifiable information is the responsibility of all marketers. Therefore, marketing companies should assume the following responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data:

- Marketers should establish information security policies and practices that assure the uninterrupted security of information systems.
- Marketers should create and implement staff policies, procedures, training, and responsiveness measures to protect personally identifiable information handled in the everyday performance of duties.
- Marketers should employ and routinely reassess protective physical safeguards and technological measures, including data retention, destruction, and deletion practices, in support of information security.
- Marketers should contractually require all business partners and service providers that handle personally identifiable information to ensure that their policies, procedures, and practices maintain a level of security consistent with the marketer's applicable information security policies.
- Marketers should, in the event of a security breach where there is a reasonable likelihood of material harm to consumers, inform those consumers who may be affected as soon as reasonably practical, unless requested by legal authorities to delay such notification.

Digital Marketing

ONLINE INFORMATION & ONLINE BEHAVIORAL ADVERTISING

Article #38

This Article addresses the collection of personally identifiable information by websites for online marketing and the collection and use of information for online behavioral advertising purposes, as defined in the Glossary of Terms.

General Notice to Online Visitors

If your organization operates an online site and/or is engaged in online behavioral advertising, you should make your information practices available to visitors in a prominent place on your website's home page or in a place on your website that is easily accessible from the home page. The notice about information practices on your website should be easy to find, read, and understand. Visitors should be able to comprehend the scope of the notice and how they can exercise their choices regarding use of personally identifiable information or information used for online behavioral advertising purposes. The notice should be available prior to or at the time personally identifiable information or information used for online behavioral advertising purposes is collected.

Your organization and its postal address, and the website(s) to which the notice applies, should be identified so visitors know who is responsible for the website. You also should provide specific contact information so visitors can contact your organization for service or information.

If your organization collects personally identifiable information from visitors and/or collects information from non-affiliate websites for online behavioral advertising purposes, your notice should include:

- The nature of the information collected online for marketing purposes, and the types of uses you make of such information, including uses for online behavioral advertising purposes;
- The use(s) of such information, including whether you transfer information to third parties for use by them for their own marketing or online behavioral advertising purposes and the mechanism by which consumers can exercise choice not to have such information transferred;
- Whether personally identifiable information is collected by, used by, or transferred to agents (entities working on your behalf) as part of the business activities related to the visitor's actions on the site, including to fulfill orders or to provide information or requested services;
- Whether you use cookies or other passive means of information collection, and whether such information collected is for internal purposes or transferred to third parties for marketing purposes, including online behavioral advertising purposes;
- What procedures your organization has put in place for accountability and enforcement purposes; and
- That your organization maintains appropriate physical, electronic, and administrative safeguards to protect information collected online.

In addition, marketers should refer to Article #32 (Personal Data) specifically to assure that marketing data are used only for marketing purposes.

Third-Party Notice for Online Behavioral Advertising
When information is collected from or used on a website for online behavioral advertising purposes, visitors should be provided with notice (easy to find, read and understand) about the third party's policies for online behavioral advertising. Third parties, as defined in the Glossary of Terms, should provide notice in one of the following ways:

- through a clear, meaningful, and prominent link described in or proximate to the advertisement delivered on the Web page where information is collected;
- on DMA's approved website(s), such as DMAchoice.org or another comprehensive industry-developed website(s), that is linked from the disclosure that describes the fact that information is being collected for online behavioral advertising purposes;
- on the web page where the information is collected if there is an arrangement with the website operator for the provision of such notice;
- if agreed to by the operator of the website(s) on its web page disclosing notice and choice regarding information collected for online behavioral advertising purposes.

Consumer Choice for Third-Party Online Behavioral Advertising
A third party should provide consumers with the ability to exercise choice with respect to the collection and use of information for online behavioral advertising purposes or the transfer of such information to a non-affiliate for such purposes. Such choice should be available through the notice options as detailed above.

Material Changes to Existing Policies
If your organization's policy changes materially with respect to the sharing of personally identifiable information with third parties including but not limited to changes for online behavioral advertising purposes, you should update your policy and give consumers conspicuous notice to that effect, offering an opportunity for individuals to select their preferences. Prior to making a materially different use of information collected from an individual for online behavioral advertising purposes, and before notice of your organization's policy change is given, organizations should obtain informed consent to such a new marketing use from the consumer.

Honoring Choice
You should honor a website visitor's choice regarding use and transfer of personally identifiable information made in accordance with your stated policy. If you have promised to honor the visitor's choice for a specific time period, and if that time period subsequently expires, then you should provide that visitor with a new notice and choice. You should provide choices online. You may also offer choice options by mail or telephone.

Providing Access
You should honor any representations made in your online policy notice regarding access.

Information Security
Your organization should maintain appropriate physical, technical and administrative safeguards and use appropriate security technologies and methods to protect information collected or used online, and to guard against unauthorized access, alteration, or dissemination of personally identifiable information during transfer and storage. Your procedures should require that employees and agents of your organization who have access to personally identifiable information use and disclose that information only in a lawful and authorized manner. Organizations should retain information that is collected and used for online behavioral advertising purposes only for as long as necessary to fulfill a legitimate business need, or as required by law.

Visitors Under 13 Years of Age

If your organization has a site directed to children under the age of 13 or collects personally identifiable information from visitors known to be under 13 years of age, your website should take the additional steps required by the Marketing to Children Articles of the Guidelines for Ethical Business Practice and inform visitors that your disclosures and practices are subject to compliance with the Children's Online Privacy Protection Act ("COPPA"). In addition, an organization should not engage in online behavioral advertising directed to children where it has actual knowledge that the children are under the age of 13, unless compliant with COPPA and these Guidelines.

Health and Financial Information

Entities should not collect and use financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for online behavioral advertising purposes without prior express consent and unless compliant with the Health Insurance Portability & Accountability Act ("HIPPA") and these Guidelines.

Accountability

There should be a meaningful, timely, and effective procedure through which your organization can demonstrate adherence to your stated online information practices. Such a procedure may include: (1) self or third-party verification and monitoring, (2) complaint resolution, and (3) education and outreach. This can be accomplished by an independent auditor, public self-certification, a third-party privacy seal program, a licensing program, and/or membership in a trade, professional or other membership association with a self-regulatory program.

Service Provider Treatment of Online Behavioral Advertising Information

A service provider, as defined in the Glossary of Terms, should not collect and use information for online behavioral advertising purposes without consent and should provide an easy-to-use ongoing means to withdraw consent to the collection and use of that information for online behavioral advertising purposes.

In addition, a service provider should take the following steps regarding information collected and used for online behavioral advertising purposes:

1. Alter, anonymize, or randomize (e.g., through "hashing" or substantial redaction) any personally identifiable information or unique identifier in order to prevent the information from being reconstructed into its original form in the ordinary course of business.

2. Disclose in the notice described above the circumstances in which information is collected and used for online behavioral advertising purposes.

3. Take reasonable steps to protect the non-identifiable nature of information if and when it is distributed to non-affiliates, including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the information, and obtaining satisfactory written assurance that such non-affiliates will not attempt to re-construct the information and will use or disclose the anonymized information only for purposes of online behavioral advertising or other uses as specified to users. This assurance will be considered satisfied if a non-affiliate does not have any independent right to use the information for its own purposes under a written contract.
4. Take reasonable steps to ensure that any non-affiliate that receives anonymized information will itself ensure that any other non-affiliate to which such information is disclosed agrees to the restrictions and conditions set forth in this subsection. This obligation is also considered satisfied if a non-affiliate does not have any independent right to use the data for its own purposes under a written contract.

Glossary of Terms

Ad Delivery – means the delivery of online advertisements or advertising-related services using ad reporting data. Ad delivery does not include the collection and use of ad reporting data when such data are used to deliver advertisements to a computer or device based on the preferences or interests inferred from information collected over time and across non-affiliate sites because this type of collection and use is covered by the definition of online behavioral advertising.

Ad Reporting – refers to the logging of page views on a website(s) or the collection or use of other information about a browser, operating system, domain name, clickstream within a site, date and time of the viewing of the Web page or advertisement, and related information for purposes including but not limited to: statistical reporting in connection with the activity on a website(s); Web analytics and analysis for improved marketing and better site design; and logging the number and type of advertisements served on a particular website(s).

Affiliate – refers to an entity that controls, is controlled by, or is under common control with, another entity.

Consent – means an individual's action in response to a clear, meaningful and prominent notice regarding the collection and use of data for online behavioral advertising purposes. Informed consent is based on information provided to an individual that allows them to select their preferences, prior express consent means consent required from an individual prior to any marketing communication from the marketer or others.

Contextual Advertising – Advertising based on a consumer's current visit to a Web page or search query. Online behavioral advertising, as defined in this Article's Glossary of Terms, does not include contextual advertising.

Control – of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the control of another entity and thus be treated as a first party under these principles, the entity must adhere to online behavioral advertising policies that are not materially inconsistent with the other entity's policies.

First Party – is the entity that is the owner of the website, or those of its affiliates, and has control over the website with which the consumer interacts.

Online Behavioral Advertising – means the collection of information from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites for the purpose of using such information to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors. Online behavioral advertising does not include the activities of first parties, ad delivery or ad reporting, or contextual advertising (i.e. advertising based on the content of the Web page being visited, a consumer's current visit to a Web page, or a search query). The activities of search engines fall within the scope of online behavioral advertising to the extent that they include collection of data regarding Web viewing behaviors over time and across non-affiliate websites in order to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.

Personally Identifiable Information & Non-Personally Identifiable Information – for purposes of this Article, personally identifiable information refers to name, address, or other information that identifies a specific individual; non-personally identifiable information (non-PII) refers to information, such as a computer's IP address, that does not

tie the information to a specific individual. Non-personally identifiable information collected by third parties from websites for online behavioral advertising should be combined with personally identifiable information collected about an individual for marketing purposes only with that individual's consent, unless the individual was provided with notice and choice with respect to such potential combination at the time the non-personally identifiable information was collected and did not opt out.

Service Provider – refers to an organization that collects and uses information from all or substantially all URLs traversed by a Web browser across websites for purposes of online behavioral advertising. Examples of service providers in this context are internet access service providers and providers of desktop applications software such as Web browser "tool bars."

Third Party – an entity is a third party to the extent that it engages in online behavioral advertising on a non-affiliate's website.

MOBILE SERVICE COMMERCIAL MESSAGE SOLICITATIONS (MSCMs) DELIVERED TO A WIRELESS DEVICE

Article #39

A Mobile Service Commercial Message (MSCM) is a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of a commercial mobile service. Marketers sending MSCMs messages should obtain prior express consent from recipients and should abide by CAN-SPAM, the Federal Communications Commission's Wireless Email Rule, DMA Guidelines for Online & Mobile Marketing, and any additional federal and state regulations.

COMMERCIAL SOLICITATIONS ONLINE

Article #40

1. DEFINITION:
   This article refers to addressable commercial solicitations initiated online by marketers (or their affiliates); including commercial solicitations sent to an individual's email address or another "direct contact point." For purposes of this article, a "direct contact point" is defined as a user ID or other unique identifier at which an individual can be communicated with online or via a mobile Internet device. This may include, for example, a text message number, personalized activity feed identifier (e.g., "twitter" ID), or user ID for postings on or to a personal social network profile page.

   Nothing in this Article or definition is meant to restrict or prohibit the use of aggregated or anonymized data pertaining to direct contact points, the use of profile data for online behavioral advertising (OBA,) or online banner advertising.

2. CHANNEL APPROPRIATE CONSENT:
   Marketers (or their affiliates) may initiate commercial solicitations online to customers or prospects under the following circumstances
   - individuals have given their channel-appropriate consent to the marketer (including, but not limited to, through the terms of a social media platform) to receive solicitations online, or

- Individuals did not opt out after the marketer has given notice of the opportunity to opt out from receiving solicitations online, or
- The marketer has received assurance from the third party list provider that the individuals whose e-mail addresses or other direct contact points appear on that list:
  - have given their channel-appropriate consent to receive solicitations online, or
  - have already received notice of the opportunity to opt out from receiving online solicitations and have not opted out, and DMA's E-Mail Preference Service (E-MPS) suppression file was used by the third party.

3. CHANNEL APPROPRIATE CHOICE:
   Marketers should furnish individuals with the appropriate notice or a point of contact and an Internet-based mechanism individuals can use to:
   - Request that the marketer not send them future online solicitations and
   - Request that the marketer not rent, sell, or exchange their e-mail addresses or other direct contact point data for online solicitation purposes.

   If individuals request that they be added to the marketer's in-house suppression list, then the marketer may not rent, sell, or exchange their e-mail addresses or other direct contact point data 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 solicitation.

   Marketers that rent, sell, or exchange personally identifiable information need to provide individuals with notice of a mechanism to opt out of personally identifiable information transfer to third-party marketers.

   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.

E-MAIL AUTHENTICATION

Article #41

Marketers that use e-mail for communication and transaction purposes should adopt and use identification and authentication protocols.

USE OF SOFTWARE OR OTHER SIMILAR TECHNOLOGY INSTALLED ON A COMPUTER OR SIMILAR DEVICE

Article #42

Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (e.g., relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

* Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar
- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including Web beacons, are not governed by this Guideline. Article #38 provides guidance regarding cookies and other passive means of data collection.

SOCIAL MEDIA & ONLINE REFERRAL MARKETING

Article #43

1. DEFINITION

   Social media marketing is the use of online communities and/or social networks (via services, websites or platforms – each a "channel") to send a commercial marketing message to an individual and/or to that individual's own network. (Social media involves user interactions which the individual has agreed to display and to be shared.) Online referral marketing is a technique marketers use to generate new marketing leads.

   Typically, the online marketer encourages an individual to do the following:

   1. Forward a commercial solicitation to another individual, or
   2. Provide the marketer with personally identifiable information, such as name and/or address/email address, about the referred individual so the marketer may contact that person directly, or
   3. Share or display a social ad and/or otherwise engage with a social media network or channel by, for example, "friending" (an invitation to establish a social media relationship), posting or otherwise sharing or displaying the ad on or via a social media channel (e.g., an activity feed such as tweeting). This interaction may involve a request from the marketer that the individual provide profile or social data about himself/herself or others in his/her network. Profile data may include, but is not limited to: name, age, gender, location, expressed personal interests and preferences, and photos. Profile data also extends to what is known as the "social graph," which are explicit online connections and interactions between individuals ("friends").

2. USING INFORMATION PROVIDED BY THE INDIVIDUAL AND/OR ABOUT OTHERS

If personally identifiable information about an individual is given to a marketer through social media channels and/or online referral marketing rather than directly from an individual, then the following steps should be taken:

A marketer should not use personally identifiable information about a referred individual provided online by another individual unless:

- The marketer has previously disclosed, in a clear and conspicuous manner, to the referring individual the intended uses of the information (Note: All notices and disclosures referenced in this article should be made in clear and conspicuous manner and in keeping with DMA's Ethical Guidelines.);

- The marketer has disclosed to the referring individual that his or her own contact information will be provided to those individuals they have referred to the marketer;

- The marketer discloses to the referred person the fact that his or her contact information was obtained from another individual. The marketer should make the referring person's contact information available in the first communication to the prospect; and

- The marketer provides channel appropriate choices to the referred individual regarding receiving future communications. (Note: The frequency and type of choice provided (e.g., first communication vs. every communication) must be appropriate for the channel being used to contact the individual. For example, email communications must include an opt-out notice and choice in every communication.)

Since marketers have not had a direct contact with the referred individual, marketers should not contact referred individuals who are on their in-house suppression lists.

Marketers should not sell, rent, share, transfer, or exchange a referred e-mail address or referred personally identifiable information unless they receive prior permission from each referred person to do so.

Prior express consent must be obtained before initiating contact using a marketing channel or platform for which a referred individual will incur a fee for receipt of the marketing message, such as premium-rate text messaging via a mobile device. (Articles #54-#58.) In addition, online referral marketers offering an incentive should adhere to Article #39 (Mobile Service Commercial Messages).

4. SENDING COMMERCIAL SOLICITATIONS VIA INDIVIDUALS' SOCIAL MEDIA NETWORKS

If a marketer is contacting an individual to send marketing messages to that individual's network of contacts, each of the following steps should be taken:

- A marketer should obtain an individual's prior consent to participate in the social media marketing process whereby the marketer is added as a "friend" or a contact to be shared with the individual's other social media contacts;

- Profile data that contains personally identifiable information provided by an individual on a social networking site should not be shared with third parties without that individual's prior consent unless the user has agreed to post or populate such information in an unrestricted publicly accessible location;

- If tracking data is being collected as part of the social media marketing process for purposes of online behavioral advertising, please refer to Article #38;

- If a social or interactive advertising application (incorporating user-generated content or user interactions that the individual has consented to being shared) is being distributed to the individual's contacts, a preview should be provided to that individual for review and approval before it is distributed by the marketer to that individual's contacts. The recipient of the ad should be provided with an opportunity to opt out of receiving future communications from the marketer and having his/her information shared; and

- Marketers should not retain personally identifiable information used for social marketing purposes except for marketing purposes, and should not share such data with any third party without the individual's prior consent unless the user has agreed to post or populate such information in an unrestricted publicly accessible location.

Marketers using testimonials and endorsements in any media, including but not limited to social media channels (e.g., online message boards, blogging, etc.) and "word-of-mouth" marketing, should comply with Article #21 – Testimonials & Endorsements – of these Guidelines. Additionally, where marketing to children is permitted by law, marketers using social media channels should comply with Articles #13 - #16 of these Guidelines and ensure the marketing is suitable for the child, taking into account the age range, knowledge, sophistication, and maturity of their intended audience.

5. OPERATORS OF SOCIAL MEDIA PLATFORMS & FORUMS

In addition to complying with the aforementioned items, operators of social media networks, platforms or other social media forums should:

- Post their privacy policy in a prominent location on their site so that it is clear and conspicuous;

- Advise individual users about their privacy policies, data deletion policy and the steps users should follow to change their privacy settings, to deactivate or to delete their accounts;

- Prevent games, quizzes and other applications developed by third parties from accessing personally identifiable information from an individual user until the marketer has provided clear and conspicuous notice to the individual before accessing their information (notice must include an opportunity to refuse marketing communications associated with the application), or obtains prior consent from that user for each category of personal information accessed.

E-MAIL APPENDING TO CONSUMER RECORDS
Article #44

Definition of e-mail address appending: E-mail address appending is the process of adding a consumer's e-mail address to that consumer's record. The e-mail address is obtained by matching those records from the marketer's database against a third-party database to produce a corresponding e-mail address.

A marketer should append a consumer's e-mail address to its database only when the consumer gives a marketer permission to add his or her e-mail address to the marketer's database; or

1. There is an established business relationship with that consumer either online or offline, and
2. The data used in the append process are from sources that provided notice and choice regarding the acceptance of receiving third-party e-mail offers and where the consumer did not opt out, and
3. Reasonable efforts are taken to ensure the appending of accurate e-mail addresses to the corresponding consumer records

Marketers should not send e-mails to appended e-mail addresses that are on their in-house e-mail suppression files. Marketers should not send Mobile Service Commercial Messages (MSCMs) to appended e-mail addresses that belong to wireless handsets or devices unless the recipient has provided prior express authorization to receive such messages from the sender. A marketer should not sell, rent, transfer, or exchange an appended e-mail address of a consumer unless it first offers notice and choice to the consumer. All messages to an e-mail appended address should include a notice and choice to continue to communicate via e-mail.

Marketers should have in place appropriate record-keeping systems to ensure compliance with these guidelines.

Telephone Marketing to Landline & Wireless Devices

REASONABLE HOURS

Article #45

Telephone contacts, whether to a landline or wireless handset or device, should be made during reasonable hours as specified by federal and state laws and regulations.

TAPING OF CONVERSATIONS

Article #46

Taping of telephone conversations by telephone marketers should only be conducted with notice to or consent of all parties, or the use of a beeping device, as required by applicable federal and state laws and regulations.

RESTRICTED CONTACTS

Article #47

A marketer should not knowingly call or send a voice solicitation message to a consumer who has an unlisted or unpublished telephone number except in instances where that specific number was provided by the consumer to that marketer for that purpose. A marketer should maintain an in-house Do-Not-Call list and refrain from calling numbers for solicitation purposes that are on the marketer's in-house Do-Not-Call list.

A marketer should not knowingly call a wireless device, except in instances where the recipient has provided prior express consent to receive such calls from that marketer.

Prior to contacting a landline or wireless device, marketers should use applicable federal and DMA Wireless Suppression Files or another comprehensive wireless suppression service. Such suppression files should assist marketers in determining whether or not they are contacting a wireless device, including landline numbers that have been ported to wireless handsets or devices.

A marketer should use DMA's Telephone Preference Service as required in Article #31 and must use the federal Do-Not-Call registry and state Do-Not-Call lists when applicable prior to using any outbound calling list.Telemarketing calls may be made to landline telephones, where the telemarketer has an established business relationship with the individuals even if the individual is on the national registry. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services within the last 3 months. (Note: State laws may vary. DMA's website at: www.the-dma.org/government/donotcalllists.shtml attempts to provide current information on state Do-Not-Call lists.) Consumers who have provided informed, written permission to the marketer do not need to be suppressed by any Do-Not-Call list. Individuals can add or remove themselves from company-specific Do-Not-Call lists either orally or in writing.

Marketers should not use randomly or sequentially generated numbers in sales or marketing solicitations.

CALLER-ID/AUTOMATIC NUMBER IDENTIFICATION REQUIREMENTS

Article #48

Marketers engaging in telemarketing to landline and wireless telephone numbers should generate caller identification information, including:

- A telephone number for 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 by making a do-not-call request, and
- Whenever the technology is available from the marketer's telecommunications carrier, the name of the seller on whose behalf the call is placed or service bureau making the call.

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, landline telephone numbers gained from ANI, except where a prior business relationship exists for the sale of directly related goods or services. With regard to mobile telephone numbers, marketers should abide by Articles #31 and #35.

USE OF AUTOMATED DIALING EQUIPMENT

Article #49

Marketers using automated dialing equipment should allow 15 seconds or four rings before disconnecting an unanswered call.

Marketers should connect calls to live representatives within two seconds of the consumer's completed greeting (except in cases where a prerecorded marketing message is used, in accordance with Article #55). If the connection does not occur within the two-second period, then the call is considered abandoned whether or not the call is eventually connected.
For any abandoned calls, the marketer should play a prerecorded identification message that includes the seller's name and telephone number, states the purpose of the call, and provides a telephone number at which the consumer can request not to receive future marketing calls.
Repeated abandoned or "hang up" calls to consumers' residential telephone numbers should be minimized. In no case should calls be abandoned more than:

- Three percent of answered calls, measured over the duration of a single calling campaign, if the campaign is less than 30 days, or separately over each successive 30-day period or portion of that period during which the campaign continues (unless a more restrictive state law applies), or
- Twice to the same telephone number within a 48-hour time period.

Marketers should only use automated dialing equipment that allows the telephone to immediately release the line when the called party terminates the connection.

When using any automated dialing equipment to reach a multi-line location, whether for business-to-consumer or business-to-business marketing, the equipment should release each line used before connecting to another.

Companies that manufacture and/or sell automated dialing equipment should design the software with the goal of minimizing abandoned calls to consumers. The software should be delivered to the user set as close to 0% as possible. Manufacturers should distribute these Guidelines for Automated Dialing Equipment to purchasers of dialing equipment and recommend that they be followed.

The dialers' software should be capable of generating a report that permits the user of the equipment to substantiate compliance with the guideline.

Glossary of Terms Used

Automated Dialing Equipment – any system or device that initiates outgoing call attempts from a predetermined list of phone numbers, based on a computerized pacing algorithm.

Abandoned Call – a call placed by automated dialing equipment to a consumer which when answered by the consumer, (1) breaks the connection because no live agent is available to speak to the consumer, or (2) no live agent is available to speak to the consumer within 2 seconds of the consumer's completed greeting.

Abandonment Rate – the number of abandoned calls over a 30-day period divided by the total number of calls that are answered by a live consumer. Calls that are not answered by a live consumer do not count in the calculation of the abandonment rate.

Campaign – refers to an offer of the same good or service for the same seller. As long as the same good or service is being offered by the same seller, the offer is part of a single campaign, regardless of whether there are changes in the terms of the offer or the wording of any marketing material, including any telemarketing script, used to convey the offer. This definition applies to Article 48 only and is based on the FTC's definition of a "campaign" for purposes of calculating the abandonment rate.

Report – reportable information that should be made available which contains key points, including the percentage of abandoned calls.

Telemarketing – a telephone call, prerecorded message or text message placed to a landline or wireless number for the purpose of promoting, advertising, marketing or offering goods or services.

USE OF PRERECORDED VOICE MESSAGING

Article #50

Marketers who use prerecorded voice messaging should not automatically terminate calls or provide misleading or inaccurate information when a live consumer answers the telephone.

Marketers should only use prerecorded voice messaging to sell good or services if they have first obtained the call recipient's prior express written agreement to receive prerecorded messages. In obtaining the consumer's written agreement, a marketer should observe the following:

- Before obtaining the consumer's informed consent, the marketer should clearly and conspicuously disclose that the purpose of the agreement is to allow the marketer to make prerecorded message calls to the consumer.
- The written agreement should evidence the consumer's informed consent to receive prerecorded calls by or on behalf of the specific marketer
- The marketer should not require that the consumer agree to receive prerecorded calls as a condition of purchasing any good or service.
- The agreement should include the consumer's telephone number and signature.
- Marketers may obtain the written agreement electronically in accordance with applicable laws such as the E-Sign Act.

Marketers should begin making the initial disclosures as specified under Article #52 within two seconds of the call recipient's completed greeting.

Immediately following the initial disclosures, marketers should provide an opt-out mechanism that the call recipient can use to be placed on the company's do-not-call list. The type of mechanism that the marketer should provide depends on whether the call can be answered by a live person or by an automated device. If the marketer is able to determine whether a prerecorded call has been answered by a live person or an automated device, the marketer should tailor the prerecorded message to include the appropriate opt-out mechanism (either option 1 or 2 below):

1. If the call is answered by a live person, then the marketer should provide an automated interactive voice and/or keypress-activated opt-out mechanism that the recipient can use to make an opt-out request. The mechanism should be available for use at any time during the message.

2. If the call is answered by an answering machine or voicemail system, then the prerecorded message should provide a toll-free telephone number that the recipient can call to make an opt-out request at any time during the telemarketing campaign. The telephone number provided should connect directly to an automated interactive voice and/or keypress-activated opt-out mechanism. Consumers should be able to call at any time of the day, and on any day, during the duration of the campaign.

If the marketer is not able to determine whether a prerecorded call has been answered by a live person or an automated device, the prerecorded message should include both options 1 and 2.

The interactive voice and/or keypress-activated opt-out mechanism – regardless of whether the prerecorded call can be answered by a live person or automated answering device – should have the following features:

- The opt-out mechanism should automatically add the number called to the entity's company-specific do-not-call list; and
- The opt-out mechanism should immediately disconnect the call once the opt-out request is made.

Marketers may use prerecorded messages that provide information, but do not induce the purchase of goods or services, without first obtaining written consent and without providing an opt-out mechanism. Such calls should promptly disclose the identity of the caller at the outset of the call and provide a telephone number sometime during the call.

USE OF TELEPHONE FACSIMILE MACHINES

Article #51

Unless there is an established business relationship, or unless prior permission has been granted, advertisements, offers and solicitations, whether sent to a consumer or a business, should not be transmitted to a facsimile machine, including computer fax machines. An established business relationship in the fax context is defined as a prior or existing relationship based on a voluntary, two-way communication between the sender and recipient of the fax. Such communication includes a purchase, transaction, inquiry, or application for or about goods or services offered by the sender. For business relationships formed after July 9, 2005, the fax number must be provided voluntarily by the recipient to the sender, or be made available voluntarily by the recipient in a directory, advertisement, or Internet site.

Each permitted transmission to a fax machine must clearly contain on the first page:

- the date and time the transmission is sent;
- the identity of the sender which is registered as a business with a state;
- the telephone number of the sender or the sending machine; and
- a clear and conspicuous opt-out notice.

The opt-out notice should:

- clearly state that the recipient may opt out of any future faxes and provide clear instructions for doing so;
- provide a domestic telephone number and fax number for recipients to transmit an opt-out request; and
- unless the telephone or fax number is toll-free, a cost-free mechanism to submit an opt-out request.

Senders must accept opt-out requests at any time.

Opt-out requests must be honored in 30 days, or sooner if feasible. An opt-out request terminates permission to send future faxes based only on an established business relationship.

PROMOTIONS FOR RESPONSE BY TOLL-FREE AND PAY-PER-CALL NUMBERS

Article #52

Promotions for response by 800 or other toll-free numbers should be used only when there is no charge to the consumer for the call itself and when there is no transfer from a toll-free number to a pay call.
Promotions for response by using 900 numbers or any other type of pay-per-call programs should clearly and conspicuously disclose all charges for the call. A preamble at the beginning of the 900 or other pay-per-call should include the nature of the service or program, charge per minute, and the total estimated charge for the call, as well as the name, address, and telephone number of the sponsor. The caller should be given the option to disconnect the call at any time during the preamble without incurring any charge. The 900 number or other pay-per-call should only use equipment that ceases accumulating time and charges immediately upon disconnection by the caller.

DISCLOSURE AND TACTICS

Article #53

Marketers should make the following initial disclosures promptly:

- The identity of the seller or charitable organization on behalf of which the call is made;
- That the purpose of the call is to sell goods or services or to solicit a charitable contribution;
- The nature of the goods or services offered during the call (if applicable); and
- If a prize promotion is offered, that no purchase or payment is necessary to be able to win a prize or participate in a prize promotion and that any purchase or payment will not increase the person's chances of winning.

Prior to asking consumers for payment authorization, telephone marketers should disclose the cost of the merchandise or service and all terms and conditions, including payment plans, whether or not there is a no refund or a no cancellation policy in place, limitations, and the amount or existence of any extra charges such as shipping and handling and insurance. At no time should high pressure tactics be utilized.

Mobile Marketing

Please refer to the Glossary of Terms at the end of this section for the complete definitions of key concepts and terms used within this section.

OBTAINING CONSENT TO CONTACT MOBILE DEVICES

Article #54

Marketers should obtain prior express consent from existing and prospective customers before sending mobile marketing to a wireless device. A marketer should be able to demonstrate that the recipients knowingly and affirmatively consented. Consent may be obtained orally, in writing or electronically.

PROVIDING NOTICE ABOUT MOBILE MARKETING PRACTICES

Article #55

Marketers that send or intend to send mobile messages should publish an easily accessible notice of their practices (which includes but is not limited to a notice in their respective privacy policies) with regard to mobile marketing. The notice must include sufficient information to allow individuals to make an informed choice about their interaction with the marketer. This should include, at minimum, any applicable terms and conditions, details of the marketer's information handling practices and clear directions about how to unsubscribe.

The notice should be easy to find, read and understand, and should comply with existing DMA Guidelines. Of particular note, mobile marketers should review and comply with the Terms of the Offer (Articles #1-6, #8, #9), Advance Consent Marketing (Article #12), Special Offers & Claims (Articles #17-#21), and Sweepstakes (Articles #22-#27).

MOBILE OPT-OUT REQUESTS

Article #56

Every mobile marketing message sent must include a simple and easy-to-use mechanism through which the individual can opt out of receiving future mobile marketing messages. Where possible, the opt-out mechanism provided should allow the recipient to opt out via reply text message.

Where individuals respond to a marketer indicating that they do not wish to receive future mobile marketing messages (e.g. an individual replies "STOP"), the marketer should honor the request. Mobile opt-out requests should be honored within 10 days of being received and in accordance with Article #31.

SPONSORSHIP OR AFFILIATE MOBILE MARKETING

Article #57

A marketer may include an affiliate or sponsorship message within a mobile marketing communication, providing that the recipient has provided prior express consent to receive mobile marketing communications from that marketer and that it is clear from the mobile marketing communication that the message has been sent by that marketer and not by the sponsor. A marketer should also comply with Article #8 - Disclosure of Sponsor and Intent.

LOCATION-BASED MOBILE MARKETING

Article #58

Marketers sending location-based mobile marketing messages to recipients should adhere to Articles #54-56. In addition, marketers should inform individuals how location information will be used, disclosed and protected so that the individual

may make an informed decision about whether or not to use the service or consent to the receipt of such communications. Location-based information must not be shared with third-party marketers unless the individual has given prior express consent for the disclosure.

MOBILE SUBSCRIPTION SERVICES AND PREMIUM-RATE MOBILE SERVICES

Article #59

Mobile subscription services and mobile premium-rate products and/or services should be offered and delivered in accordance with DMA Guidelines, in particular the Terms of the Offer (Articles #1-6, #8, #9), Advance Consent Marketing (Article #12), Marketing to Children (Article #13-#16), Special Offers & Claims (Articles #17-#21) and Sweepstakes (Articles #22-#27). All advertising and marketing for mobile subscription services or premium-rate mobile products/services should clearly define the service offered and outline the terms and conditions of the offer in accordance with these articles. Mobile subscription services or premium-rate mobile services should not be supplied unless the recipient has actively requested to receive the specific service to be supplied. Further, prior express consent should be obtained from a recipient prior to supplying additional or separate mobile subscription services and premium-rate mobile services at a subsequent date.

In accordance with Articles #12 and #48, and prior to sending or charging recipients for mobile subscription services and/or premium-rate mobile products/services, marketers should:

- provide the individual with an opportunity to see or hear the terms and conditions relating to the subscription service, including:
  - the cost per unit or the total cost of the subscription or premium-rate service;
  - the term of the subscription or premium-rate service;
  - the frequency of the subscription or premium-rate service;
  - payment intervals;
  - how to terminate the subscription or premium-rate service including any terms and conditions that apply to such termination.

- obtain prior express consent from recipients to receive and be charged for said subscriptions, products and/or services;
- inform recipients in the initial offer and in renewal reminders of their right to cancel their participation in the plan, and include contact information within the initial and renewal messages that allows the recipient to directly contact them;
- provide renewal reminders at the frequency specified in the initial offer;
- promptly honor requests for refunds due upon a consumer's cancellation of the plan;
- abide by Articles #13-#16 and #48, and take reasonable precautions and implement adequate technical accountability and authentication measures to ascertain that

  - (a) the mobile phone number or email address provided indeed belongs to the intended recipient of the subscriptions, products or services, and

  - (b) periodically, and not less than once a month, include contact information within the mobile subscription service message or premium-rate mobile service message that allows the individual to directly contact the marketer.

Glossary of Terms Used

Individuals – refers to the recipients or potential recipients of mobile marketing communications. For purposes of opting out (refer to Article #56), individuals refers to the number(s) and/or electronic address(es) of the wireless device(s) used by the recipients.

Location-Based Services – marketing text message targeted to a recipient dependent on their location, by a handset or user's physical location.

Mobile Marketing – refers to a sales and promotion technique in which promotional materials are delivered to a wireless phone or device. It can include both 'direct mobile marketing' (i.e. marketing communications targeted, sent or "pushed" to a wireless handset or device, such as marketing text messages) and 'indirect mobile marketing' (i.e. marketing that can be accessed or "pulled" by an individual via a wireless handset or device such as a mobile enabled website). Examples include the sending of SMS, MMS or WAP push messages, Bluetooth messaging and other interrupt based marketing to wireless devices.

Mobile Service Commercial Message (MSCM) – a commercial electronic message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service.

Multi-Media Messaging Services (MMS) – an extension of a the Short Message Service Technology that permits the marketer to send marketing messages to a wireless handset that include multimedia objects such as images, audio and video.

Mobile Subscription Service – a service that is provided periodically or on an ongoing basis that is delivered to an individual via a wireless handset or device. This includes free services and paid subscription services.

Premium Rate Mobile Services – a service that is provided in a single instance, periodically or on an ongoing basis that is delivered to an individual via a wireless handset or device whereby the recipient pays a rate that exceeds the standard tariff to either receive or send a mobile message.

Prior Express Consent – refers to affirmative, express and informed consent. A marketer should be able to demonstrate that recipients knowingly and affirmatively consented to be contacted on their wireless devices by that marketer for any purposes. Consent may be obtained orally, in writing or electronically. The notice to obtain consent should include a clear and conspicuous disclosure and require an active step on the part of the recipient to demonstrate that he/she agrees to receive the communication and/or product or service. This consent may be obtained via any channel. A pre-checked box, for example, would not suffice as an adequate means for obtaining consent.

Recipient – any natural or legal person or business that receives a mobile marketing communication.

Short Message Service (SMS) – a marketing message sent as a text message.

Text message – a brief electronic message sent between mobile phones, containing text composed by the sender, usually input via a lettering system on a cell phone's numeric keypad.

Wireless Application Protocol (WAP) – Refers to a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators.

Wireless – Refers to telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.

Wireless Handset – Umbrella term for devices, typically with keys to input data, that are mobile and can be operated by hand. Examples are mobile phones, pagers, two-way radios, smartphones and communicators.

FUNDRAISING

Article #60

In addition to compliance with these guidelines, fundraisers and other charitable solicitors should, whenever requested by donors or potential donors, provide financial information regarding use of funds.

LAWS, CODES, AND REGULATIONS

Article #61

Direct marketers should operate in accordance with laws and regulations of the United States Postal Service, the Federal Trade Commission, the Federal Communications Commission, the Federal Reserve Board, and other applicable federal, state, and local laws governing advertising, marketing practices, and the transaction of business.

Other DMA Resources

- "Do the Right Thing" Compliance Guide
- Commitment to Consumer Choice Member Compliance Guide
- Preference Services Subscriber Information
- DMA's consumer website: **www.DMAchoice.org**
- Privacy Policy Generators
- Environmental Resources and Generator (The "Green 15")
- E-Commerce Integrity Resource Center
- Information Security: Safeguarding Personal Data in Your Care

See DMA's Resources for Businesses Guide for numerous other resources developed by the Department of Corporate & Social Responsibility:
www.dmaresponsibility.org

DMA can also provide your company with information on the following Federal Trade Commission (FTC) and Federal Communications Commission (FCC) regulations and rules affecting direct marketers:

FTC:

- Mail or Telephone Order Merchandise Rule
- Telemarketing Sales Rule
- Children's Online Privacy Protection Rule
- Negative Option Rule
- Guides against Deceptive Pricing

FCC:

- Telephone Consumer Protection Act

The US Postal Service's *Fighting Mail Order Fraud and Theft: Best Practices for the Mail Order Industry Reference Guide* is available, as well as other DMA and government titles, and a variety of consumer education brochures.

DMA's Department of Corporate & Social Responsibility

In its continuing efforts to improve and advance the practices of direct marketing and the marketer's relationship with customers, the DMA sponsors several activities through its Department of Corporate & Social Responsibility:

- Ethical Guidelines are maintained, updated periodically, and distributed to the direct marketing community.
- The Committee on Ethical Business Practice investigates and examines promotions and practices throughout the direct marketing community that are brought to its attention.
- The Ethics Policy Committee revises the Guidelines as needed, and initiates programs and projects directed toward improved ethical awareness in the direct marketing arena.
- The Committee on the Environment and Social Responsibility identifies ways for members to be good corporate citizens and recommends relevant best practices.
- "Dialogue" meetings between direct marketing professionals and consumer affairs and regulatory representatives facilitate increased communication between direct marketers and their customers.
- DMA's Commitment to Consumer Choice builds consumer trust in the marketing process by offering individual choices online and offline.

www.DMAchoice.org offers consumers assistance in managing their mail and email marketing preferences, and provides consumer education. www.Aboutads.info provides consumers choices for online behavioral advertising. The DMA CSR department oversees compliance by marketers to ensure consumer choices are being honored.

For additional information contact DMA's Washington Office:

1615 L Street, NW, Suite 1100
Washington, DC 20036
202.955.5030
Fax: 202.955.0085
www.dmaresponsibility.org
E-mail: ethics@the-dma.org

Direct Marketing Association, Inc. Headquarters:
1120 Avenue of the Americas
New York, New York 10036-6700
212.768.7277
Fax: 212.302.6714
www.the-dma.org

Direct Marketing Association, Inc.
Headquarters:

1120 Avenue of the Americas
New York, New York 10036-6700
212.768.7277
Fax: 212.302.6714
www.the-dma.org

EXHIBIT 2

Direct Marketing Association's • GUIDELINES • for Ethical Business Practice

2014

DIRECT MARKETING ASSOCIATION GUIDELINES for Ethical Business Practice

The Direct Marketing Association's Guidelines for Ethical Business Practice are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct. These guidelines reflect DMA's long-standing policy of high levels of ethics and the responsibility of the Association, its members, and all marketers to maintain consumer and community relationships that are based on fair and ethical principles. In addition to providing general guidance to the industry, the Guidelines for Ethical Business Practice are used by DMA's Committee on Ethical Business Practice, an industry peer review committee, as the standard to which direct marketing promotions that are the subject of complaint to DMA are compared.

These guidelines represent DMA's general philosophy that self-regulatory measures are preferable to governmental mandates. Self-regulatory actions are more readily adaptable to changing techniques and economic and social conditions. They encourage widespread use of sound business practices.

Because dishonest, misleading or offensive communications discredit all means of advertising and marketing, including direct marketing, observance of these guidelines by all concerned is expected. All persons involved in direct marketing should take reasonable steps to encourage other industry members to follow these guidelines as well.

DMA Guidelines provide the basis for DMA member compliance for ethical marketing practices and compliance primarily under U.S. laws. Global companies should be reviewing international rules in addition to U.S. rules. For compliance examples and specific best practices which may be over and above baseline guidelines, please refer to DMA's guidance and best practice documents, such as its "Do the Right Thing" guidance. The DMA also asks its members to review the Fair Information Practices and Principles (FIPPs.) Send questions to ethics@the-dma.org.

January, 2014

DMA
Advancing and Protecting
Responsible Data-Driven Marketing

DMA Member Principles

DMA Member Principles are the underlying framework for the *Guidelines for Ethical Business Practice* as detailed herein, and for Guidelines that will be drafted in the future. These Principles apply to DMA members' relationships with current and prospective customers, donors, and members, and are the grounding for all DMA members, which includes those who market directly not only to consumers, but also to businesses, government agencies, and "SOHO" (small-office/home-office) entities. The Principles provide a general statement to the public of the expectations they can have when dealing with DMA members.

A DMA Member:

1. Is committed to customer satisfaction, good corporate citizenship, and responsible environmental, community and financial stewardship
2. Clearly, honestly, and accurately represents its products, services, terms and conditions
3. Delivers its products and services as represented
4. Communicates in a respectful and courteous manner
5. Responds to inquiries and complaints in a constructive, timely way
6. Maintains appropriate security policies and practices to safeguard information
7. Provides information on its policies about the transfer of personally identifiable information for marketing purposes
8. Honors requests not to have personally identifiable information transferred for marketing purposes
9. Honors requests not to receive future solicitations from its organization
10. Follows the spirit and letter of the law as well as DMA's *Guidelines for Ethical Business Practice*

Table of Contents

The Terms of the Offer

HONESTY AND CLARITY OF OFFER
Article #1
All offers should be clear, honest, and complete so that the consumer may know the exact nature of what is being offered, the price, the terms of payment (including all extra charges) and the commitment involved in the placing of an order. Before publication of an offer, marketers should be prepared to substantiate any claims or offers made. Advertisements or specific claims that are untrue, misleading, deceptive, or fraudulent should not be used.

ACCURACY AND CONSISTENCY
Article #2
Simple and consistent statements or representations of all the essential points of the offer should appear in the promotional material. The overall impression of an offer should not be contradicted by individual statements, representations, or disclaimers.

CLARITY OF REPRESENTATIONS
Article #3
Representations which, by their size, placement, duration, or other characteristics are unlikely to be noticed or are difficult to understand should not be used if they are material to the offer.

ACTUAL CONDITIONS
Article #4
All descriptions, promises, and claims of limitation should be in accordance with actual conditions, situations, and circumstances existing at the time of the promotion.

DISPARAGEMENT
Article #5
Disparagement of any person or group on grounds addressed by federal or state laws that prohibit discrimination is unacceptable.

DECENCY
Article #6
Solicitations should not be sent to consumers who have indicated to the marketer that they consider those solicitations to be vulgar, immoral, profane, pornographic, or offensive in any way and who do not want to receive them.

PHOTOGRAPHS AND ART WORK
Article #7
Photographs, illustrations, artwork, and the situations they describe should be accurate portrayals and current reproductions of the products, services, or other subjects they represent.

DISCLOSURE OF SPONSOR AND INTENT
Article #8
All marketing contacts should disclose the name of the sponsor and each purpose of the contact. No one should make offers or solicitations in the guise of one purpose when the intent is a different purpose regardless of the marketing channel used.

ACCESSIBILITY
Article #9
Every offer should clearly identify the marketer's name and street address or telephone number, or both, at which the individual may obtain service and exercise their marketing preferences. If an offer is made online, the marketer should provide its name, an Internet-based contact mechanism, and a street address. For email solicitations, marketers should comply with Article #40 (Commercial Solicitations Online). For mobile marketing solicitations, marketers should comply with Articles #54-56 to provide adequate notice to consumers to allow them to exercise their marketing preferences.

SOLICITATION IN THE GUISE OF AN INVOICE OR GOVERNMENTAL NOTIFICATION
Article #10
Offers that are likely to be mistaken for bills, invoices, or notices from public utilities or governmental agencies should not be used.

POSTAGE, SHIPPING, OR HANDLING CHARGES
Article #11
Postage, shipping, or handling charges, if any, should bear a reasonable relationship to actual costs incurred.

ADVANCE CONSENT/NEGATIVE OPTION MARKETING
Article #12
These guidelines apply to all media and address marketing plans where the consumer gives consent to receive and pay for goods or services in the future *on a continuing or periodic basis, unless and until the consumer cancels the plan.*

The following should apply to all advance consent or negative option marketing plans:

1. Initial Offer:

   CONSENT: Regardless of channel, marketers should have the consumer's express informed consent to participate in any advance consent or negative option marketing plan before the consumer is billed or charged. For example, a pre-checked box without further action, such as clicking a response button or sending back a response to confirm individual consent is not sufficient. In telephone sales where the consumer agrees to the offer in a way other than by credit or debit card payment, the consumer consent must be written or audio recorded.

- Marketers should inform consumers in the initial offer of their right to cancel their participation in the plan and any outstanding fees that may be owed.

- Marketers should inform consumers in the initial offer of the length of any trial period, including a statement that the consumer's account will be charged after the trial period (including the date of the charge) unless the consumer takes an affirmative step to cancel, providing the consumer a reasonable time period to cancel, and the steps needed to avoid charges.

MATERIAL TERMS & CONDITIONS: Regardless of channel, marketers should clearly and conspicuously disclose all material terms and conditions before obtaining the consumer's billing information, including:

- A description of the goods or services being offered
- The identity of the marketer and contact information for service or cancellation
- The interval between shipments or services to be provided
- The price or the range of prices of the goods or services purchased by the consumer, including whether there are any additional charges should be disclosed
- Whether the consumer will be billed or automatically charged
- When and how frequently the consumer will be billed or charged
- Any terms with regards to a "free to keep" incentive as applicable
- The fact that the consumer must take affirmative action to cancel in order to avoid future billing or charges
- The specific and easy steps that consumers should follow to cancel the plan and to stop recurring charges from being placed on the consumer's account, and
- The time period within which the consumer must cancel.

When applicable, the following terms and conditions should also be clearly and conspicuously disclosed in the initial offer:

- That the current plan or renewal prices of the goods or services are subject to change
- The length of any free, trial or approval period in time or quantity
- The length of membership period, and the length of subsequent renewal or billing periods
- The fact that goods or services will continue after the free period unless the consumer cancels
- Any minimum purchase obligations, and
- The terms and conditions of any refund policy

In instances where the marketer uses pre-acquired account information under a free-to-pay conversion plan, the marketer should:

- Obtain from the consumer the complete account number to be charged within the appropriate data security protocols (such as PCI compliance)
- Obtain affirmative consent from the consumer to charge such account, and
- Provide channel specific proof (an email or hard copy confirmation, or if via telephone, audio record the entire transaction.)

In instances where the marketer uses pre-acquired account information but does not engage in a free-to-pay conversion plan, the marketer should:

- Identify with specificity the account that will be charged, and
- Obtain affirmative consent from the consumer to charge such account

2. Providing the Goods & Services to the Consumer:

- Marketers may provide products or services and bills concurrently; however, consumers should not be obligated to pay bills prior to the expiration of any trial period.

- Marketers should inform consumers in renewal reminders of their right to cancel their participation in the plan, and any outstanding fees owed.

- Marketers should provide renewal reminders at the frequency specified in the initial offer.

3. Cancellation:

- Marketers should promptly honor requests for refunds due upon consumers' cancellation of the plan.

- Marketers should allow consumers a reasonable length of time between receipt of renewal reminders and the renewal date, after which consumers can cancel the plan.

- Marketers should honor the time period they provided for a cancellation and should honor a cancellation after the expiration of the trial period.

4. For Internet Sales:

The initial merchant must never disclose a credit card, debit card or other financial account number or other billing information that is used to charge the customer of the initial merchant to any post-transaction third party seller for use in an Internet-based sale of any goods or services from that post-transaction third party seller.

Post-Transaction Third Party Sales:

For post-transaction third party sellers:
No charges should apply to a consumer's account before obtaining the consumer's billing information as follows:

The third party seller has first clearly and conspicuously disclosed to the purchaser a description of the goods and services being offered and all material terms of the offer including:

- The fact that the third party seller is not affiliated with the initial merchant;
- The costs of such goods or services;
- And the consumer has provided express informed consent for the charges by providing the complete account information to be charged, providing the consumer's name and address and a means to contact the consumer, and providing confirmation such as clicking a confirmation button or otherwise demonstrating consent to the charges.

All marketing partners or service providers should comply with these guidelines.

Marketing to Children

MARKETING TO CHILDREN
Article #13
Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online, via wireless devices such as a mobile phone, or in any other medium, or by providing a commercial website or other online services directed to children under 13, marketers should first determine whether the collection and use of the child's data for marketing purposes or the sending of marketing material to the child is permitted under federal law, such as the Children's Online Privacy Protection Act (COPPA), or state law. Where marketing to children is permitted by law, marketers should ensure the marketing is suitable for the child taking into account the age range, knowledge, sophistication, and maturity of their intended audience.

Definitions:

Covered Entities for COPPA and related online data issues: These include operators of commercial websites and online services (including mobile apps or any service available over the Internet or that connects to the Internet or a wide-area network) directed to children under 13 that collect, use or disclose personal information from children; third parties (e.g. social plug ins and ad networks) with actual knowledge of such information collection. Further, first parties are held strictly accountable for the actions of third parties on that first party's site or service.

Personal Information:
This includes the following:

- First and last name;
- A home or other physical address;
- Online contact information;
- A screen or user name that functions as online contact information;
- A telephone number;
- A social security number;
- A persistent identifier that serves to recognize a user over time across different websites or online services;
- A video, photograph or audio file where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of the child that the operator collects online from the child and combines with an identifier described above.

Direct Notice to Parents: Parents must be provided with a detailed direct notice of the operator's personal information collection, use and disclosure practices, not through a hyperlink.

PARENTAL RESPONSIBILITY AND CHOICE
Article #14
Marketers communicating commercial appeals, operators of commercial websites, and online services (such as mobile apps) directed to children under 13 should provide direct notice (as defined above) and an opportunity to opt out of the marketing process so that parents have the ability to limit the collection, use, and disclosure of their children's names, addresses, or other personally identifiable information prior to such collection, use and disclosure.

Parents must be provided the choice of consenting to the operator's collection and internal use of a child's information. Such information may never be disclosed to third parties (unless the disclosure is integral to the site or service, in which case that must be made clear to the parent.)

Parents must have access to their child's personal information to review and/or have that information deleted.

Parents must be given an opportunity to prevent further use or online collection of a child's personal information.

COLLECTION AND USE OF INFORMATION FROM OR ABOUT CHILDREN
Article #15
Marketers should limit the collection, use, and dissemination of personally identifiable information collected from or about children to that information that is required for the promotion, sale, and delivery of goods and services; the provision of customer services; conducting market research; and engaging in other appropriate marketing activities.

Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected.

Upon request from a parent, marketers should promptly provide the source and general nature of information maintained about a child and allow for removal or correction.

Marketers should implement the strictest security measures to ensure against unauthorized access, alteration, or dissemination of the data collected from or about children, and should provide information regarding such measures upon request to the parent or guardian of the minor.

Operators should retain personally identifiable information only as long as is reasonably necessary, and must delete personally identifiable information using reasonable measures.

ONLINE MARKETING TO CHILDREN UNDER 13 YEARS OF AGE
Article #16

This Article applies to online marketing as follows:

Online marketers (operators of general audience websites or online services) should not knowingly collect personally identifiable information online or via wireless handsets or devices

from a child under 13 without prior verifiable parental consent and direct parental notification of the nature and intended use of such information, and shall provide an opportunity for the parent to prevent such use and participation in the activity.

Operators of websites and online services must provide a privacy notice with clear and concise description of their information policies and practices. This notice should be easy to read on smaller screens (e.g., mobile devices.) for parents and allow them to provide verifiable consent.

Marketers are not required to ask the age of a child and may rely on the information provided by the user. Marketers may age screen users and apply notice and consent requirements only for users that identify themselves as being under age 13. If an operator later determines that a particular user is a child under the age of 13, parental notice and consent requirements are triggered.

Online and wireless/mobile contact information should only be used to directly respond to an activity initiated by a child and not to re-contact a child for other purposes without verifiable prior parental consent.

Marketers should not knowingly collect, without verifiable prior parental consent, personally identifiable information online or via a wireless handset or device from children that would permit any offline contact with the child.

Marketers should not knowingly distribute to any third parties, without verifiable prior parental consent, information collected from a child that would permit any contact with that child.

Marketers should take reasonable steps to prevent the online publication or posting of information that would allow a third party to contact a child offline unless the marketer has verifiable prior parental consent.

Marketers should not entice a child online to divulge personally identifiable information by the prospect of a special game, prize, or other offer.

Marketers should not make a child's access to website or mobile content contingent on the collection of personally identifiable information. Only online contact information used to enhance the interactivity of the site is permitted.

The following assumptions underlie these online guidelines:

- When a marketer directs a site at a certain age group, it can expect that the visitors to that site are in that age range, and
- When a marketer asks the age of the child, the marketer can assume the answer to be truthful.

Special Offers and Claims

USE OF THE WORD "FREE" AND OTHER SIMILAR REPRESENTATIONS
Article #17
A product or service that is offered without cost or obligation to the recipient may be unqualifiedly described as "free."

If a product or service is offered as "free," all qualifications and conditions should be clearly and conspicuously disclosed, in close conjunction with the use of the term "free" or other similar phrase. When the term "free" or other similar representations are made (for example, 2-for-1, half-price, or 1-cent offers), the product or service required to be purchased should not have been increased in price or decreased in quality or quantity.

PRICE COMPARISONS
Article #18
Price comparisons, including those between a marketer's current price and a former, future, or suggested price, or between a marketer's price and the price of a competitor's comparable product, should be fair and accurate.

In each case of comparison to a former, manufacturer's suggested, or competitor's comparable product price, recent substantial sales should have been made at that price in the same trade area.

For comparisons with a future price, there should be a reasonable expectation that the new price will be charged in the foreseeable future.

GUARANTEES
Article #19
If a product or service is offered with a guarantee or a warranty, either the terms and conditions should be set forth in full in the promotion, or the promotion should state how the consumer may obtain a copy. The guarantee should clearly state the name and address of the guarantor and the duration of the guarantee.

Any requests for repair, replacement, or refund under the terms of a guarantee or warranty should be honored promptly. In an unqualified offer of refund, repair, or replacement, the customer's preference should prevail.

USE OF TEST OR SURVEY DATA
Article #20
All test or survey data referred to in advertising should be valid and reliable as to source and methodology, and should support the specific claim for which it is cited. Advertising claims should not distort test or survey results or take them out of context.

TESTIMONIALS AND ENDORSEMENTS

Article #21

Testimonials and endorsements in any media (including but not limited to such comments on a company's website and via social networking sites, online message boards, blogging and "word-of-mouth" marketing) should be used only if they:

a. Are authorized by the person quoted;

b. Are accurate, genuine and related to the experience of the person giving them, both at the time made and at the time of the promotion, and disclose the expertise of the endorser in terms of whether he or she is an expert for the purposes of the advertisement or simply a consumer endorser;

c. Are not taken out of context so as to distort the endorser's opinion or experience with the product or service;

d. Clearly and conspicuously disclose any material connections between the endorser and marketer, which the consumer would not expect. A material connection refers to a connection between the endorser and marketer that materially affects the weight or credibility of the endorsement, such as payments or free products, or an employer/employee relationship; and

e. Clearly and conspicuously disclose the generally expected, or typical, results/performance of the advertised products or services, if the claims made are not typical of what a user could expect under normal circumstances.

A marketer should be able to provide prior and adequate substantiation, including providing reliable scientific evidence, as necessary, for any claims of efficacy (i.e. whether the product/service will actually do what the marketer says it will do, typicality (i.e. whether the typical consumer will have an experience like that of the endorser), and environmental benefit. The marketer should also be able to substantiate that the endorser was a bona fide user of the product at the time of the endorsement.

Additionally, marketers should ensure that their celebrity endorsers disclose their relationships with marketers when making endorsements outside the context of traditional advertisements, such as on talk shows or in social media, and they should not knowingly make statements that are false or unsubstantiated.

For purposes of this article, the terms "testimonial" and "endorsement" refer to an advertising or marketing message made in any channel that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsor of the message, even if the views expressed by that party are identical to those of the sponsor. Testimonials and endorsements can be verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization.

Sweepstakes

USE OF THE TERM "SWEEPSTAKES"
Article #22
Sweepstakes are promotional devices by which items of value (prizes) are awarded to participants by chance without the promoter's requiring the participants to render something of value (consideration) to be eligible to participate. The co-existence of all three elements -- prize, chance and consideration -- in the same promotion constitutes a lottery. It is illegal for any private enterprise to run a lottery without specific governmental authorization.

When skill replaces chance, the promotion becomes a skill contest. When gifts (premiums or other items of value) are given to all participants independent of the element of chance, the promotion is not a sweepstakes. Promotions that are not sweepstakes should not be held out as such.

Only those promotional devices that satisfy the definition stated above should be called or held out to be a sweepstakes.

NO PURCHASE OPTION
Article #23
Promotions should clearly state that no purchase is required to win sweepstakes prizes. They should not represent that those who make a purchase or otherwise render consideration with their entry will have a better chance of winning or will be eligible to win more or larger prizes than those who do not make a purchase or otherwise render consideration. The method for entering without ordering should be easy to find, read, and understand. When response devices used only for entering the sweepstakes are provided, they should be as easy to find as those utilized for ordering the product or service.

CHANCES OF WINNING
Article #24
No sweepstakes promotion, or any of its parts, should represent that a recipient or entrant has won a prize or that any entry stands a greater chance of winning a prize than any other entry when this is not the case. Winners should be selected in a manner that ensures fair application of the laws of chance.

PRIZES
Article #25
Sweepstakes prizes should be advertised in a manner that is clear, honest, and complete so that the consumer may know the exact nature of what is being offered. For prizes paid over time, the annual payment schedule and number of years should be clearly disclosed.

Photographs, illustrations, artwork, and the situations they represent should be accurate portrayals of the prizes listed in the promotion.

No award or prize should be held forth directly or by implication as having substantial monetary value if it is of nominal worth. The value of a non-cash prize should be stated at regular retail value, whether actual cost to the sponsor is greater or less.

All prizes should be awarded and delivered without cost to the participant. If there are certain conditions under which a prize or prizes will not be awarded, that fact should be disclosed in a manner that is easy to find, read, and understand.

PREMIUMS

Article #26

Premiums should be advertised in a manner that is clear, honest, and complete so that the consumer may know the exact nature of what is being offered.

A premium, gift or item should not be called or held out to be a "prize" if it is offered to every recipient of or participant in a promotion. If all participants will receive a premium, gift, or item, that fact should be clearly disclosed.

DISCLOSURE OF RULES

Article #27

All terms and conditions of the sweepstakes, including entry procedures and rules, should be easy to find, read, and understand. Disclosures set out in the rules section concerning no purchase option, prizes, and chances of winning should not contradict the overall impression created by the promotion.

The following should be set forth clearly in the rules:

- No purchase of the advertised product or service is required in order to win a prize
- A purchase will not improve the chances of winning
- Procedures for entry
- If applicable, disclosure that a facsimile of the entry blank or other alternate means (such as a 3"x 5" card) may be used to enter the sweepstakes
- The termination date for eligibility in the sweepstakes. The termination date should specify whether it is a date of mailing or receipt of entry deadline
- The number, retail value (of non-cash prizes), and complete description of all prizes offered, and whether cash may be awarded instead of merchandise. If a cash prize is to be awarded by installment payments, that fact should be clearly disclosed, along with the nature and timing of the payments
- The estimated odds of winning each prize. If the odds depend upon the number of entries, the stated odds should be based on an estimate of the number of entries
- The method by which winners will be selected
- The geographic area covered by the sweepstakes and those areas in which the offer is void
- All eligibility requirements, if any
- Approximate dates when winners will be selected and notified
- Publicity rights regarding the use of winner's name
- Taxes are the responsibility of the winner
- Provision of a mailing address to allow consumers to receive a list of winners of prizes over $25.00 in value

Fulfillment

UNORDERED MERCHANDISE OR SERVICE
Article #28
Merchandise or services should not be provided without having first received the customer's permission. The exceptions are samples or gifts clearly marked as such, and merchandise mailed by a charitable organization soliciting contributions, as long as all items are sent with a clear and conspicuous statement informing the recipient of an unqualified right to treat the product as a gift and to do with it as the recipient sees fit, at no cost or obligation to the recipient.

PRODUCT AVAILABILITY AND SHIPMENT
Article #29
Direct marketers should offer merchandise only when it is on hand or when there is a reasonable expectation of its timely receipt.

Direct marketers should ship all orders according to the terms of the offer or within 30 days where there is no promised shipping date, unless otherwise directed by the consumer, and should promptly notify consumers of any delays.

DRY TESTING
Article #30
Direct marketers should engage in dry testing only when the special nature of the offer is made clear in the promotion.

Collection, Use, and Maintenance of Marketing Data

For purposes of the *Guidelines for Ethical Business Practice*, the following definitions are used:

Consumer refers to the subject of the data.

Marketing data means actual or inferred information consistent with a person's commercial or charitable inquiry or transaction, or market research or market survey information. Such information can be derived from either a direct contact or marketing partnership when linked to a person's name, postal or email address, or telephone number, or any other personally identifiable information. When obtained from a publicly available source, information (including public record information), not combined with other information, is not marketing data.

Marketing purpose means any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to allow or induce consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers.

PROVIDING CONSUMER CHOICE & THE COLLECTION, USE, AND TRANSFER OF PERSONALLY IDENTIFIABLE DATA

Article #31
This article is applicable to all addressable media and applies to senders of marketing offers or fundraising solicitations:

A. Providing Consumer Choice and Privacy Notice Information:

- Marketers should provide consumers a point of contact where they may add, modify or eliminate direct marketing communications from a company or an organization and obtain the company or organization's privacy policy with regards to collection, use and transfer of their information. The point of contact information (such as a website, telephone number or address) should appear upon or within each written marketing offer, or upon request by the consumer.

- Online marketers should provide notice in accordance with Article #38.

- Email marketers should provide notice in accordance with Article #39 and the CAN-SPAM Act.

- Mobile marketers must obtain prior express consent and provide a notice in accordance with Articles #54 and #55.)

- The point of contact notice should: be easy for the consumer to find, read, understand, and act upon.

- A marketer periodically should provide existing customers with notice of its policy concerning the rental, sale, exchange, or transfer of data about them and of the opportunity to opt out of the marketing process. All such opt-out requests should be honored promptly.

- An in-house suppression request from a consumer should be interpreted as meaning that the consumer also wants to opt out of the transfer of his or her personal information

- Upon request by a consumer, a marketer should disclose the source from which it obtained personally identifiable information about that consumer.

B. Processing Consumer Choices:

- A consumer's request for elimination of future marketing offers should be processed:
  - within 30 days of the consumer's request or as required by law, whichever is the shorter time period
  - for a period of at least three years from the date of receipt of the request

- Where an affiliate, division, or subsidiary markets under a different company or brand name, and is perceived as separate by the consumer, each corporate entity or brand should separately honor requests received by it.

- A marketer should establish internal policies and practices that assure accountability for honoring consumer preference requests regardless of the marketing channel, in compliance with this guideline, and at no cost to consumers. Should those policies substantially change, the marketer has an obligation to inform consumers of that change prior to the rental, sale, exchange, or transfer of data, and to offer consumers an opportunity to opt out of the marketing process at that time.

C. DMAchoice and Related Consumer Choice Files:

- For each prospecting list that is rented, sold, exchanged, or transferred, the names registered on the applicable DMAchoice (DMA's consumer choice web site) name-removal lists should be removed prior to use.

- DMAchoice name-removal lists include:

    - the relevant categorical opt-out mailing lists for Catalog, Magazine, Pre-screened Credit Offers or Other categories, as well as future categories designated by the DMA; and

    - the Email Preference Service and Telephone Preference Service, as well as future DMA preference service lists.

- The use of the DMAchoice name-removal lists and preference service lists is not required for the company's and organization's existing customer or donor lists, only for prospects.

- Members should be listed on the DMAchoice site to demonstrate their compliance with the DMA Guidelines and to provide a direct connection to consumers for further choice requests.

    - The company or organization listed must provide the correct point of contact where the consumer may exercise their marketing preferences. (*See Also* Article #9 Accessibility: Every offer should clearly identify the marketer's name and street address or telephone number, or both, at which the individual may obtain service and exercise their marketing preferences.)

  In all instances, the most recent *monthly* release of the relevant DMAchoice file should be used.

  In addition to adhering to these guidelines, a marketer should cooperate with DMA when requested in demonstrating its compliance with the Commitment to Consumer Choice and the marketer's own consumer preference policies.

PERSONAL DATA
Article #32
Marketers should be sensitive to the issue of consumer privacy and should only collect, combine, rent, sell, exchange, or use marketing data. Marketing data should be used only for marketing purposes.

Data and selection criteria that by reasonable standards may be considered sensitive and/or intimate should not be disclosed, be displayed, or provide the basis for lists made available for rental, sale or exchange when there is a reasonable expectation by the consumer that the information will be kept confidential.

Credit card numbers, checking account numbers, and debit account numbers are considered to be personal information and therefore should not be transferred, rented, sold, or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.

Social Security numbers are also considered to be personal information and therefore should not be transferred, rented, sold, or exchanged for use by a third party when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of Social Security numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers. Social Security numbers, however, are used by direct marketers as part of the process of extending credit to consumers or for matching or verification purposes.

HEALTH INFORMATION PRIVACY & PROTECTION
Article #33

Nothing in these guidelines is meant to prohibit research, marketing, or other uses of health-related data which are not personally identifiable, and which are used in the aggregate since there are no restrictions on the use of de-identified health information.

Health Information Data Protection:

Protected Health Information:
Protected health information is individually identifiable information held or transmitted by a covered entity (a health plan, or a health care clearinghouse, or a health care provider) or its business associate in any form or media, whether written or oral. This information includes demographic information collected from an individual that can reasonably be used to identify the individual. Identifiers can include the individual's name, specific dates such as birth, admission, discharge, death, medical record number, photographs, city, zip code or geographic or other identifiers held as protected health data. Additionally, protected health information is information created or received by a health care provider, health plan, employer, or health care

clearinghouse; and relates to the past, present or future physical or mental health condition of the individual.

These principles apply to any individual or entity that collects, maintains, uses, and/or transfers such protected health information for marketing purposes, whether or not marketing is a primary purpose.

This includes business associates (including the subcontractors of the business associate) who perform functions or services for covered entities that involve the use of protected health information.

Such business associates may only use the protected health information if they have a written agreement to use such protected information for the covered entity's own marketing purposes.

Principles:

1. Protected health information gained in the context of a relationship between an individual and health or medical care providers or medical treatment facilities should not be transferred for marketing purposes without that individual's specific prior consent through a written signed authorization form. All marketing communications (receipt of financial remuneration in exchange for the communication) must have such prior written authorization and must include a statement that the organization will be paid for the marketing activity if the marketing includes direct or indirect payment from a third party.

   Exceptions:
   -Covered entities may provide offers for products and services in face-to-face encounters (this is to protect the doctor-patient relationship.)
   -Health and wellness communications may be provided by the covered entity about its own products and services.
   -General wellness and prevention communications may be provided.

2. Individually identifiable health-related information gained in the context of a relationship between individuals and health care providers or medical treatment facilities (as defined above) or other covered entities should not be used to contact those individuals for marketing purposes without the required prior written authorization.

3. Individually identifiable health-related information volunteered by individuals, and gathered outside of the relationship between individuals and covered entities, should be considered sensitive and personal in nature. Such information should not be collected, maintained, used, and/or transferred for marketing purposes unless those individuals receive, at the time the information is collected, a clear notice of the marketer's intended uses of the information, whether the marketer will transfer the information to third parties for further use, the name of the collecting organization, and the opportunity to opt out of transfer of the information. Such information includes, but is not limited to, information volunteered by individuals when responding to surveys and questionnaires. The notice should be easy to find, read, and understand.

4. Individually identifiable health-related information inferred about individuals, and gathered outside of the relationship between individuals and covered entities, should also be considered sensitive and personal in nature. This is information based on individual purchasing behavior. Such information includes, but is not limited to, data captured by inquiries, donations, purchases, frequent shopper programs, advertised toll-free telephone numbers, or other consumer response devices. Any entity, including a seller of over-the-counter drugs, which uses inferred health-related information should promptly provide the individual with notice and the opportunity to opt out of any transfer of the data for marketing purposes.

5. Marketers using individually identifiable health-related information should provide both the source and the nature of the information they have about that individual upon the request of that individual and the receipt of that individual's proper identification.

6. Individuals should not be required to release individually identifiable health-related information about themselves or to provide written authorizations to allow their health information be used for marketing purposes as a condition of receiving insurance coverage, treatment, services or information, or otherwise completing their health care-related transaction.

7. The text, appearance, and nature of solicitations directed to individuals on the basis of their health-related information should take into account the sensitive nature of such information.

8. Marketers should ensure that safeguards are built into their systems to protect individually identifiable health-related information from unauthorized access, alteration, abuse, theft, or misappropriation. Employees who have access to individually identifiable health-related information should agree in advance to use such information only in an authorized manner.

9. If individually identifiable health-related information is transferred from one direct marketer to another for a legitimate marketing purpose as established by written agreement, the transferor should arrange the most strict security measures to assure that unauthorized access to the information is not likely during the transfer process. Transfers of individually identifiable health-related information should not be permitted for any marketing uses that are in violation of any of DMA's *Guidelines for Ethical Business Practice*, state or federal laws.

10. **Fundraising exception for limited protected health information:** Entities are allowed to use or disclose to a business entity or institution or institutionally-related foundation limited protected health information (demographics and dates of care) about an individual for that entity's fundraising without a prior written authorization. However, the fundraising entity must ensure its fundraising material includes an opt-out notice that is clear and conspicuous, and if it is over the phone, an opt-out disclosure must be made. If the individual does opt-out, no more fundraising communications across all marketing channels may be made.

For the opt-out notice:

-the opt-out notice must be included in each fundraising communication;
-the opt-out method must be free;
-the entity cannot condition the treatment or services on an individual's choice to receive fundraising communication.

PROMOTION OF MARKETING LISTS
Article #34
Any advertising or promotion for marketing lists being offered for rental, sale, or exchange should reflect the fact that a marketing list is an aggregate collection of marketing data. Such promotions should also reflect a sensitivity for the consumers on those lists.

MARKETING LIST USAGE
Article #35
List owners, brokers, managers, and users of marketing lists should ascertain the nature of the list's intended usage for each materially different marketing use prior to rental, sale, exchange, transfer, or use of the list. List owners, brokers, and managers should not permit the rental, sale, exchange, or transfer of their marketing lists, nor should users use any marketing lists for an offer that is in violation of these guidelines. Mobile opt-in lists should not be rented or exchanged for the purpose of sending mobile marketing solicitations to those on the list, without obtaining prior express consent from those on the list.

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.

DATA SECURITY
Article #37
The protection of personally identifiable information is the responsibility of all organizations. Therefore, organizations should assume the following responsibilities to provide secure transactions and to protect databases containing personally identifiable information against unauthorized access, alteration, or dissemination of data:

- Establish written data security policies and procedures reflective of current business practices (including written policies and procedures related to personal devices v. company-provided devices.) Organizations should ensure there are reasonable information security policies and practices that seek to assure the uninterrupted security of information systems within their organizations.

- Provide data security training for relevant staff. Organizations should create and implement reasonable staff procedures, training, and responsiveness measures to protect personally identifiable information handled by relevant staff in the everyday performance of their duties.

- Train staff that use their own devices on steps designed to help prevent unauthorized access to the organization's data as well as educate them about the inherent risks, and ensure the organization has reasonable data security policies and safeguards in place for such devices.

- Monitor and assess data security safeguards periodically. Organizations should employ and routinely assess protective physical safeguards and technological measures within their organizations, including data retention, destruction, deletion practices, and the monitoring and analysis of systems logs in support of information security.

- Include contractual safeguards. Organizations should contractually require all business partners and service providers that handle personally identifiable data to ensure that their policies, procedures, and practices maintain a level of security consistent with or higher than the organizations applicable information security policies, including partners' own employees and contractors accessing data through their own devices.

- Set up a data security breach readiness plan. Organizations should develop and maintain a data security breach readiness plan reasonable for the size and nature of the organization, their level of data collection, and type of data collected.

    - Include the following as reasonable within their organization:
        - Periodic audit of data retention. What is stored, on what servers, and who has access?
        - Employ appropriate data loss prevention technologies.
        - Employ an appropriate data minimization plan including a data destruction and purge process.
        - Maintain an inventory of system access and credentials.
        - Segment and isolate networks based on business function to avoid compromising sensitive personal information that is used in a network.
        - Create a reasonable incident response plan including vendor and law enforcement contacts as well as notification requirements.
        - Maintain a reasonable and ongoing employee training program.
        - Provide the appropriate one way encryption.
        - Maintain a reasonable password policy including minimum standards for passwords complexity and changes.

- If a data security breach occurs, immediately inform compliance or legal staff as identified in your data breach readiness plan. Organizations should, in the event of a security breach where there is a reasonable likelihood of material harm to consumers, inform those consumers who may be affected in the most expedient time practical (or as required by state laws) unless requested by legal authorities to delay such notification due to an ongoing criminal investigation.

- For email, organizations should implement the appropriate email authentication protocol (SPF, DKIM, DMARC as appropriate) to help reduce the risk of spoofed emails.

- Organizations collecting sensitive data must ensure added data security measures are taken to protect such data online. The appropriate digital certificate should be employed meaning the Extended Validation Secure Socket Layer Certificates (EV SSL) should be used on all relevant pages of sites requesting sensitive data.

Digital Marketing

ONLINE INFORMATION & ONLINE BEHAVIORAL ADVERTISING
Article #38
This Article addresses the collection of personally identifiable information by websites for online marketing generally, and the collection and use of information for online behavioral advertising purposes, as defined in the Glossary of Terms.

General Notice to Online Visitors
If your organization operates an online site and/or is engaged in online behavioral advertising, you should make your information practices available to visitors in a prominent place on your website's home page or in a place on your website that is easily accessible from the home page.

In addition, if your organization offers a mobile application, you should make your information practices reasonably accessible to the consumers of your application.

This notice about information practices should be easy to find, read, and understand. Visitors should be able to comprehend the scope of the notice and how they can exercise their choices regarding use of personally identifiable information or information used for online behavioral advertising purposes. The notice should be available prior to or at the time personally identifiable information or information used for online behavioral advertising purposes is collected.

Your organization and its postal address, and the website(s) or mobile application(s) to which the notice applies, should be identified so visitors know who is responsible for the website or mobile application. You also should provide specific contact information so visitors can contact your organization for service or information.

If your organization collects personally identifiable information from visitors your notice should include:

- The nature of the information collected online for marketing purposes, and the types of uses you make of such information, including uses for online behavioral advertising purposes;
- The use(s) of such information, including whether you transfer information to third parties for use by them for their own marketing or online behavioral advertising purposes and the mechanism by which consumers can exercise choice not to have such information transferred;
- Whether personally identifiable information is collected by, used by, or transferred to agents (entities working on your behalf) as part of the business activities related to the

visitor's actions on the site or application, including to fulfill orders or to provide information or requested services;
- Whether you use cookies or other passive means of information collection, and whether such information collected is for internal purposes or transferred to third parties for marketing purposes, including online behavioral advertising purposes;
- What procedures your organization has put in place for accountability and enforcement purposes; and
- That your organization maintains appropriate physical, electronic, and administrative safeguards to protect information collected online and keeps your personal information secure.
- If your organization maintains a process for a consumer who uses or visits your website or mobile application to review and request changes to any of their personally identifiable information that is collected through the website or mobile application, you should describe that process.
- If the notice is for a mobile application, the notice should include applicable information under Article #55 and Article #58 below.
- The effective date of the notice should be provided.

If you knowingly permit network advertisers to collect information on their own behalf or on behalf of their clients on your Website or mobile application, you should also provide notice of fact that these types of entities collect information from your site or application and a link to a mechanism by which a visitor can exercise their choice of not having such information collected by these types of entities if they provide such choice. (Network advertisers are third parties that attempt to target online advertising and make it more relevant to visitors based on Web traffic information collected over time across the websites of others or application usage collected over time across applications offered by others.)

In addition, marketers should refer to Article #32 (Personal Data) specifically to assure that marketing data are used only for marketing purposes.

Third-Party Notice for Online Behavioral Advertising

When information is collected from or used on a website or mobile application for online behavioral advertising purposes, visitors should be provided with notice (easy to find, read and understand) about the third party's policies for online behavioral advertising. Third parties, as defined in the Glossary of Terms, should provide notice in one of the following ways:

- through a clear, meaningful, and prominent link described in or proximate to the advertisement delivered on the Web page or through the application where information is collected;
- on DMA's approved website(s), such as DMAchoice.org or another comprehensive industry-developed website(s), that is linked from the disclosure that describes the fact that information is being collected for online behavioral advertising purposes;
- on the web page where the information is collected if there is an arrangement with the website operator for the provision of such notice;
- if agreed to by the operator of the website(s) on its web page disclosing notice and choice regarding information collected for online behavioral advertising purposes.

Consumer Choice for Third-Party Online Behavioral Advertising
A third party should provide consumers with the ability to exercise choice with respect to the collection and use of information for online behavioral advertising purposes or the transfer of such information to a non-affiliate for such purposes. Such choice should be available through the notice options as detailed above.

Material Changes to Existing Policies
If your organization's policy changes materially with respect to the sharing of personally identifiable information with third parties including but not limited to changes for online behavioral advertising purposes, you should update your policy and give consumers conspicuous notice to that effect, offering an opportunity for individuals to select their preferences. Prior to making a materially different use of information collected from an individual for online behavioral advertising purposes, and before notice of your organization's policy change is given, organizations should obtain informed consent to such a new marketing use from the consumer.

Honoring Choice
You should honor a website visitor's choice regarding use and transfer of personally identifiable information made in accordance with your stated policy. If you have promised to honor the visitor's choice for a specific time period, and if that time period subsequently expires, then you should provide that visitor with a new notice and choice. You should provide choices online. You may also offer choice options by mail or telephone.

Providing Access
You should honor any representations made in your online policy notice regarding access.

Information Security
Your organization should maintain appropriate physical, technical and administrative safeguards and use appropriate security technologies and methods to protect information collected or used online, and to guard against unauthorized access, alteration, or dissemination of personally identifiable information during transfer and storage. Your procedures should require that employees and agents of your organization who have access to personally identifiable information use and disclose that information only in a lawful and authorized manner. Organizations should retain information that is collected and used for online behavioral advertising purposes only for as long as necessary to fulfill a legitimate business need, or as required by law.

Visitors Under 13 Years of Age
If your organization has a site or a mobile application directed to children under the age of 13 or collects personally identifiable information from visitors known to be under 13 years of age, your website should take the additional steps required by the *Marketing to Children* Articles of the *Guidelines for Ethical Business Practice* and inform visitors that your disclosures and practices are subject to compliance with the Children's Online Privacy Protection Act ("COPPA"). In addition, an organization should not engage in online behavioral advertising directed to children where it has actual knowledge that the children are under the age of 13, unless compliant with COPPA and these Guidelines.

Health and Financial Information
Entities should not collect and use financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for online behavioral advertising purposes without prior express consent and unless compliant with the Health Insurance Portability & Accountability Act ("HIPPA") health laws and regulations, financial rules and regulations, and these Guidelines.

Accountability
There should be a meaningful, timely, and effective procedure through which your organization can demonstrate adherence to your stated online information practices. Such a procedure may include: (1) self or third-party verification and monitoring, (2) complaint resolution, and (3) education and outreach. This can be accomplished by an independent auditor, public self-certification, a third-party privacy seal program, a licensing program, and/or membership in a trade, professional or other membership association with a self-regulatory program.

Service Provider Treatment of Online Behavioral Advertising Information
A service provider, as defined in the Glossary of Terms, should not collect and use information for online behavioral advertising purposes without consent and should provide an easy-to-use ongoing means to withdraw consent to the collection and use of that information for online behavioral advertising purposes.

In addition, a service provider should take the following steps regarding information collected and used for online behavioral advertising purposes:

1. Alter, anonymize, or randomize (e.g., through "hashing" or substantial redaction) any personally identifiable information or unique identifier in order to prevent the information from being reconstructed into its original form in the ordinary course of business.

2. Disclose in the notice described above the circumstances in which information is collected and used for online behavioral advertising purposes.

3. Take reasonable steps to protect the non-identifiable nature of information if and when it is distributed to non-affiliates, including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the information, and obtaining satisfactory written assurance that such non-affiliates will not attempt to re-construct the information and will use or disclose the anonymized information only for purposes of online behavioral advertising or other uses as specified to users. This assurance will be considered satisfied if a non-affiliate does not have any independent right to use the information for its own purposes under a written contract.

4. Take reasonable steps to ensure that any non-affiliate that receives anonymized information will itself ensure that any other non-affiliate to which such information is disclosed agrees to the restrictions and conditions set forth in this subsection. This obligation is also considered satisfied if a non-affiliate does not have any independent right to use the data for its own purposes under a written contract.

Glossary of Terms

Ad Delivery -- means the delivery of online advertisements or advertising-related services using ad reporting data. Ad delivery does not include the collection and use of ad reporting data when such data are used to deliver advertisements to a computer or device based on the preferences or interests inferred from information collected over time and across non-affiliate sites because this type of collection and use is covered by the definition of online behavioral advertising.

Ad Reporting -- refers to the logging of page views on a website(s) or the collection or use of other information about a browser, operating system, domain name, clickstream within a site, date and time of the viewing of the Web page or advertisement, and related information for purposes including but not limited to: statistical reporting in connection with the activity on a website(s); Web analytics and analysis for improved marketing and better site design; and logging the number and type of advertisements served on a particular website(s).

Affiliate -- refers to an entity that controls, is controlled by, or is under common control with, another entity.

Consent -- means an individual's action in response to a clear, meaningful and prominent notice regarding the collection and use of data for online behavioral advertising purposes. Informed consent is based on information provided to an individual that allows them to select their preferences, prior express consent means consent required from an individual prior to any marketing communication from the marketer or others.

Contextual Advertising -- Advertising based on a consumer's current visit to a Web page or search query. Online behavioral advertising, as defined in this Article's Glossary of Terms, does not include contextual advertising.

Control -- of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the control of another entity and thus be treated as a first party under these principles, the entity must adhere to online behavioral advertising policies that are not materially inconsistent with the other entity's policies.

First Party -- is the entity that is the owner of the website, or those of its affiliates, and has control over the website with which the consumer interacts.

Online Behavioral Advertising -- means the collection of information from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites for the purpose of using such information to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors. Online behavioral advertising does not include the activities of first parties, ad delivery or ad reporting, or contextual advertising (i.e. advertising based on the

content of the Web page being visited, a consumer's current visit to a Web page, or a search query). The activities of search engines fall within the scope of online behavioral advertising to the extent that they include collection of data regarding Web viewing behaviors over time and across non-affiliate websites in order to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.

Personally Identifiable Information & Non-Personally Identifiable Information -- for purposes of this Article, personally identifiable information refers to name, address, or other information that identifies a specific individual; non-personally identifiable information (non-PII) refers to information, such as a computer's IP address, that does not tie the information to a specific individual. Non-personally identifiable information collected by third parties from websites for online behavioral advertising should be combined with personally identifiable information collected about an individual for marketing purposes only with that individual's consent, unless the individual was provided with notice and choice with respect to such potential combination at the time the non-personally identifiable information was collected and did not opt out.

Service Provider -- refers to an organization that collects and uses information from all or substantially all URLs traversed by a Web browser across websites for purposes of online behavioral advertising. Examples of service providers in this context are internet access service providers and providers of desktop applications software such as Web browser "tool bars."

Third Party -- an entity is a third party to the extent that it engages in online behavioral advertising on a non-affiliate's website.

MOBILE SERVICE COMMERCIAL MESSAGE SOLICITATIONS (MSCMs) DELIVERED TO A WIRELESS DEVICE
Article #39

A Mobile Service Commercial Message (MSCM) is a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of a commercial mobile service. Marketers sending MSCMs messages should obtain prior express consent from recipients and should abide by CAN-SPAM, the Federal Communications Commission's Wireless Email Rule, DMA Guidelines for Online & Mobile Marketing, and any additional federal and state regulations.

COMMERCIAL SOLICITATIONS ONLINE
Article #40

1. DEFINITION:
This article refers to addressable commercial solicitations initiated online by marketers (or their affiliates); including commercial solicitations sent to an individual's email address or another "direct contact point." For purposes of this article, a "direct contact point" is defined as a user ID or other unique identifier at which an individual can be communicated with online or via a mobile Internet device. This may include, for

example, a text message number, personalized activity feed identifier (e.g., “twitter” ID), or user ID for postings on or to a personal social network profile page.

Nothing in this Article or definition is meant to restrict or prohibit the use of aggregated or anonymized data pertaining to direct contact points, the use of profile data for online behavioral advertising (OBA,) or online banner advertising.

2. CHANNEL APPROPRIATE CONSENT:
Marketers (or their affiliates) may initiate commercial solicitations online to customers or prospects under the following circumstances

- individuals have given their channel-appropriate consent to the marketer (including, but not limited to, through the terms of a social media platform) to receive solicitations online, or
- Individuals did not opt out after the marketer has given notice of the opportunity to opt out from receiving solicitations online, or
- The marketer has received assurance from the third party list provider that the individuals whose email addresses or other direct contact points appear on that list:
    - have given their channel-appropriate consent to receive solicitations online, or
    - have already received notice of the opportunity to opt out from receiving online solicitations and have not opted out, and DMA’s Email Preference Service (E-MPS) suppression file was used by the third party.

3. CHANNEL APPROPRIATE CHOICE:

Marketers should furnish individuals with the appropriate notice or a point of contact and an Internet-based mechanism individuals can use to:

- Request that the marketer not send them future online solicitations and
- Request that the marketer not rent, sell, or exchange their email addresses or other direct contact point data for online solicitation purposes.

If individuals request that they be added to the marketer’s in-house suppression list, then the marketer may not rent, sell, or exchange their email addresses or other direct contact point data 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 solicitation.

Marketers that rent, sell, or exchange personally identifiable information need to provide individuals with notice of a mechanism to opt out of personally identifiable information transfer to third-party marketers.

Solicitations sent via email 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

email 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.

EMAIL AUTHENTICATION

Article #41

Marketers that use email for communication and transaction purposes should adopt and use identification and authentication protocols.

USE OF SOFTWARE OR OTHER SIMILAR TECHNOLOGY INSTALLED ON A COMPUTER OR SIMILAR DEVICE

Article #42

Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (e.g., relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

*Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar
- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including Web beacons, are not governed by this Guideline. Article #38 provides guidance regarding cookies and other passive means of data collection.

SOCIAL MEDIA & ONLINE REFERRAL MARKETING
Article #43

1. DEFINITION:
Social media marketing is the use of online communities and/or social networks (via services, websites or platforms – each a "channel") to send a commercial marketing message to an individual and/or to that individual's own network. (Social media involves user interactions which the individual has agreed to display and to be shared.) Online referral marketing is a technique marketers use to generate new marketing leads.

Typically, the online marketer encourages an individual to do the following:

1. Forward a commercial solicitation to another individual, or
2. Provide the marketer with personally identifiable information, such as name and/or address/email address, about the referred individual so the marketer may contact that person directly, or
3. Share or display a social ad and/or otherwise engage with a social media network or channel by, for example, "friending" (an invitation to establish a social media relationship), posting or otherwise sharing or displaying the ad on or via a social media channel (e.g., an activity feed such as tweeting). This interaction may involve a request from the marketer that the individual provide profile or social data about himself/herself or others in his/her network. Profile data may include, but is not limited to: name, age, gender, location, expressed personal interests and preferences, and photos. Profile data also extends to what is known as the "social graph," which are explicit online connections and interactions between individuals ("friends").

2. USING INFORMATION PROVIDED BY THE INDIVIDUAL AND/OR ABOUT OTHERS:

If personally identifiable information about an individual is given to a marketer through social media channels and/or online referral marketing rather than directly from an individual, then the following steps should be taken:

A marketer should not use personally identifiable information about a referred individual provided online by another individual unless:

- The marketer has previously disclosed, in a clear and conspicuous manner, to the referring individual the intended uses of the information (Note: All notices and disclosures referenced in this article should be made in clear and conspicuous manner and in keeping with DMA's Ethical Guidelines.);

- The marketer has disclosed to the referring individual that his or her own contact information will be provided to those individuals they have referred to the marketer;
- The marketer discloses to the referred person the fact that his or her contact information was obtained from another individual. The marketer should make the referring person's contact information available in the first communication to the prospect; and
- The marketer provides channel appropriate choices to the referred individual regarding receiving future communications. (Note: The frequency and type of choice provided (e.g., first communication vs. every communication) must be appropriate for the channel being used to contact the individual. For example, email communications must include an opt-out notice and choice in every communication.)

Since marketers have not had a direct contact with the referred individual, marketers should not contact referred individuals who are on their in-house suppression lists.

Marketers should not sell, rent, share, transfer, or exchange a referred email address or referred personally identifiable information unless they receive prior permission from each referred person to do so.

Prior express consent must be obtained before initiating contact using a marketing channel or platform for which a referred individual will incur a fee for receipt of the marketing message, such as premium-rate text messaging via a mobile device. (Articles #54-#58.) In addition, online referral marketers offering an incentive should adhere to Article #39 (Mobile Service Commercial Messages).

3. SENDING COMMERCIAL SOLICITATIONS VIA INDIVIDUALS' SOCIAL MEDIA NETWORKS:

If a marketer is contacting an individual to send marketing messages to that individual's network of contacts, each of the following steps should be taken:

- A marketer should obtain an individual's prior consent to participate in the social media marketing process whereby the marketer is added as a "friend" or a contact to be shared with the individual's other social media contacts;
- Profile data that contains personally identifiable information provided by an individual on a social networking site should not be shared with third parties without that individual's prior consent unless the user has agreed to post or populate such information in an unrestricted publicly accessible location;
- If tracking data is being collected as part of the social media marketing process for purposes of online behavioral advertising, please refer to Article #38;
- If a social or interactive advertising application (incorporating user-generated content or user interactions that the individual has consented to being shared) is being distributed to the individual's contacts, a preview should be provided to that individual for review and approval before it is distributed by the marketer to that individual's contacts. The recipient of the ad should be provided with an opportunity

to opt out of receiving future communications from the marketer and having his/her information shared; and

- Marketers should not retain personally identifiable information used for social marketing purposes except for marketing purposes, and should not share such data with any third party without the individual's prior consent unless the user has agreed to post or populate such information in an unrestricted publicly accessible location.

Marketers using testimonials and endorsements in any media, including but not limited to social media channels (e.g., online message boards, blogging, etc.) and "word-of-mouth" marketing, should comply with Article #21 – Testimonials & Endorsements – of these Guidelines. Additionally, where marketing to children is permitted by law, marketers using social media channels should comply with Articles #13 - #16 of these Guidelines and ensure the marketing is suitable for the child, taking into account the age range, knowledge, sophistication, and maturity of their intended audience.

4. OPERATORS OF SOCIAL MEDIA PLATFORMS & FORUMS:

In addition to complying with the aforementioned items, operators of social media networks, platforms or other social media forums should:

- Post their privacy policy in a prominent location on their site so that it is clear and conspicuous;
- Advise individual users about their privacy policies, data deletion policy and the steps users should follow to change their privacy settings, to deactivate or to delete their accounts;
- Prevent games, quizzes and other applications developed by third parties from accessing personally identifiable information from an individual user until the marketer has provided clear and conspicuous notice to the individual before accessing their information (notice must include an opportunity to refuse marketing communications associated with the application), or obtains prior consent from that user for each category of personal information accessed.

EMAIL APPENDING TO CONSUMER RECORDS
Article #44

Definition of email address appending: Email address appending is the process of adding a consumer's email address to that consumer's record. The email address is obtained by matching those records from the marketer's database against a third-party database to produce a corresponding email address.

A marketer should append a consumer's email address to its database only when the consumer gives a marketer permission to add his or her email address to the marketer's database; or

1. There is an established business relationship with that consumer either online or offline, and

2. The data used in the append process are from sources that provided notice and choice regarding the acceptance of receiving third-party email offers and where the consumer did not opt out, and
3. Reasonable efforts are taken to ensure the appending of accurate email addresses to the corresponding consumer records

Marketers should not send emails to appended email addresses that are on their in-house email suppression files. Marketers should not send Mobile Service Commercial Messages (MSCMs) to appended email addresses that belong to wireless handsets or devices unless the recipient has provided prior express authorization to receive such messages from the sender. A marketer should not sell, rent, transfer, or exchange an appended email address of a consumer unless it first offers notice and choice to the consumer. All messages to an email appended address should include a notice and choice to continue to communicate via email.

Marketers should have in place appropriate record-keeping systems to ensure compliance with these guidelines.

Telephone Marketing to Landline & Wireless Devices

REASONABLE HOURS
Article #45
Telephone contacts, whether to a landline or wireless handset or device, should be made during reasonable hours as specified by federal and state laws and regulations.

TAPING OF CONVERSATIONS
Article #46
Taping of telephone conversations by telephone marketers should only be conducted with notice to or consent of all parties, or the use of a beeping device, as required by applicable federal and state laws and regulations.

RESTRICTED CONTACTS
Article #47
A marketer should not knowingly call or send a voice solicitation message to a consumer who has an unlisted or unpublished telephone number except in instances where that specific number was provided by the consumer to that marketer for that purpose. A marketer should maintain an in-house Do-Not-Call list and refrain from calling numbers for solicitation purposes that are on the marketer's in-house Do-Not-Call list.

A marketer should not knowingly call a wireless device, except in instances where the recipient has provided prior express consent to receive such calls from that marketer.

Prior to contacting a landline or wireless device, marketers should use applicable federal and DMA Wireless Suppression Files or another comprehensive wireless suppression service. Such suppression files should assist marketers in determining whether or not they are contacting a wireless device, including landline numbers that have been ported to wireless handsets or devices.

A marketer should use DMA's Telephone Preference Service as required in Article #31 and must use the federal Do-Not-Call registry and state Do-Not-Call lists when applicable prior to using any outbound calling list. Telemarketing calls may be made to landline telephones, where the telemarketer has an established business relationship with the individuals even if the individual is on the national registry. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services within the last 3 months. (Note: State laws may vary. DMA's website at: www.the-dma.org/government/donotcalllists.shtml attempts to provide current information on state Do-Not-Call lists.) Consumers who have provided informed, written permission to the marketer do not need to be suppressed by any Do-Not-Call list. Individuals can add or remove themselves from company-specific Do-Not-Call lists either orally or in writing.

Marketers should not use randomly or sequentially generated numbers in sales or marketing solicitations.

CALLER-ID/AUTOMATIC NUMBER IDENTIFICATION REQUIREMENTS
Article #48

Marketers engaging in telemarketing to landline and wireless telephone numbers should generate caller identification information, including:

- A telephone number for 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 by making a do-not-call request, and
- Whenever the technology is available from the marketer's telecommunications carrier, the name of the seller on whose behalf the call is placed or service bureau making the call.

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, landline telephone numbers gained from ANI, except where a prior business relationship exists for the sale of directly related goods or services. With regard to mobile telephone numbers, marketers should abide by Articles #31 and #35.

USE OF AUTOMATED DIALING EQUIPMENT, "ROBO" CALLING
Article #49

Marketers using automated dialing equipment should allow 15 seconds or four rings before disconnecting an unanswered call.

Marketers should connect calls to live representatives within two seconds of the consumer's completed greeting (except in cases where a prerecorded marketing message is used, in accordance with Article #55).

If the connection does not occur within the two-second period, then the call is considered abandoned whether or not the call is eventually connected.

Whenever a live representative is not available within two seconds of the consumer's completed greeting, the marketer should play a prerecorded identification message that includes the seller's name and telephone number, states that the call was made for "telemarketing purposes," and provides a telephone number at which the consumer can request not to receive future marketing calls. The message must also contain an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the called party to make a do not call request prior to terminating the call, including brief explanatory instructions on how to use such mechanism.

When the called party elects to opt-out using such mechanism, the mechanism must automatically record the called party's number to the seller's do not call list and immediately terminate the call.

Repeated abandoned or "hang up" calls to consumers' residential or wireless telephone numbers should be minimized.

In no case should calls be abandoned more than:

Three percent of answered calls within each calling campaign, if the campaign is less than 30 days, or separately over each successive 30-day period or portion of that period during which the campaign continues (unless a more restrictive federal or state law applies), or
twice to the same telephone number within a 48-hour time period.

Marketers should only use automated dialing equipment that allows the telephone to immediately release the line when the called party terminates the connection.

When using any automated dialing equipment to reach a multi-line location, whether for business-to-consumer or business-to-business marketing, the equipment should release each line used before connecting to another.

Companies that manufacture and/or sell automated dialing equipment should design the software with the goal of minimizing abandoned calls to consumers. The software should be delivered to the user set as close to 0% as possible. Manufacturers should distribute these Guidelines for Automated Dialing Equipment to purchasers of dialing equipment and recommend that they be followed.

The dialers' software should be capable of generating a report that permits the user of the equipment to substantiate compliance with the guideline.

Glossary of Terms Used

Automated Dialing Equipment -- any system or device that automatically initiates outgoing call attempts (including text messages) in a random or sequential manner or from a predetermined list of phone numbers. This term includes any equipment that constitutes an

"automatic telephone dialing system" as defined under the Telephone Consumer Protection Act ("TCPA") and/or the FCC's TCPA regulations.

Abandoned Call -- a call placed by automated dialing equipment to a consumer which when answered by the consumer, (1) breaks the connection because no live agent is available to speak to the consumer, or (2) no live agent is available to speak to the consumer within 2 seconds of the consumer's completed greeting.

Abandonment Rate -- the number of abandoned calls over a 30-day period divided by the total number of calls that are answered by a live consumer. Calls that are not answered by a live consumer do not count in the calculation of the abandonment rate.

Campaign -- refers to an offer of the same good or service for the same seller. As long as the same good or service is being offered by the same seller, the offer is part of a single campaign, regardless of whether there are changes in the terms of the offer or the wording of any marketing material, including any telemarketing script, used to convey the offer. This definition applies to Article 48 only and is based on the FTC's definition of a "campaign" for purposes of calculating the abandonment rate.

Report -- reportable information that should be made available which contains key points, including the percentage of abandoned calls.

Telemarketing – a telephone call, prerecorded message or text message placed to a landline or wireless number for the purpose of promoting, advertising, marketing or offering goods or services.

USE OF PRERECORDED VOICE & TEXT MESSAGING
Article #50
Marketers who use prerecorded voice messaging should not automatically terminate calls or provide misleading or inaccurate information when a live consumer answers the telephone.

Consent Required:
Marketers should only use text messaging sent via Automated Dialing Equipment or prerecorded voice to sell goods or services if they have first obtained the call recipient's prior express written agreement to receive prerecorded messages through a written form which may be electronic to the extent permitted by law. In obtaining the consumer's express written agreement, a marketer should observe the following:

- Before obtaining the consumer's informed consent, the marketer should clearly and conspicuously disclose that the purpose of the agreement is to allow the marketer to make prerecorded message calls or send autodialed texts to the consumer.

- The written agreement should evidence the consumer's informed consent to receive prerecorded calls or text messages by or on behalf of the specific marketer

- The marketer should not require that the consumer agree to receive prerecorded calls or text messages as a condition of purchasing any good or service.

- Disclosures that the individual's consent allows the marketer to make prerecorded calls and/or text messages, and that providing consent is not a condition of any purchase, should be made at the time the marketer is seeking written consent.

- Disclosure that by executing the agreement, the individual authorizes the marketer to deliver to the individual marketing text messages using Automatic Dialing Equipment or a prerecorded voice;

- The agreement should include the consumer's telephone number and signature.

- Marketers may obtain the written agreement electronically in accordance with applicable laws such as the E-Sign Act.

Choice Mechanism: Marketers should provide an in-call opt-out mechanism that the call recipient can use to be placed on the company's do-not-call list during the each prerecorded call, or provide an opt-out mechanism within the text message. The type of opt-out mechanism that the marketer should provide depends on whether the call can be answered by a live person or by an automated device. If the marketer is able to determine whether a prerecorded call has been answered by a live person or an automated device, the marketer should tailor the prerecorded message to include the appropriate opt-out mechanism (either option 1 or 2 below):

(1) If the call is answered by a live person, then the marketer should provide an automated interactive voice and/or keypress-activated opt-out mechanism that the recipient can use to make an opt-out request. The mechanism should be available for use at any time during the message.

(2) If the call is answered by an answering machine or voicemail system, then the prerecorded message should provide a toll-free telephone number that the recipient can call to make an opt-out request at any time during the telemarketing campaign. The telephone number provided should connect directly to an automated interactive voice and/or keypress-activated opt-out mechanism. Consumers should be able to call at any time of the day, and on any day, during the duration of the campaign.

If the marketer is not able to determine whether a prerecorded call has been answered by a live person or an automated device, the prerecorded message should include both options 1 and 2.

The interactive voice and/or keypress-activated opt-out mechanism – regardless of whether the prerecorded call can be answered by a live person or automated answering device – should have the following features:

The opt-out mechanism should automatically add the number called to the entity's company-specific do-not-call list; and
the opt-out mechanism should immediately disconnect the call once the opt-out request is made.

Marketers may use prerecorded messages that provide information, but do not induce the purchase of goods or services, without first obtaining prior written consent and without providing an opt-out mechanism. Such calls should promptly disclose the identity of the caller at the outset of the call and provide a valid telephone number sometime during the call.

USE OF TELEPHONE FACSIMILE MACHINES
Article #51
Unless there is an established business relationship, or unless prior permission has been granted, advertisements, offers and solicitations, whether sent to a consumer or a business, should not be transmitted to a facsimile machine, including computer fax machines. An established business relationship in the fax context is defined as a prior or existing relationship based on a voluntary, two-way communication between the sender and recipient of the fax. Such communication includes a purchase, transaction, inquiry, or application for or about goods or services offered by the sender. For business relationships formed after July 9, 2005, the fax number must be provided voluntarily by the recipient to the sender, or be made available voluntarily by the recipient in a directory, advertisement, or Internet site.

Each permitted transmission to a fax machine must clearly contain on the first page:

- the date and time the transmission is sent;
- the identity of the sender which is registered as a business with a state;
- the telephone number of the sender or the sending machine; and
- a clear and conspicuous opt-out notice.

The opt-out notice should:

- clearly state that the recipient may opt out of any future faxes and provide clear instructions for doing so;
- provide a domestic telephone number and fax number for recipients to transmit an opt-out request; and
- unless the telephone or fax number is toll-free, a cost-free mechanism to submit an opt-out request.

Senders must accept opt-out requests at any time.

Opt-out requests must be honored in 30 days, or sooner if feasible. An opt-out request terminates permission to send future faxes based only on an established business relationship.

PROMOTIONS FOR RESPONSE BY TOLL-FREE AND PAY-PER-CALL NUMBERS
Article #52
Promotions for response by 800 or other toll-free numbers should be used only when there is no charge to the consumer for the call itself and when there is no transfer from a toll-free number to a pay call.

Promotions for response by using 900 numbers or any other type of pay-per-call programs should clearly and conspicuously disclose all charges for the call. A preamble at the beginning of the 900 or other pay-per-call should include the nature of the service or program, charge per

minute, and the total estimated charge for the call, as well as the name, address, and telephone number of the sponsor. The caller should be given the option to disconnect the call at any time during the preamble without incurring any charge. The 900 number or other pay-per-call should only use equipment that ceases accumulating time and charges immediately upon disconnection by the caller.

DISCLOSURE AND TACTICS

Article #53

Marketers should make the following initial disclosures promptly:

- The identity of the seller or charitable organization on behalf of which the call is made;
- That the purpose of the call is to sell goods or services or to solicit a charitable contribution;
- The nature of the goods or services offered during the call (if applicable); and
- If a prize promotion is offered, that no purchase or payment is necessary to be able to win a prize or participate in a prize promotion and that any purchase or payment will not increase the person's chances of winning.

Prior to asking consumers for payment authorization, telephone marketers should disclose the cost of the merchandise or service and all terms and conditions, including payment plans, whether or not there is a no refund or a no cancellation policy in place, limitations, and the amount or existence of any extra charges such as shipping and handling and insurance. At no time should high pressure tactics be utilized.

Mobile Marketing

Please refer to the Glossary of Terms at the end of this section for the complete definitions of key concepts and terms used within this section.

OBTAINING CONSENT TO CONTACT MOBILE DEVICES

Article #54

Marketers should obtain prior express written consent from existing and prospective customers before using automated dialing equipment to send mobile marketing to a wireless device. When obtaining prior express written consent, marketers shall meet the following requirements:

1) Before obtaining the consumer's informed consent, the marketer should clearly and conspicuously disclose that the purpose of the agreement is to allow the marketer to make autodialed calls to the consumer's wireless telephone.
2) The written agreement should evidence the consumer's informed consent to receive autodialed calls by or on behalf of the specific marketer.
3) The marketer shall not require that the consumer agree to receive prerecorded calls as a condition of purchasing any good or service.
4) The marketer shall disclose that the individual's consent allows the marketer to make autodialed calls to the person's wireless telephone and that providing consent is not a condition of any purchase.
5) The agreement shall include the consumer's telephone number and signature.

6) Marketers may obtain the written agreement electronically in accordance with applicable laws such as the E-Sign Act.

PROVIDING NOTICE AND CHOICE ABOUT MOBILE MARKETING PRACTICES
Article #55
Marketers that send or intend to send mobile messages should publish an easily accessible notice of their information practices (which includes but is not limited to a notice in their respective privacy policies) with regards to mobile marketing. The notice must include sufficient information to allow individuals to make an informed choice about their interaction with the marketer. This should include, at minimum, any applicable terms and conditions, details of the marketer's information handling practices and clear directions about how to unsubscribe from future solicitations.

The mobile marketing notice should be easy to find, read and understand on mobile screens, and should comply with existing DMA Guidelines. Of particular note, mobile marketers should review and comply with the Terms of the Offer (Articles #1-6, #8, #9), Advance Consent Marketing (Article #12), Special Offers & Claims (Articles #17-#21), and Sweepstakes (Articles #22-#27).

MOBILE OPT-OUT REQUESTS
Article #56
Every mobile marketing message sent must include a simple and easy-to-use mechanism through which the individual can opt out of receiving future mobile marketing messages. Where possible, the opt-out mechanism provided should allow the recipient to opt out via reply text message.

Where individuals respond to a marketer indicating that they do not wish to receive future mobile marketing messages (e.g. an individual replies "STOP"), the marketer should honor the request. Mobile opt-out requests should be honored within 10 days of being received and in accordance with Article #31.

SPONSORSHIP OR AFFILIATE MOBILE MARKETING
Article #57
A marketer may include an affiliate or sponsorship message within a mobile marketing communication, providing that the recipient has provided prior express consent to receive mobile marketing communications from that marketer and that it is clear from the mobile marketing communication that the message has been sent by that marketer and not by the sponsor. A marketer should also comply with Article #8 - Disclosure of Sponsor and Intent.

LOCATION-BASED MOBILE MARKETING
Article #58
Marketers sending location-based mobile marketing messages to recipients should adhere to Articles #54-56. In addition, marketers should inform individuals how location information will be used, disclosed and protected so that the individual may make an informed decision about whether or not to use the service or consent to the receipt of such communications. Location-based information must not be shared with third-party marketers unless the individual has given prior express consent for the disclosure.

MOBILE SUBSCRIPTION SERVICES AND PREMIUM-RATE MOBILE SERVICES
Article #59

Mobile subscription services and mobile premium-rate products and/or services should be offered and delivered in accordance with DMA Guidelines, in particular the Terms of the Offer (Articles #1-6, #8, #9), Advance Consent Marketing (Article #12), Marketing to Children (Article #13-#16), Special Offers & Claims (Articles #17-#21) and Sweepstakes (Articles #22-#27). All advertising and marketing for mobile subscription services or premium-rate mobile products/services should clearly define the service offered and outline the terms and conditions of the offer in accordance with these articles. Mobile subscription services or premium-rate mobile services should not be supplied unless the recipient has actively requested to receive the specific service to be supplied. Further, prior express consent should be obtained from a recipient prior to supplying additional or separate mobile subscription services and premium-rate mobile services at a subsequent date.

In accordance with Articles #12 and #48, and prior to sending or charging recipients for mobile subscription services and/or premium-rate mobile products/services, marketers should:

- provide the individual with an opportunity to see or hear the terms and conditions relating to the subscription service, including:
  - the cost per unit or the total cost of the subscription or premium-rate service;
  - the term of the subscription or premium-rate service;
  - the frequency of the subscription or premium-rate service;
  - payment intervals;
  - how to terminate the subscription or premium-rate service including any terms and conditions that apply to such termination.

- obtain prior express consent from recipients to receive and be charged for said subscriptions, products and/or services;

- inform recipients in the initial offer and in renewal reminders of their right to cancel their participation in the plan, and include contact information within the initial and renewal messages that allows the recipient to directly contact them;

- provide renewal reminders at the frequency specified in the initial offer;

- promptly honor requests for refunds due upon a consumer's cancellation of the plan;

- abide by Articles #13-#16 and #48, and take reasonable precautions and implement adequate technical accountability and authentication measures to ascertain that

  - (a) the mobile phone number or email address provided indeed belongs to the intended recipient of the subscriptions, products or services, and

  - (b) periodically, and not less than once a month, include contact information within the mobile subscription service message or premium-rate mobile service message that allows the individual to directly contact the marketer.

Glossary of Terms Used

- **Individuals** -- refers to the recipients or potential recipients of mobile marketing communications. For purposes of opting out (refer to Article #56), individuals refers to the number(s) and/or electronic address(es) of the wireless device(s) used by the recipients.

- **Location-Based Services** --marketing text message targeted to a recipient dependent on their location, by a handset or user's physical location.

- **Mobile Marketing --** refers to a sales and promotion technique in which promotional materials are delivered to a wireless phone or device. It can include both 'direct mobile marketing' (i.e. marketing communications targeted, sent or "pushed" to a wireless handset or device, such as marketing text messages) and 'indirect mobile marketing' (i.e. marketing that can be accessed or "pulled" by an individual via a wireless handset or device such as a mobile enabled website). Examples include the sending of SMS, MMS or WAP push messages, Bluetooth messaging and other interrupt based marketing to wireless devices.

- **Mobile Service Commercial Message (MSCM) --** a commercial electronic message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service.

- **Multi-Media Messaging Services (MMS) --** an extension of a the Short Message Service Technology that permits the marketer to send marketing messages to a wireless handset that include multimedia objects such as images, audio and video.

- **Mobile Subscription Service** --a service that is provided periodically or on an ongoing basis that is delivered to an individual via a wireless handset or device. This includes free services and paid subscription services.

- **Premium Rate Mobile Services** -- a service that is provided in a single instance, periodically or on an ongoing basis that is delivered to an individual via a wireless handset or device whereby the recipient pays a rate that exceeds the standard tariff to either receive or send a mobile message.

- **Prior Express Consent** -- refers to affirmative, express and informed consent. A marketer should be able to demonstrate that recipients knowingly and affirmatively consented to be contacted on their wireless devices by that marketer for any purposes. Consent may be obtained orally, in writing or electronically. The notice to obtain consent should include a clear and conspicuous disclosure and require an active step on the part of the recipient to demonstrate that he/she agrees to receive the communication and/or product or service. This consent may be obtained via any channel. A pre-checked box, for example, would not suffice as an adequate means for obtaining consent.

- **Recipient** -- any natural or legal person or business that receives a mobile marketing communication.

- **Short Message Service (SMS)** -- a marketing message sent as a text message.

- **Text message** --a brief electronic message sent between mobile phones, containing text composed by the sender, usually input via a lettering system on a cell phone's numeric keypad.

- **Wireless Application Protocol (WAP)** -- Refers to a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators.

- **Wireless** -- Refers to telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.

- **Wireless Handset** -- Umbrella term for devices, typically with keys to input data, that are mobile and can be operated by hand. Examples are mobile phones, pagers, two-way radios, smartphones and communicators.

FUNDRAISING

Article #60

In addition to compliance with these guidelines, fundraisers and other charitable solicitors should, whenever requested by donors or potential donors, provide financial information regarding use of funds.

LAWS, CODES, AND REGULATIONS

Article #61

Direct marketers should operate in accordance with laws and regulations of the United States Postal Service, the Federal Trade Commission, the Federal Communications Commission, the Federal Reserve Board, and other applicable federal, state, and local laws governing advertising, marketing practices, and the transaction of business.

DMA Resources

- "*Do the Right Thing*" Compliance Guide
- *Commitment to Consumer Choice* Member Compliance Guide
- Preference Services Subscriber Information
- DMA's consumer preference website: www.DMAchoice.org
- Privacy Policy Generators
- Environmental Resources and Generator (The "Green 15")
- E-Commerce Integrity Resource Center
- Information Security: Safeguarding Personal Data in Your Care

See DMA's website for numerous other resources developed by the Department of Corporate & Social Responsibility:
www.thedma.org/compliance

DMA can also provide its members with information on the following Federal Trade Commission (FTC) and Federal Communications Commission (FCC) regulations and rules affecting direct marketers:

FTC:

- Mail or Telephone Order Merchandise Rule
- Telemarketing Sales Rule
- Children's Online Privacy Protection Rule
- Negative Option Rule…and much more!

FCC:

- Telephone Consumer Protection Act

Report a Complaint:

To report a complaint regarding a marketing practice that may violate these Guidelines, please email us at ethics@the-dma.org; or submit a written complaint with a copy of the marketing promotion to: Attention: DMA Ethics & Consumer Affairs, 1615 L Street NW, Washington, DC 20036.

DMA's Department of Corporate & Social Responsibility

In its continuing efforts to improve and advance the practices of direct marketing and the marketer's relationship with customers, the DMA sponsors several activities through its Department of Corporate & Social Responsibility:

- Ethical Guidelines are maintained, updated periodically, and distributed to the direct marketing community.
- The Committee on Ethical Business Practice investigates and examines promotions and practices throughout the direct marketing community that are brought to its attention.
- The Ethics Policy Committee revises the Guidelines as needed, and initiates programs and projects directed toward improved ethical awareness in the direct marketing arena.
- The Committee on the Environment and Social Responsibility identifies ways for members to be good corporate citizens and recommends relevant best practices.
- DMA's Commitment to Consumer Choice builds consumer trust in the marketing process by offering individual choices online and offline. www.DMAchoice.org offers consumers assistance in managing their mail and email marketing preferences, and provides consumer education. www.Aboutads.info provides consumers choices for online behavioral advertising. The DMA CSR department oversees compliance by marketers to ensure consumer choices are being honored.

For additional information contact DMA's Washington Office:

1615 L Street, NW, Suite 1100
Washington, DC 20036
202.955.5030
Fax: 202.955.0085
www.dmaresponsibility.org
Email: ethics@the-dma.org

***

Direct Marketing Association, Inc.
Headquarters:
1120 Avenue of the Americas
New York, New York 10036-6700
212.768.7277
Fax: 212.302.6714
www.thedma.org

EXHIBIT 3

DO THE RIGHT THING

A COMPANION TO DMA'S GUIDELINES FOR ETHICAL BUSINESS PRACTICE

FROM THE CORPORATE RESPONSIBILITY DEPARTMENT

ETHICS:

"Knowing the difference between what you have a right to do and what is the right thing to do."

Former Supreme Court Justice Potter Stewart

DMA
Direct Marketing Association
Department of Corporate Responsibility

The Direct Marketing Association staff wants to assist its members in their efforts to market ethically – for the protection of their customers and donors, the reputation of their company or organization, and the future of the direct marketing community.

Every day, DMA staff gives direct marketers advice on how to assure their business practices comply with DMA Guidelines for Ethical Business Practice. This booklet puts in writing some of that advice, and outlines questions you should be asking yourself to determine whether your organization is *doing the right thing.*

Revised January 2009

Guidelines for Ethical Business Practice

The Direct Marketing Association's Guidelines for Ethical Business Practice are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct. These guidelines reflect DMA's long-standing policy of high levels of ethics and the responsibility of the Association, its members, and all marketers to maintain consumer and community relationships that are based on fair and ethical principles. In addition to providing general guidance to the industry, the Guidelines for Ethical Business Practice are used by DMA's Committee on Ethical Business Practice, an industry peer review committee, as the standard to which direct marketing promotions that are the subject of complaint to DMA are compared.

These self-regulatory guidelines are intended to be honored in light of their aims and principles. All marketers should support the guidelines in spirit and not treat their provisions as obstacles to be circumvented by legal ingenuity.

These guidelines also represent DMA's general philosophy that self-regulatory measures are preferable to governmental mandates. Self-regulatory actions are more readily adaptable to changing techniques and economic and social conditions. They encourage widespread use of sound business practices.

Because dishonest, misleading or offensive communications discredit all means of advertising and marketing, including direct marketing, observance of these guidelines by all concerned is expected. All persons involved in direct marketing should take reasonable steps to encourage other industry members to follow these guidelines as well.

DMA Member Principles

DMA Member Principles are the underlying framework for the *Guidelines for Ethical Business Practice* as detailed herein, and for Guidelines that will be drafted in the future. These Principles apply to DMA members' relationships with current and prospective customers, donors, and members, and are the grounding for all DMA members, which includes those who market directly not only to consumers, but also to businesses, government agencies, and "SOHO" (small-office/home-office) entities. The Principles provide a general statement to the public of the expectations they can have when dealing with DMA members.

A DMA Member:

1. Is committed to its customers' satisfaction
2. Clearly, honestly, and accurately represents its products, services, terms and conditions
3. Delivers its products and services as represented
4. Communicates in a respectful and courteous manner
5. Responds to inquiries and complaints in a constructive, timely way
6. Maintains appropriate security policies and practices to safeguard information
7. Provides information on its policies about the transfer of personally identifiable information for marketing purposes
8. Honors requests not to have personally identifiable information transferred for marketing purposes
9. Honors requests not to receive future solicitations from its organization
10. Follows the spirit and letter of the law as well as *DMA's Guidelines for Ethical Business Practice*

TABLE OF CONTENTS

The Terms of the Offer

This section of the guidelines covers the basics for any direct marketer, specifically that consumers should be clearly informed *who* is promoting the offer, *what* the offer is, and *how* the company can be contacted for service.

HONESTY AND CLARITY OF OFFER

Article #1

All offers should be clear, honest and complete so that the consumer may know the exact nature of what is being offered, the price, the terms of payment (including all extra charges) and the commitment involved in the placing of an order. Before publication of an offer, marketers should be prepared to substantiate any claims or offers made. Advertisements or specific claims that are untrue, misleading, deceptive or fraudulent should not be used.

Comment:

- Suppose you are marketing a weight loss product. You want to say that people can lose weight with your program. To do so, you should be able to show to yourself - and keep records so you can show others - that many consumers have, in fact, had success with your company's diet. You also want to make sure you do not exaggerate the amount of weight typical consumers can lose-or the ease of losing it.
- If you are with an advertising agency or Web site design firm, you also have a responsibility to make sure that advertisements are clear, honest and not deceptive. Catalog marketers, in fact, should ask for material to back up questionable claims rather than merely repeat what the manufacturer says about the merchandise. And, if the manufacturer refuses to give you proof or gives you questionable proof, that should serve as a red flag.

Questions to Ask:

- Are you accurately describing the size and other attributes, and/or the quality of what you are offering, taking care not to imply that the merchandise is bigger or better than it is?
- Have you included all information that would be important to a consumer making a purchase decision?
- Have you made the total final price – or terms of payment - easy to find so that consumers do not have to search for this information?
- Do you have the facts at hand to feel confident that the claims you are making are true, or do you only "have a feeling" that they may be true?

ACCURACY AND CONSISTENCY

Article #2
Simple and consistent statements or representations of all the essential points of the offer should appear in the promotional material. The overall impression of an offer should not be contradicted by individual statements, representations or disclaimers.

Comment:

- Keep in mind that a disclaimer or disclosure alone usually is not enough to remedy a misleading or false claim.
- A promotion might state in large bold headlines that the recipient is the definite winner of a large monetary prize. Individual statements elsewhere in the promotion, however, note that almost all recipients actually win only $1. In this instance, details that explain the promotion should be given, and you should make sure that the details will be noticed by the average consumer and that they do not merely explain away the promotion's overall impression.

Questions to Ask:

- Is the language understandable for the average reasonable consumer under the circumstances, or is it too complex for the average consumer to understand?
- Did you make sure that statements in different parts of the ad do not contradict each other?
- Is the overall impression the average person takes away from reading the promotion likely to be a true picture of what the promotion is?
- Have you included all the details that an average reasonable person would need to make a good decision, and are they all easy to find and understand?
- Have you taken care to avoid a "shout and whisper" technique, that is, have you avoided points in prominent language being "shouted" contradicted by essential information in fine print being "whispered?"

CLARITY OF REPRESENTATIONS

Article #3
Representations which, by their size, placement, duration or other characteristics are unlikely to be noticed or are difficult to understand should not be used if they are material to the offer.

Comment:

- A promotion, for instance, that uses "mouse type" at the bottom of a page or flashes important information on the TV screen very briefly would render the promotion difficult to read and unclear.
- Representations can be both expressly made or implied.

Questions to Ask:

- Are all important facts clearly and conspicuously stated, and is any surrounding material likely to detract from their being noticed?

- Is the average consumer you are marketing to likely to be able to easily read the type size and font used?
- Does the graphic format make it easy to find and read important information?

ACTUAL CONDITIONS

Article #4
All descriptions, promises and claims of limitation should be in accordance with actual conditions, situations and circumstances existing at the time of the promotion.

Comment:

- A discount travel certificate received in the mail contains small print on the back which discloses that travel is only for certain limited times, there are numerous other restrictions, and there are several "advance fees" that must be paid. Most consumers would view these disclaimers as material to the offer and contrary to the impression first made.
- If a promotion's outer envelope claims something specific is "inside," you should ensure that what is advertised is actually inside the envelope. If, instead, there is an explanation of how the consumer goes about obtaining what was claimed to be "inside," then the outer envelope should clearly disclose that condition by stating, for instance, "more details inside."

Questions to Ask:

- Do you inform the consumer of all details immediately so he or she can make an intelligent and considered decision, taking care not to wait until the last minute to disclose some important limitation on the offer?
- Do you take care not to create a false impression of urgency, limited quantity or unqualified suitability when that is not the case?
- Do you have systems in place to make sure that all advertised promises can be honored, barring circumstances beyond your control?

DISPARAGEMENT

Article #5
Disparagement of any person or group on grounds addressed by federal or state laws that prohibit discrimination is unacceptable.

Comment:

- Think, for example, about an advertisement for some new electronic device that portrays people who use wheelchairs as unable to travel outside of their home. While meaning to promote a useful product, this advertisement might disparage wheelchair users as people who are helpless and unable to get around – an unflattering and untrue picture, and should be avoided.

Questions to Ask:

- Have you taken care not to picture a person or group in a negative light?
- Have you included or eliminated a group based on stereotype?

- Are you knowledgeable about or have you consulted legal counsel regarding laws concerning disparagement and discrimination? For instance, improper targeting based on certain zip code selections could be illegal if seen as an attempt to deny credit to certain populations.

DECENCY

Article #6
Solicitations should not be sent to consumers who have indicated to the marketer that they consider those solicitations to be vulgar, immoral, profane, pornographic or offensive in any way, and who do not want to receive them.

Comment:

- "Offensive" or "profane" is in the mind of the beholder. Lingerie ads that most consumers would not consider vulgar, for example, might offend one of your prospects. If that individual asks to be removed from your mailing list, it would be improper not to suppress the name as quickly as possible.

Questions to Ask:

- Do you have in place quick, easy and effective mechanisms for removing people from lists they don't wish to be on?
- Do you use (if relevant to your business) the U.S. Postal Service's name-removal list for Sexually Oriented Advertisements (the "pander" file)?

PHOTOGRAPHS AND ART WORK

Article #7
Photographs, illustrations, artwork and the situations they describe should be accurate portrayals and current reproductions of the products, services or other subjects they represent.

Comment:

- If your catalog, for example, illustrates a realistic-looking three-dimensional reproduction of a famous statue, you are sure to disappoint your customers if they receive one with a size or scale far different than the one depicted – or a poster or picture of one instead of the real thing.

Questions to Ask:

- Do you make sure that you use current or actual photos and not "stock" photos or drawings that are not accurate portrayals?
- Do you describe the height, weight, color or any other critical details in the copy?
- Do you take care not to use photos or illustrations that, through graphic representation, overstate the size or value of the product being offered?
- Are your customer service reps trained to give advice and details on items?

DISCLOSURE OF SPONSOR AND INTENT

Article #8

All marketing contacts should disclose the name of the sponsor and each purpose of the contact. No one should make offers or solicitations in the guise of one purpose when the intent is a different purpose.

Comment:

- This article requires, for example, that if you are sending a fundraising promotion, the promotion should not pretend that it is simply a survey. It may be fine to have both a survey and a request for funds in the same promotion; however, as long as the survey is bona fide, that is, you plan to tabulate and use the information provided by respondents. In this example, the intent of each part of the promotion should be made clear to the consumer.

Questions to Ask:

- Does your promotion clearly have your company or organization name on it and where and how it can be reached?
- Does the promotion clearly state what its purpose is, for instance, to sell products, solicit funds for a charity or conduct a sweepstakes?
- Does the reader understand what action you are asking him or her to take, for instance, to place an order, send a check, or return an entry form?

ACCESSIBILITY

Article #9

Every offer should clearly identify the marketer's name and street address or telephone number, or both, at which the individual may obtain service. If an offer is made online, the marketer should provide its name, an Internet-based contact mechanism and a street address. For e-mail solicitations, marketers should comply with Article #39 (Commercial Solicitations Online).

Comment:

- It is important for the promotion to clearly identify your company by a name that is sufficient for the consumer to know who the marketer is, even if a service entity is actually used to contact the consumer. The address and telephone number given should be usable for customer service inquiries to avoid confusion and difficulty in obtaining needed assistance. Return e-mail addresses that don't allow the consumer to actually contact your company are useless and frustrating to consumers.

Questions to Ask:

- Does the promotion clearly have your company or organization name on it?
- Does the offer contain a customer service address and/or telephone number and, if relevant, an e-mail address?

- If a potential customer needs more information about the offer, will it be easy to contact your company and get that information?
- If one of your customers needs assistance with an order, will it be clear what telephone number or address should be contacted to get that assistance?

SOLICITATION IN THE GUISE OF AN INVOICE OR GOVERNMENTAL NOTIFICATION

Article #10
Offers that are likely to be mistaken for bills, invoices, or notices from public utilities or governmental agencies should not be used.

Comment:

- If your company is soliciting new business for a directory, for example, you should not state "amount due" or "billing number" or otherwise make the promotion look like an actual invoice for a prior order or renewal when it is not.
- Likewise, if your company is offering a service to advise consumers of government-sponsored auctions, you should make sure that the promotion, including the outer envelope, does not look like it is from the government agency itself. Government symbols and advisories about not obstructing mail delivery should not be misused to make consumers believe that promotions are official government documents.
- The intent of this guideline is not to stunt marketers' creativity, but the line between "creativity" and deception should not be crossed.

Questions to Ask:

- Do you avoid using the term "invoice" or "reference number" or "amount due" on an unsolicited advertisement for new business?
- Does the wording clearly state that the offer is not a bill?
- Is the overall impression the consumer takes away likely to be that the promotion is from a private business, and not a government agency?
- Does the promotion clearly and conspicuously state it is not from the government?
- Does the promotion avoid using terms like "official" and referring to mailing regulations and penalties for misuse of the U.S. mails?
- Do you take care to not have the graphics and/or format make the promotion appear to be an invoice or from the government?

POSTAGE, SHIPPING OR HANDLING CHARGES

Article #11
Postage, shipping or handling charges, if any, should bear a reasonable relationship to actual costs incurred.

Comment:

- Many consumers question what they view as excessive shipping and handling charges. When figuring shipping and handling fees, it is important to reflect these costs as accurately as possible so that your customers or prospects are not likely to view these fees as a company "profit

center." Such an attitude can contribute to consumer hesitancy in using and trusting direct marketing. You should also clearly and conspicuously disclose what the shipping and handling costs are -- to avoid unpleasant surprises and customer dissatisfaction.

- The DMA has established *Guidance for Establishing and Substantiating Shipping and Handling Charges* to assist you in understanding legal risks and setting justifiable costs. See www.dmaresponsibility.org/SH.
- In addition, many consumers object to insurance fees for lost or damaged merchandise as unnecessary, and simply adding to the company's profits. If you charge an insurance fee, it would be helpful to explain why -- that the insurance fee is meant to expedite the process of re-sending merchandise and that you will make good on the order promptly. Shipment of consumers' orders in a timely fashion, however, should not be affected by whether or not they pay the insurance fee.

Questions to Ask:

- Are your customers likely to view your postage and handling charges as reasonable rather than as a company "profit center"?
- Are the charges appropriate in accordance with established methods of determining shipping and handling, such as by the product's weight or cost?
- Have you established a fulfillment cost study for your shipping and handling charges? (See www.dmaresponsibility.org/SH.)
- Is any insurance charge appropriate for the service you perform?

Advance Consent Marketing

The following guidelines were approved by DMA's Board of Directors in order to address increasing complaints to government regulatory agencies and to DMA alleging unauthorized credit card charges for unordered goods or services. They were subsequently updated to ensure consistency with the Federal Trade Commission's revised Telemarketing Sales Rule.

Article #12
These guidelines address marketing plans where the consumer gives consent to receive and pay for goods or services in the future *on a continuing or periodic basis unless and until the consumer cancels the plan.*

The following principles apply to all advance consent marketing plans:

- **Marketers should have the consumer's informed consent to participate in any advance consent marketing plan before the consumer is billed or**

charged. In telephone sales where the consumer pays in a way other than by credit or debit card, this consent must be written or audio recorded.

- Marketers may provide products or services and bills concurrently; however, consumers should not be obligated to pay bills prior to the expiration of any trial period.

- Marketers should inform consumers in the initial offer and in renewal reminders of their right to cancel their participation in the plan.

- Marketers should provide renewal reminders at the frequency specified in the initial offer. Marketers should allow consumers a reasonable length of time between receipt of renewal reminders and the renewal date, before which consumers can cancel the plan.

- Marketers should promptly honor requests for refunds due upon consumers' cancellation of the plan.

Marketers should clearly and conspicuously disclose material terms and conditions before obtaining the consumer's consent, including:

- a description of the goods or services being offered
- the identity of the marketer and contact information for service or cancellation
- the interval between shipments or services to be provided
- the price or the range of prices of the goods or services purchased by the consumer, including whether there are any additional charges
- whether the consumer will be billed or automatically charged
- when and how frequently the consumer will be billed or charged
- the fact that the consumer must take affirmative action to cancel in order to avoid future billing or charges
- the specific and easy steps that consumers should follow to cancel the plan and avoid the charges, and
- the time period if any within which the consumer must cancel

When applicable, the following terms and conditions should also be clearly and conspicuously disclosed in the initial offer:

- that the current plan or renewal prices of the goods or services are subject to change
- the length of any free, trial, or approval period in time or quantity
- the length of any membership period, and the length of subsequent renewal or billing periods

- **the fact that goods or services will continue after the free period unless the consumer cancels**
- **any minimum purchase obligations, and**
- **terms and conditions of any refund policy**

In telephone sales where the marketer uses pre-acquired account information under a free-to-pay conversion plan, the marketer should:

- **obtain from the consumer the last 4 digits of the account to be charged**
- **obtain consent from the consumer to charge such account, and**
- **audio record the entire transaction**

In telephone sales where the marketer uses pre-acquired account information but does not engage in a free-to-pay conversion plan, the marketer should:

- **identify with specificity the account that will be charged, and**
- **obtain consent from the consumer to charge such account**

All marketing partners or service providers should comply with these guidelines.

Comment:

- This article addresses plans where the consumer consents in advance to receive and pay for goods or services in the future on *an ongoing basis unless and until the consumer cancels the plan.* In contrast, the Federal Trade Commission's Prenotification Negative Option Rule applies to marketing plans that involve the sale of a *specific number* of goods, or the sale of goods or services for a *specific period* of time where the marketer gives the consumer advance notice before each shipment, along with the opportunity to decline the goods before delivery.
- Marketers should ensure that consumers consent to participating in marketing programs and to having their credit card accounts charged. Inadvertently surprising consumers with charges for products or services they did not consent to or misleading them by processing credit card charges or debits during what they thought was a "free trial" is not *doing the right thing* or enhancing consumer confidence in direct marketing.
- Advance consent marketing plans can use a variety of terminology, for instance:
    - Free Trial Offers
    - Preview Offers
    - "Free-to-Pay" Conversions
    - Automatic Renewal Plans
    - Continuity Programs
    - "On Approval" Offers
- Often membership or buying clubs and magazine subscriptions are sold via advance consent marketing plans. There are a variety of ways such plans are advertised and operated. Depending on the specific offer, trial goods or services may, or may not, be free regardless of whether the consumer continues the program. For instance, a buying club may be offered on a 3-month trial basis, after which time the consumer continues membership in the club and even if the consumer cancels after the trial period, is liable for the 3-month trial. Or, a consumer may accept

a free introductory offer to a magazine, and if he or she does not wish to continue with a subscription, writes "cancel" on the invoice and does not owe for the introductory issues received. While both are fair practices, disclosures must make it clear to consumers whether or not they must pay for the trial period at the time of their agreement to participate.

- Regardless of the specific plan offered by your company, the main premise of this guideline is that a consumer must unequivocally understand the purchasing plan and give informed consent before being enrolled. This means that you should receive your prospective customer's permission before processing any charges or submitting any bills. Although you can send an invoice along with your products, you should make it clear that the consumer is not obligated to begin making payments until after the end of any promised trial, or initial, period.
- Marketers should clearly inform consumers of all important details of the offer before seeking consumer consent (whether the plan is presented in written form, online, or via a teleservices call).
- Consumers should be clearly informed of any price change in their ongoing programs and their right to cancel.
- If you call prospective customers because of their customer relationship with an unrelated marketer, and would like to charge the credit account they used for the previous purchase, you must follow Teleservices Sales Rule provisions. (See www.the-dma.org/telemarketing/tsr_compliance_guide.pdf.) The DMA and regulatory agencies have received numerous consumer complaints alleging that credit card account information was transferred from one marketer to another without their consent. Although there are legal and legitimate reasons for such transfers to take place, including between corporate affiliates and for credit account verification, consumers do not always understand the reasons for these transfers. Consumer consent should always be on record before any charges are processed.
- Consumers need to be informed both upfront and in renewal notices about their rights to cancel participation in the program. Cancellation notices should be easy to find, read and understand. You do not have to provide a free method of canceling (such as a toll-free number), but it should be easy for the consumer to exercise the cancellation right.

Questions to Ask:

- Do your promotional materials disclose all important terms clearly and conspicuously, including what is being offered, the price of the goods (or range of prices), how frequently the consumer will receive the products offered, and how frequently the consumer will receive bills or be charged?
- Are any additional costs, such as shipping and handling (or ranges of these costs), clearly disclosed in your promotional materials?
- Do your written materials and/or teleservices script clearly state who is offering the products or services and provide contact information for customer service?
- Are consumers informed, in the initial offer and in renewal reminders, of their rights to cancel the program, and of terms and conditions in any refund policy? Are renewal reminders sent according to the promised frequency?
- Are consumers informed in renewal reminders of any changes in price, going forward, and of their right to cancel the program?
- Is a straightforward method of cancellation provided that is easily understood by the average consumer? Do you honor cancellation requests and provide any refunds due promptly?
- Do you take affirmative steps to ensure that teleservices reps follow your scripts and obtain consumer consent prior to enrolling consumers in your marketing plan?
- Do you ask for and receive assurances from your business partners that they also comply with these guidelines in order to protect consumers?

Marketing to Children

This section of the guidelines is meant to help marketers who count children as among their customer segments, if not their major customers. Marketing to children involves a different sensitivity from marketing to adults, especially in the interactive online world. Children increasingly make buying decisions, but need special protections. Online marketing to children has led to an increase of legislative and media attention to all forms of marketing to children. Given this attention, the Association responded by strengthening its guidelines in this area.

MARKETING TO CHILDREN

Article #13

Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online or in any other medium, marketers should address the age range, knowledge, sophistication and maturity of their intended audience.

Comment:

- Products and services not meant for young individuals, such as credit cards or online gambling, should not be promoted to them. Inasmuch as the age of majority determines whether one can be bound to a contract, even marketing magazine renewals to young teens has come under scrutiny by some state regulators; marketers should evaluate the "climate" before engaging in such marketing campaigns.
- Because children are less experienced consumers than adults, they are often not aware of what they may be obligating themselves to. They are also not legally responsible for the resulting contracts or bills.

Questions to Ask:

- Are you careful to clean your lists so children do not mistakenly receive marketing materials not appropriate for them?
- Do you have quick and effective mechanisms in place to remove children's names when requested?
- If the promotion is appropriate for children, do you use language that is easily understood by children in the specific age range you are marketing to?
- Are any pictures and graphics clear, appropriate and complete?

- Do your promotions encourage young children to involve their parents in all purchasing decisions?

PARENTAL RESPONSIBILITY AND CHOICE

Article #14

Marketers should provide notice and an opportunity to opt out of the marketing process so that parents have the ability to limit the collection, use and disclosure of their children's names, addresses or other personally identifiable information.

Comment:

- Your company's youth-oriented magazine, for example, could have a notice in its masthead or other area where subscriber information is located that children's names and addresses are sometimes exchanged with other companies offering suitable products for children. The notice, which could also be included in a customer service letter to parents, would clearly disclose how to limit the exchange of such information.

Questions to Ask:

- Do you state, in a notice that is easy to find, read and understand, that children's names and addresses may be rented or transferred to other companies offering relevant products?
- Do you clearly state how parents can opt out of receiving prospect advertising from other companies?

INFORMATION FROM OR ABOUT CHILDREN

Article #15

Marketers should take into account the age range, knowledge, sophistication and maturity of children when collecting information from them. Marketers should limit the collection, use and dissemination of information collected from or about children to information required for the promotion, sale and delivery of goods and services, provision of customer services, conducting market research and engaging in other appropriate marketing activities.

Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected.

Upon request from a parent, marketers should promptly provide the source and general nature of information maintained about a child. Marketers should implement strict security measures to ensure against unauthorized access, alteration or dissemination of the data collected from or about children.

Comment:

Marketing to children is one of the most sensitive areas of direct marketing. This article addresses several data usage aspects:

- Information that is not needed to serve or market to a child should not be collected and kept by marketers.
- Parents understandably want to know the source of unsolicited promotions directed to or about their children, so they should be given this information upon request.

> Keep in mind that under the law (the Children's Online Privacy Protection Act (COPPA, effective April 21, 2000), and the Federal Trade Commission (FTC) regulations that implement the Act, you must get verifiable parental consent to collect information online from children. See Article #16.

- Because marketing to children raises security issues in some parents' minds, it makes sense to direct promotions "to the parents of…" rather than to the child.
- It also may not make sense to use language such as: "We have learned about your child" which could be frightening to parents.
- Since security is uppermost in parents' minds, information must be kept and handled with utmost care.

Questions to Ask:

- Are you using clear age-appropriate language to tell children, when applicable, why you are asking for certain information?
- Do you state clearly to parents why information is requested?
- Is the information you are collecting from or about children needed only for order fulfillment and other appropriate marketing purposes?
- Do you have procedures in place to allow customer service reps to tell parents, upon their request, the source of information about their children?
- Do you train your customer service reps to knowledgeably and satisfactorily respond to parents' requests for information about what you know about their children?
- Do you train your staff and have in place monitoring systems to securely handle data from or about children?

MARKETING ONLINE TO CHILDREN UNDER 13 YEARS OF AGE

Article #16

Marketers should not collect personally identifiable information online from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of such information online, and an opportunity for the parent to prevent such use and participation in the activity. Online contact information should only be used to directly respond to an activity initiated by a child and not to re-contact a child for other purposes without prior parental consent. However, a marketer may contact

and get information from a child for the purpose of obtaining parental consent.

Marketers should not collect, without prior parental consent, personally identifiable information online from children that would permit any off-line contact with the child.

Marketers should not distribute to third parties, without prior parental consent, information collected from a child that would permit any contact with that child.

Marketers should take reasonable steps to prevent the online publication or posting of information that would allow a third party to contact a child off-line unless the marketer has prior parental consent.

Marketers should not entice a child to divulge personally identifiable information by the prospect of a special game, prize or other offer.

Marketers should not make a child's access to a Web site contingent on the collection of personally identifiable information. Only online contact information used to enhance the interactivity of the site is permitted.

The following assumptions underlie these online guidelines:

- **When a marketer directs a site at a certain age group, it can expect that the visitors to that site are in that age range; and**
- **When a marketer asks the age of the child, the marketer can assume the answer to be truthful.**

Comment:

- In the world of online marketing to children, it is essential – both to be in compliance with federal law and to *do the right thing* – to clearly explain to both children and their parents why your company is asking for information. For example, you could say to young children: "If you give us your e-mail address, we'll tell you when new toys arrive, but your parents must say that it's ok." You could ask parents for permission, saying: "Information collected from children at this site is used only to understand their preferences among products and to notify them of new toys."
- In addition, online marketers should, to the best of their ability using the technology that is currently available, try to obtain parents' permission before collecting information from children. You should, for example, use language such as: "Your mom or dad must say it's ok before you answer these questions."

> According to the FTC's regulations implementing the Children's Online Privacy Protection Act, e-mail can be used to get parental consent for all internal uses of personal information. In instances where a child's personal information may be disclosed to third parties or made available publicly, a more reliable method of gaining consent must be used. Such methods could include getting a signed form from the parent via postal mail or fax; accepting and verifying a credit card number; taking calls from parents through a toll-free number; e-mail accompanied by a digital signature; and e-mail accompanied by a PIN or password obtained through one of the already-mentioned verification methods.

- "Kids: fill out this short survey telling us about yourself and then you can play these fun games and win great prizes" would be an example of "enticing" a child by the prospect of a special game, prize or other offer.

Questions to Ask:

- What is the age range of the children you are directing your messages to? If under age 13, have you gotten parental permission to collect information?
- Are you using information collected from a child only so you can respond to his or her request or inquiry, or have you asked the parents for approval to respond?
- Do you take care not to convey to children that they will get a special prize, or can play a game, only if they give information about themselves to your company?
- Are you using information collected to contact the child so you can obtain parental consent for any additional information uses?
- Do you have secure data handling procedures in place to prevent distribution of information to third parties or online posting of information?

> Note: the FTC regulations implementing COPPA were issued November 1999; see separate industry compliance guide containing detailed guidance at: www.the-dma.org/privacy/children.shtml.

Special Offers and Claims

In addition to basic product or service information that should be part of any offer, some promotions have additional offers or claims, including guarantees, price comparisons or the like. This section and any regulations referenced should be reviewed carefully by marketers using such special claims.

USE OF THE WORD "FREE" AND OTHER SIMILAR REPRESENTATIONS

Article #17
A product or service that is offered without cost or obligation to the recipient may be unqualifiedly described as "free."

If a product or service is offered as "free," all qualifications and conditions should be clearly and conspicuously disclosed, in close conjunction with the use of the term "free" or other similar phrase. When the term "free" or other similar representations are made (for example, 2-for-1, half-price or 1-cent offers), the product or service required to be purchased should not have been increased in price or decreased in quality or quantity.

Comment:

- Most consumers understand "free" to mean without further obligation of any kind. If they respond to a "free" offer in which additional items need to be purchased, or it turns out that they are really joining a continuity program, they should be clearly informed of the terms and conditions in the initial promotion before they are billed so there are no misunderstandings. Clear disclosures explaining the offer should appear near a representation that something is "free," before you can be fairly confident that average consumers will understand the offer.
- "Free" is subject to legal requirements, as are other terms such as "sale" and "new." Check with your legal counsel to make sure such terms are used in accordance with legal requirements.

Questions to Ask:

- Are all important facts and conditions clearly stated?
- If asked, can you demonstrate that no part of the price of the "free" item has been built into the item to be purchased?

PRICE COMPARISONS

Article #18
Price comparisons including those between a marketer's current price and a former, future or suggested price, or between a marketer's price and the price of a competitor's comparable product should be fair and accurate.

In each case of comparison to a former, manufacturer's suggested or competitor's comparable product price, recent substantial sales should have been made at that price in the same trade area.

For comparisons with a future price, there should be a reasonable expectation that the new price will be charged in the foreseeable future.

Comment:

- Trust in buying via direct response can only be sustained when consumers are satisfied that the advertised discounts are bona fide. So, if you advertise leather coats for $79.99 and say "compare to retail," then the coats should actually be selling in the same trade area in substantial quantities at a higher retail price so that the offer of savings is valid.
- Although price testing is different from price comparisons, price testing is worth mentioning with this article. Sometimes consumers question the ethics of price testing, noting, for example, that a catalog sent to one geographical area may have higher prices for the same merchandise than a catalog sent to a different area. Price testing is an acceptable way of establishing prices, but to build trust, the test should run only for a finite period of time and you might want to consider allowing consumers who question pricing discrepancies to buy the desired item at the lower advertised price.

Questions to Ask:

- Do you use the term "sale" in your promotions to compare to your former higher price only when you have actually made substantial sales at those former prices?
- If you use terms such as "compare to manufacturer's suggested retail price," have you assured yourself that substantial sales have actually been made at that price?

GUARANTEES

Article #19
If a product or service is offered with a guarantee or a warranty, either the terms and conditions should be set forth in full in the promotion, or the promotion should state how the consumer may obtain a copy. The guarantee should clearly state the name and address of the guarantor and the duration of the guarantee.

Any requests for repair, replacement or refund under the terms of a guarantee or warranty should be honored promptly. In an unqualified offer of refund, repair or replacement, the customer's preference should prevail.

Comment:

- Warranty information is important to consumers, so when a warranty is referred to in a promotion, consumers should be told what the warranty covers, who offers the warranty (the seller or the manufacturer of the product) and how to get warranty service. This information should either be in the promotion itself, or the consumer should be told how to obtain a free copy of the warranty before purchase.
- You are not required by federal law to have a specific guarantee or return policy. But, if you use phrases such as "satisfaction guaranteed" or "money-back guarantee," the Federal Trade Commission's regulation on warranties requires that you must be willing to give full refunds for

any reason. Whatever guarantee policy you advertise must, of course, be honored. If your policy is "all sales final," that should be disclosed.

Questions to Ask:

- Are all important facts concerning the warranty or guarantee either clearly stated in your promotion or a reference made where the consumer can learn about the warranty before making the purchase?
- If you advertise a "lifetime" guarantee, is it clear what lifetime – the buyer's, the product's, your company's – is referred to?
- Is it clear how the consumer goes about getting warranty service, if it should be needed?

USE OF TEST OR SURVEY DATA

Article #20

All test or survey data referred to in advertising should be valid and reliable as to source and methodology, and should support the specific claim for which it is cited. Advertising claims should not distort test or survey results or take them out of context.

Comment:

- "Latest medical research shows 95% of consumers using this herb lower their cholesterol" would be sure to capture consumers' attention, but taken out of context -- for instance, a small sample of people with certain medical conditions was tested at a non-certified medical establishment -- such test results could be misleading and perhaps even harmful to some consumers.

Questions to Ask:

- Do you have back-up materials from the survey source to substantiate the ad claims?
- Do you trust the credentials of the research source?
- Do you "have a feeling" that the survey result seems unrealistic or is controversial?
- Does the group that experienced the results you're advertising seem large enough and enough like the consumers you're advertising to?

TESTIMONIALS AND ENDORSEMENTS

Article #21

Testimonials and endorsements should be used only if they are:

a. **Authorized by the person quoted;**
b. **Genuine and related to the experience of the person giving them both at the time made and at the time of the promotion; and**
c. **Not taken out of context so as to distort the endorser's opinion or experience with the product.**

Comment:

- Famous personalities or actors announcing the effectiveness of the newest exercise equipment, for example, can be effective representatives. But keep in mind that any endorsements you use should be as current as possible in addition to being genuine. Make sure the endorser's opinion has not changed and that the product itself has not been modified. If the product has been changed, make sure the endorser's statements still apply.

Questions to Ask:

- What is the source of the endorsement, and are you confident that it is reliable?
- Is the endorsement or testimonial current or dated?
- Does instinct tell you the customer testimonials don't ring true?

Sweepstakes

This section of the guidelines gives essential information to any marketer who uses or plans to use sweepstakes as a promotional tool in any medium. Sweepstakes are popular among consumers who enjoy the chance to win a valuable prize at no cost to themselves, and most consumers understand the basic nature of sweepstakes – that many will enter and few will win. However, this marketing technique was under increased regulatory, legislative and media scrutiny, and some consumers were identified as taking actions that seemed not to be in their own best interests. Congress passed a law in 1999, the Deceptive Mail Prevention & Enforcement Act, to help eliminate confusion and protect consumers from deceptive promotions. Since many states also have laws regarding sweepstakes and prize promotions, legal counsel should be consulted to review your sweepstakes.

USE OF THE TERM "SWEEPSTAKES"

Article #22
Sweepstakes are promotional devices by which items of value (prizes) are awarded to participants by chance without the promoter's requiring the participants to render something of value (consideration) to be eligible to participate. The co-existence of all

three elements -- prize, chance and consideration -- in the same promotion constitutes a lottery. It is illegal for any private enterprise to run a lottery without specific governmental authorization.

When skill replaces chance, the promotion becomes a skill contest. When gifts (premiums or other items of value) are given to all participants independent of the element of chance, the promotion is not a sweepstakes. Promotions that are not sweepstakes should not be held out as such.

Only those promotional devices that satisfy the definition stated above should be called or held out to be a sweepstakes.

Comment:

- One concern about the use of the term "sweepstakes" has to do with promotions that are offers to purchase information about sweepstakes in a report, which typically contains a listing of various sweepstakes and how to enter them. If "sweepstakes" is used in the prominent heading or in the name of the promotion, consumers often view the promotion itself as a sweepstakes when it is really an offer for information about sweepstakes. Sometimes the term "sweepstakes" is used just to add interest to a promotion and encourage consumers to buy the items being offered even when there is no sweepstakes involved.
- Be aware that if you advertise, for example, that the first ten respondents to your promotion get a prize, an "early bird special," you may be promoting an illegal lottery.
- The law requires sweepstakes mailings to include the name of the sponsor and an address at which the sponsor may be contacted. The mailing must also display, clearly and conspicuously, an address or a toll-free number where a consumer or an individual acting in his stead may request that the consumer's name be removed from the sponsor's sweepstakes mailing list. The sponsor will have up to 60 days to remove the name from its sweepstakes promotion mailing list. (Individuals have the right to sue the sponsor for failure to comply.)

Questions to Ask:

- Does your sweepstakes offer meet the legal test for a sweepstakes -– a prize being awarded by chance and without a requirement to submit payment or something else of value?
- If your company offers reports or listings of sweepstakes, is the nature of your offer clear to consumers?
- If your sweepstakes is offered online rather than in the print medium, do you still make certain that your offer meets the legal test for a sweepstakes, including a way for consumers to enter without making a payment or purchase?
- Do you have processes in place to ensure that you honor name-removal requests as required by federal law?

NO PURCHASE OPTION

Article #23

Promotions should clearly state that no purchase is required to win sweepstakes prizes. They should not represent that those who make a purchase, or otherwise render consideration with their entry, will have a better chance of winning or will be eligible to win more or larger prizes than those who do not make a purchase or otherwise render consideration. The method for entering without ordering should be easy to find, read and understand. When response devices used only for entering the sweepstakes are provided, they should be as easy to find as those utilized for ordering the product or service.

Comment:

- Late in 1999, Congress enacted a law requiring statements that no purchase is necessary and that a purchase will not increase the odds of winning in the mailing, in the rules and on the order form. These statements must be shown clearly and more conspicuously than other required disclosures. (See DMA's *Sweepstakes Do's and Don'ts for Marketers: A "Plain Language" Guide to the Deceptive Mail Prevention and Enforcement Act of 1999* at www.dmaresponsibility.org/Sweepstakes.)
- You should consider how consumers view sweepstakes that require them, when not ordering, to go through several extra steps to enter. Marketers shouldn't make consumers feel guilty about winning when they didn't purchase anything.
- The new law forbids any statement that sweepstakes offers will cease if the consumer doesn't place an order.

Questions to Ask:

- Do you in the mailing, in the rules and on the order form clearly state that no purchase is necessary to enter and that a purchase will not enhance the odds of the entry winning?
- Is your response device for entering without ordering just as easy for consumers to find, read and understand as the device used for entering with an order?

CHANCES OF WINNING

Article #24

No sweepstakes promotion, or any of its parts, should represent that a recipient or entrant has won a prize or that any entry stands a greater chance of winning a prize than any other entry when this is not the case. Winners should be selected in a manner that ensures fair application of the laws of chance.

Comment:

- It is essential for sweepstakes marketers to consider the overall impression their promotions make on consumers. The law forbids any representation that an individual is a winner unless that individual is, in fact, a winner.
- Sweepstakes promoters should consider how consumers will react to language such as: "Check off the prizes you want;" "How do you want your cash?" "When will you be available to receive your prize?" Will such phrases unfairly lead consumers to believe that the mailing is notifying them that they already are the winners, or that making a purchase increases the chance of winning?
- Contradictory statements in any mailing containing sweepstakes entry materials will render the mailing non-mailable, according to the law, enforced by the U.S. Postal Service.
- Requiring the mailing of an entry without an order to be sent to a different location from an entry accompanied by an order may make it appear to consumers that their entries do not have as good a chance of winning because they are not sent to the "good" address.

Questions to Ask:

- Is it likely that the language used in the promotion could be misunderstood by the recipient as meaning he or she holds the winning number and only has to send it back in order to redeem the prize?
- Do you take care that the graphics used, as well as various type sizes and styles, do not add to a mistaken impression that the recipient is the holder of the actual winning entry number when he or she is most likely not?
- Does the promotion make it clear that a different address is used for entries with orders so that orders can be quickly processed and fulfilled, but that entries with and without orders still have an equal chance of winning?

PRIZES

Article #25

Sweepstakes prizes should be advertised in a manner that is clear, honest and complete so that the consumer may know the exact nature of what is being offered. For prizes paid over time, the annual payment schedule and number of years should be clearly disclosed.

Photographs, illustrations, artwork and the situations they represent should be accurate portrayals of the prizes listed in the promotion.

No award or prize should be held forth directly or by implication as having substantial monetary value if it is of nominal worth. The value of a non-cash prize should be stated at regular retail value, whether actual cost to the sponsor is greater or less.

All prizes should be awarded and delivered without cost to the participant. If there are certain conditions under which a prize or

prizes will not be awarded, that fact should be disclosed in a manner that is easy to find, read and understand.

Comment:

- Disappointment and loss of consumer trust can be avoided by steering clear of an overall impression that implies to recipients they won the grand prize when that is most likely not the case.
- The law requires the clear and conspicuous disclosure of the odds of winning each prize and the schedule of payments.
- The likelihood of "winning" a nominal amount of money, for example, 50 cents, versus winning one of the major awards, also can be problematic to consumers. If recipients understand their "prize" is likely to be a few cents, that's fine -– they may still want to enter for the chance of winning big, but such "prizes" need to be stated clearly and conspicuously, not just in the "fine print."
- Marketers offering reports about how to enter sweepstakes should not make it seem as though the consumer will win a prize if a fee is paid. The sweepstakes report itself may have valuable information and instructions on entering various contests with lots of prize money. However, the promotion needs to clearly convey that any fee is only for the report itself.

Questions to Ask:

- Are prizes clearly and accurately portrayed in words and/or pictures?
- Have you substantiated that non-monetary prizes are worth the amount stated?
- If the sweepstakes has various levels, awards and expiration dates, are they described in language the average consumer will understand (without having to read the piece several times)?

PREMIUMS

Article #26
Premiums should be advertised in a manner that is clear, honest and complete so that the consumer may know the exact nature of what is being offered.

A premium, gift or item should not be called or held out to be a "prize" if it is offered to every recipient of or participant in a promotion. If all participants will receive a premium, gift or item, that fact should be clearly disclosed.

Comment:

- When everyone who responds to a sweepstakes offer will receive the inexpensive item (e.g., the fake pearl), the promotion should clearly note the odds in the rules section as 1:1, and add language in the promotion's text to the effect that everyone will receive the premium. Recipients should not be led to believe they are among a chosen few to receive the premium.
- In addition, the term "sweepstakes" should not be used for offers in which everyone receives a premium and there is no prize of higher value. It is, of course, possible to have in the same promotion both sweepstakes prizes that only a few will win and premiums that everyone else will receive.

Questions to Ask:

- Does the promotion state in clear language that everybody who sends back the entry will receive the premium?
- Are you careful not to call a premium offer a "sweepstakes" when it does not meet the criteria for a sweepstakes?

DISCLOSURE OF RULES

Article #27
All terms and conditions of the sweepstakes, including entry procedures and rules, should be easy to find, read and understand. Disclosures set out in the rules section concerning no purchase option, prizes and chances of winning should not contradict the overall impression created by the promotion.

The following should be set forth clearly in the rules:

- **No purchase of the advertised product or service is required in order to win a prize.**
- **A purchase will not improve the chances of winning.**
- **Procedures for entry.**
- **If applicable, disclosure that a facsimile of the entry blank or other alternate means (such as a 3"x5" card) may be used to enter the sweepstakes.**
- **The termination date for eligibility in the sweepstakes. The termination date should specify whether it is a date of mailing or receipt of entry deadline.**
- **The number, retail value (of non-cash prizes) and complete description of all prizes offered, and whether cash may be awarded instead of merchandise. If a cash prize is to be awarded by installment payments, that fact should be clearly disclosed, along with the nature and timing of the payments.**
- **The estimated odds of winning each prize. If the odds depend upon the number of entries, the stated odds should be based on an estimate of the number of entries.**
- **The method by which winners will be selected.**
- **The geographic area covered by the sweepstakes and those areas in which the offer is void.**
- **All eligibility requirements, if any.**
- **Approximate dates when winners will be selected and notified.**
- **Publicity rights regarding the use of winner's name.**
- **Taxes are the responsibility of the winner.**
- **Provision of a mailing address to allow consumers to receive a list of winners of prizes over $25.00 in value.**

Comment:

- Marketers offering sweepstakes should consider the "readability" of their rules section, including the size of the print, the layout and the location. For example, rules presented in all capital letters in one paragraph are very difficult for most consumers to read. A graphic presentation using light type is also difficult to read.
- Consumers generally want to know the value of all prizes they are eligible for, so even though printing space may be limited, it is still a good idea to list this information.
- The law requires 1) the estimated odds of winning; 2) the quantity, estimated retail value, and nature of each prize; and 3) the schedule of payments made over time to appear in the rules.

Questions to Ask:

- Are you careful not to make any statements in the promotion, or convey an impression, that would seem to be contradicted by the information contained in the rules section?
- Is the rules section easy to find, read and understand?
- Do you list all the prizes, including the lesser-valued ones, in the rules?
- Are the odds or an estimation of the odds of winning the various prizes clearly listed?
- Do the rules clearly explain how to enter both with and without an order?

> See DMA's separate industry compliance document which explains the sweepstakes law in detail at: www.dmaresponsibility.org/Sweepstakes.

Fulfillment

In this section, various aspects regarding the fulfillment of the direct marketing order are covered. Because this is an area subject to federal regulation, much of the following discussion explains these requirements as simply as possible, often by examples. Marketers are also referred to other helpful resources and are reminded to work with legal counsel familiar with the subject.

UNORDERED MERCHANDISE OR SERVICE

Article #28

Merchandise or services should not be provided without having first received the customer's permission. The exceptions are samples or gifts clearly marked as such, and merchandise mailed by a charitable organization soliciting contributions, as long as all items are sent with a clear and conspicuous statement informing the recipient of an unqualified right to treat the product as a gift

and to do with it as the recipient sees fit, at no cost or obligation to the recipient.

Comment:

- Sometimes consumers complain that they received unordered merchandise or services and subsequent invoices when they actually had committed themselves to an automatic renewal program. Such a misunderstanding could be avoided if the initial advertising clearly discloses all important information. This is particularly important if the offer is made on the phone and the consumer receives no other information prior to payment. (See Article #12 Advance Consent Marketing.)
- Consumers, according to federal law, may keep any merchandise that was not ordered and treat it as a gift.

Questions to Ask:

- If you use samples as a marketing tool, do you clearly state that they are samples and that no customer payment is required?
- Are your customers likely to understand, because you have given clear disclosure of all important points, when they are signing up for a continuity or automatic renewal program, so they will not think they are receiving unordered merchandise or services?

PRODUCT AVAILABILITY AND SHIPMENT

Article #29

Direct marketers should offer merchandise only when it is on hand or when there is a reasonable expectation of its timely receipt.

Direct marketers should ship all orders according to the terms of the offer or within 30 days where there is no promised shipping date, unless otherwise directed by the consumer, and should promptly notify consumers of any delays.

Comment:

> Promptly fulfilling orders is the right thing to do, but in addition, marketers are legally subject to the Federal Trade Commission's (FTC) Mail or Telephone Order Merchandise Rule ("The 30-Day Rule"). A compliance booklet prepared by DMA and the FTC is available through the DMA Washington, D.C. office; contact us at ethics@the-dma.org. It can also be viewed at: www.dmaresponsibility.org/30DayRule.

- Sometimes marketers ask whether they can or should charge consumers' credit cards upon receipt of the order. The 30-Day Rule allows that the "shipping clock" begins as soon as a properly completed order is received, whether or not the marketer charges the consumer's account then or at the time the product is shipped. Although it is legal to put the charge through as soon as the order is received, you may want to wait until the time the order is shipped to charge the account. This could avoid situations in which consumers complain that they received their credit card bill before delivery of the goods they ordered.

- If your promotion doesn't state when orders will be shipped, but you advise people when they call and order that you'll ship within 72 hours, for example, 72 hours becomes the promised shipment date. If you find you cannot then ship within the 72 hours, you have to let your customers know and provide them with a delay notice and an opportunity to cancel the order.
- If you run into a delay situation, you should notify consumers as soon as possible and let them know when you'll be able to ship. If the first delay is 30 days or less, you can assume that they will wait. If the delay is more than 30 days or if you have a second or subsequent delay or an indefinite delay, you have to cancel the order unless the customer notifies you that he or she will wait. For good customer service, you should explain this in your delay notice; otherwise the consumer may be very upset upon finding the order has been cancelled.
- You have to provide a free way for the consumer to tell you what he or she wants to do, such as a postage paid postcard to mail or a toll-free number to call.
- If the consumer ordered merchandise online, the Rule still applies. Delay notices can be given via the consumer's e-mail and the consumer can respond via e-mail as well, if desired.
- Refunds have to be issued promptly, within one billing cycle (if billed) or within 7 working days (if payment was by check).
- Substitutions should not be made unless consent is obtained or that policy is clearly noted in your promotional materials and returns of substituted merchandise are allowed.
- Some mail or telephone order transactions and how the 30-Day Rule applies are not as clear-cut as others. The FTC has over the years filed legal charges against companies for certain practices and issued advisory opinions, both of which can help you know what the right thing is to do.

  For instance, consumers sending in coupons that are redeemable for merchandise must still be informed of your inability to ship the merchandise when promised, offered delay options, and provided with reasonable compensation if the merchandise cannot ever be made available.

  Or, occasionally you might have a situation where a small balance is owed a consumer. It is expensive for your company and doesn't seem to make sense to issue a check in the amount of 10 cents, for instance. Since this is actually a complex legal issue, you should consult legal counsel regarding this type of situation.

Questions to Ask:

- Are you confident that you have sufficient inventory overall when offering your merchandise?
- Are you confident that you can ship within the time stated in your promotion or, if no time is stated, within 30 days?
- Does your promotion notify consumers clearly as to how long it will take to ship their orders?
- Do you have an efficient system in place to promptly notify consumers of delay situations once you become aware of them?
- Are consumers given free options of notifying you of their desire to wait for an order or cancel it, as per the 30-Day Rule?
- Do you credit or refund consumers promptly and in full, as required?
- If you provide substitutions for unavailable items, do you first get your customer's consent or clearly describe such a policy and accept returned merchandise?

DRY TESTING

Article #30
Direct marketers should engage in dry testing only when the special nature of the offer is made clear in the promotion.

Comment:

- Dry testing occurs when you want to "test the waters" for interest in a new product, i.e., one that does not yet exist. On its face, testing the market for a product that doesn't yet exist appears to violate the 30-Day Rule, as the Rule requires a seller who makes an offer to have a reasonable basis that the goods ordered will be shipped. However, you may dry test as long as consumers are not misled and are informed, for example, by stating something like: "This new magazine is being planned; we will let you know if it will not be published, and of course, if it is not, we will promptly credit your account by (date)."
- You may want to delay accepting payment for a product that is not yet available, or refrain from charging an account.
- Also, you should know that the FTC has stated in an advisory opinion that substitutions may not be made in this kind of situation.
- "Price testing" is sometimes confused with "dry testing." As noted under *Price Comparisons*, price testing is an acceptable and common way of testing the market -– for example, setting a different price for the same merchandise in a different geographic location. It is recommended that consumers who complain to you about this practice be offered the merchandise at the lower advertised price, and that the test be of finite duration.

Questions to Ask:

- Does your advertising clearly reflect that the offer is for a product or service that is not yet available?
- If it is determined for whatever reason that the product will not be made available, do you notify consumers of this fact promptly and issue credits or refunds, if payment had been accepted?

Collection, Use and Maintenance of Marketing Data

This section of the guidelines covers the essential area of information usage, without which there would be no direct marketing as we know it. In order to continue marketing without overly burdensome regulations, it is highly recommended that the following be carefully considered and implemented. Also, of course, as widely promoted, DMA requires that the basic principles of fair information practices be utilized, as per the *Commitment to Consumer Choice.*

This section covers the areas of collection, use and transfer of personally identifiable information and sensitive information, information security, and, pertinent also to business-to-business marketers, promotion of marketing lists and list usage, and the responsibilities of database compilers.

***Please note that DMA began to gradually phase out the Telephone Preference Service (TPS), referenced throughout this section. New consumer registrations for TPS are no longer being accepted. However, DMA members must continue to suppress prospective customers listed on TPS through December 31, 2011 (thus honoring TPS registrant requests for five years). DMA now only accepts TPS registrations for consumers living in the states of PA and WY, because TPS serves as those states' official lists. Other consumers who wish to decrease the amount of unsolicited telemarketing calls they receive should register with the Federal Trade Commission's National Do Not Call Registry at: www.donotcall.gov or by phone 1.888.382.1222.**

For purposes of the *Guidelines for Ethical Business Practice*, the following definitions are used:

Consumer **refers to the subject of the data.**

Marketing data **means actual or inferred information consistent with a person's commercial or charitable inquiry or transaction, or market research or market survey information. Such information can be derived from either a direct contact or marketing partnership when linked to a person's name, postal or e-mail address, or telephone number, or any other personally identifiable information. When obtained from a publicly available source, information (including public record information), not combined with other information, is not marketing data.**

Marketing purpose **means any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to allow or induce consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers.**

Comment:

- The definition of marketing purpose includes fraud prevention, verification, and data hygiene purposes. Fraud prevention is encompassed within marketing because it is part of facilitating the marketing activity of providing assurance that the consumer is who he says he

is. Verification is also in furtherance of marketing to update and maintain the marketing database, as is data hygiene.

- Uses/requests by government agencies, without legal process, are not included.
- Individual reference or look-up services are not marketing purposes.

COLLECTION, USE AND TRANSFER OF PERSONALLY IDENTIFIABLE DATA

Article #31
This article is applicable to all media, and includes special requirements for mailers.

- **A marketer using the mail channel should provide existing and prospective customers with notice of an opportunity to modify or eliminate direct marketing communications to be received from that company or organization. This guideline applies to senders of marketing offers. (Online marketers should provide notice in accordance with Article #38. Email marketers should provide notice in accordance with Article #39 and the CAN-SPAM Act.)**

- **The notice in the mailing should:**
  - **appear in every marketing offer and**
  - **be easy for the consumer to find, read, understand, and act upon**

- **A consumer's request for elimination of future marketing offers should be processed:**
  - **within 30 days or as required by law, whichever is the shorter time period**
  - **for a period of at least three years from the date of receipt of the request**

- **A marketer periodically should provide existing customers with notice of its policy concerning the rental, sale, exchange, or transfer of data about them and of the opportunity to opt out of the marketing process. All such opt-out requests should be honored promptly.**

- **An in-house suppression request from a consumer should be interpreted as meaning that the consumer also wants to opt out of the transfer of his or her personal information.**

- Where an affiliate, division, or subsidiary markets under a different company or brand name, and is perceived as separate by the consumer, each corporate entity or brand should separately honor requests received by it.

- A marketer should establish internal policies and practices that assure accountability for honoring requests, in compliance with this guideline, and at no cost to consumers. Should those policies substantially change, the marketer has an obligation to inform consumers of that change prior to the rental, sale, exchange, or transfer of such data, and to offer consumers an opportunity to opt out of the marketing process at that time.

- For each prospecting list that is rented, sold, exchanged, or transferred, the names registered on the applicable DMAchoice name-removal lists should be removed prior to use. DMAchoice name-removal lists include:
  - the relevant categorical opt-out mailing lists for Catalog, Magazine, Pre-screened Credit Offers or Other categories, as well as future categories designated by the DMA; and
  - the eMail Preference Service and Telephone Preference Service, as well as future DMA preference service lists

  Use of the above DMAchoice name-removal lists is not required on customer/donor lists.

  The following DMAchoice name-removal lists should be used on current customer/donor lists, as well as prospect lists:
    - the marketer's own DMAchoice company/organization brand opt-out mailing list

  In all instances, the most recent *monthly* release of the relevant DMAchoice file should be used.

- In addition to adhering to these guidelines, a marketer should cooperate with DMA when requested in demonstrating compliance with the *Commitment to Consumer Choice*.

- Upon request by a consumer, a marketer should disclose the source from which it obtained personally identifiable data about that consumer.

Comment:

- These principles -- disclosing notice of your information practices, offering consumers the choice to opt out, honoring their opt-out requests, suppressing customer and prospect names upon request and using DMA's name-removal services –– are among the requirements for membership in DMA.

> The *Commitment to Consumer Choice* (approved by DMA's Board of Directors in October 2007) expands upon the principles of DMA's 1999 *Privacy Promise to American Consumers.* Detailed information and numerous "notice" examples, as well as background as to why the CCC was promulgated, are in a separate member compliance guide – available at www.DMACCC.org.
>
> Subscription information for the Preference Services can be found at http://preference.the-dma.org/products.

Here are a few other helpful tips for complying with this guideline article:

- Referring consumers to DMA when what they want is removal from *your* customer or prospect list is not helpful to anyone and definitely *not* the right thing to do. Consumers often think DMA is your list source and that DMA can remove them from your files. Make sure employees at your company or organization understand that consumers should be referred to DMA when they want an overall reduction in unsolicited national mailings. Consumers can find information about DMA's Preference Services at www.DMAchoice.org.
- As noted in the children's marketing section, you should be able to answer questions about the source of information. Consumers trying to reduce the amount of their mail or a relative's mail are not happy to hear you say you can't tell them the source of their name on a mailing list. You should tell consumers the source of their name on your list. If, for some reason, you cannot be specific as to the source, at least tell consumers the kinds of sources you use.
- Also, you should not enter into agreements with list sources that would prohibit disclosing the source of information to consumers. Make sure your own lists are not exchanged with this non-disclosure requirement.
- You might question whether you have to honor name-removal requests you receive from a third party as part of customer service. Many enterprises have sprung up which claim to offer consumers help in decreasing the number of unsolicited promotions they receive. Although you must maintain an in-house suppression list (required by two federal laws for telephone calling lists in addition to DMA's membership requirement), you are not obligated to accept requests that come from such third parties. That is up to your organization. DMAchoice offers a company specific opt-out function for the catalog segment (as of October 2008) which should also be used by applicable members. DMAchoice should be used on a monthly basis, instead of quarterly.
- Consumers understandably are upset when they receive promotions directed to deceased relatives, especially if the individuals died years ago. That is why, in January 2006, DMA's Board of Directors approved the requirement for members to suppress deceased individuals' information when such information is provided to DMA. This information is available via the Deceased Do Not Contact list and is also flagged on the other Preference Service files.

- DMA has always encouraged marketers to make every attempt to clean lists against "deceased" files maintained by some service bureaus to avoid the circumstance of contacting individuals who have died. (This is particularly important when marketing to the mature marketplace and to households believed to have newborn children.)
- DMA does not receive information from government agencies like the Social Security Administration or other sources about deceased consumers; therefore, the Deceased Do Not Contact file is not a complete listing of deceased individuals' names.

> In addition to using DMA's Deceased Do Not Contact file, you can also contact the Washington, D.C. office for information on service bureaus offering "deceased" files.

- Although these guidelines apply to business-to-consumer marketing, it is recommended that they be honored when marketing to businesses also. Honoring opt-out requests for business names and generally cleaning your business lists is just good business.
- Finally, the guidelines say that in addition to complying with the *Commitment to Consumer Choice*, member companies who are asked to provide documentation of their compliance cooperate promptly with DMA staff. It is essential in demonstrating self-regulation to policymakers that DMA regularly monitor its members, and that members cooperate with DMA.

Questions to Ask:

- Does your company have an internal policy regarding fair information principles and practices, and an executive charged with oversight for its implementation?
- Are all employees trained as to what the policy means and how it should be implemented?
- Does your company give clear notice to consumers about its collection and use of customer data?
- Does your organization provide notice (in commercial mailings) of an opportunity to modify or eliminate direct marketing communications?
- Do you have systems and procedures in place for removing customers and prospects from your lists -- within 30 days for telephone lists and within 10 days for email lists according to federal law?
- Do you have procedures for removing deceased persons from your lists?
- Are your customer service reps trained to identify and handle name-removal requests?
- Are your customer service reps trained to disclose the source of information to consumers, upon their request?
- Does your company, or your service bureau, use the appropriate Preference Service files before contacting prospective customers?
- If data are rented, sold, exchanged or transferred online, do you take steps to ensure that the data are secure and/or encrypted?
- If requested by DMA, does your company promptly provide documentation that it follows the guidelines and the *Commitment to Consumer Choice*?

PERSONAL DATA

Article #32
Marketers should be sensitive to the issue of consumer privacy and should only collect, combine, rent, sell, exchange or use marketing data. Marketing data should be used only for marketing purposes.

Data and selection criteria that by reasonable standards may be considered sensitive and/or intimate should not be disclosed, displayed or provide the basis for lists made available for rental, sale or exchange when there is a reasonable expectation by the consumer that the information will be kept confidential.

Credit card numbers, checking account numbers and debit account numbers are considered to be personal information and therefore should not be transferred, rented, sold or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.

Social Security numbers are also considered to be personal information and therefore should not be transferred, rented, sold or exchanged for use by a third party when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of Social Security numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers. [Social Security numbers, however, are used by direct marketers as part of the process of extending credit to consumers or for matching or verification purposes.]

Comment:

- The first part of this article addresses the fact that marketing data, for example, from subscriber files, warranty cards, consumer surveys, etc. should not be used for non-marketing purposes, such as reference or "look up" services. Reference services would include such services as "people-finding" and skip tracing and would be obtained from publicly available information.
- Sensitive information generally includes, but is not limited to, consumer information that is financial- or health-related.
- Many consumers and business people have expressed concern after receiving a promotion with a "stick-on note" that seems to be a personalized message from someone they know. The note generally encourages the recipient to try the advertised product. Although this technique can be viewed as creative, people who complain to DMA note their confusion about the sender and

concern that the sender knows something personal about them -- for example, that they could use a weight loss program or need help with their communication skills.

- The practice of "reverse append," for example, matching a consumer's credit card number against a credit bureau file to obtain the consumer's address, is not specifically covered in this article. It may be an acceptable practice if the consumer gives you a credit card number and you use the number to obtain an address to which to mail your latest offer. But, reverse appending and transferring the information to another marketer may be outside of what consumers would reasonably expect. Indeed, many consumers expect that a credit card number will be used only to complete a transaction. (See Article #43 regarding E-mail Appending to Consumer Records.)
- Although it might be reasonable to assume that your company would maintain credit account numbers for its own customers, many people would assume this kind of sensitive information would not be transferred to another marketer.
- Also, consumers are increasingly wary of credit identity theft. That occurs when a thief uses someone's credit account and other numbers to establish new lines of credit under that person's name. Consumers may not learn about their credit problems until they apply for a mortgage or job, and then it can take years to straighten out. This is another reason why it makes sense to be especially careful in handling financial account information.
- Consider whether mailing a promotion with a consumer's Social Security number on it may be seen as violating that consumer's expectation of confidentiality, especially if the information is visible on the outside of the promotion. Although Social Security numbers have long been used as personal identifiers in a number of ways, consumers are becoming more aware of the potential for their misuse as well as the misuse of credit account numbers.
- Because of this heightened concern, account numbers and other customer identification numbers should no longer be based on a customer's Social Security number.

Questions to Ask:

- Consider the purpose for which you are collecting data from or about consumers. Are you avoiding the collection of data for which you have no marketing usage?
- Do you believe reasonable consumers would expect your company to be collecting and/or using certain kinds of data about them that could be viewed as sensitive?
- Do you believe consumers would understand and agree with how financial, health-related or other data are used?
- Do you guard your customers' financial information carefully, taking care not to share it with other companies that weren't authorized by your customers to have it?
- Are you careful to maintain and use such information securely and to employ encryption, where appropriate, online?
- Is it necessary for your company to collect, maintain or use consumers' Social Security numbers?
- Do you take special care to ensure that your customers' Social Security numbers are kept private and safe?
- Do you take care not to share this personal information without your customers' knowledge?
- Are Social Security numbers visible through a window envelope or in any other way when included within a promotion?

COLLECTION, USE & TRANSFER OF HEALTH-RELATED DATA

Article #33
Health-related data constitute information related to consumers':

- **illnesses or conditions;**
- **treatments for those illnesses or conditions, such as prescription drugs, medical procedures, devices or supplies; or**
- **treatments received from doctors (or other health care providers), at hospitals, at clinics or at other medical treatment facilities.**

These fair information practices and principles apply to any individual or entity that collects, maintains, uses and/or transfers health-related data for marketing purposes, whether or not marketing is a primary purpose. These principles are applicable to nonprofit as well as for-profit entities.

1. Personally identifiable health-related data gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities should not be transferred for marketing purposes without the specific prior consent of those consumers. Health or medical care providers include licensed health care practitioners, such as doctors, nurses, psychologists, pharmacists and counselors, and those who support health care providers and therefore have access to personally identifiable information, such as insurance companies, pharmacy benefits managers or other business partners, and businesses that sell prescription drugs.

2. Personally identifiable health-related data, including the occurrence of childbirth, gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities (as defined in #1) should not be used to contact those consumers for marketing purposes without giving consumers a clear notice of the marketer's intended uses of the data and the opportunity to request not to be so contacted.

3. Personally identifiable health-related data volunteered by consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. Such data should not be collected, maintained, used and/or transferred for marketing purposes unless those consumers receive, at the time the data are collected, a clear notice of the marketer's intended uses of the data, whether the marketer will transfer the data to third parties for further use, the name of the collecting organization, and the opportunity to opt out of transfer of the data. Such data include, but are not limited to, data volunteered by consumers

when responding to surveys and questionnaires. Clear notice should be easy to find, read and understand.

4. Personally identifiable health-related data inferred about consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. These are data based on consumers' purchasing behavior. Such data include, but are not limited to, data captured by inquiries, donations, purchases, frequent shopper programs, advertised toll-free telephone numbers, or other consumer response devices. Any entity, including a seller of over-the-counter drugs, which uses inferred health-related data should promptly provide notice and the opportunity to opt out of any transfer of the data for marketing purposes.

5. Marketers using personally identifiable health-related data should provide both the source and the nature of the information they have about that consumer, upon request of that consumer and receipt of that consumer's proper identification.

6. Consumers should not be required to release personally identifiable health-related information about themselves to be used for marketing purposes as a condition of receiving insurance coverage, treatment or information, or otherwise completing their health care-related transaction.

7. The text, appearance and nature of solicitations directed to consumers on the basis of health-related data should take into account the sensitive nature of such data.

8. Marketers should ensure that safeguards are built into their systems to protect personally identifiable health-related data from unauthorized access, alteration, abuse, theft or misappropriation. Employees who have access to personally identifiable health-related data should agree in advance to use those data only in an authorized manner.

If personally identifiable health-related data are transferred from one direct marketer to another for a marketing purpose, the transferor should arrange strict security measures to assure that unauthorized access to the data is not likely during the transfer process. Transfers of personally identifiable health-related data should not be permitted for any marketing uses that are in violation of any of DMA's Guidelines for Ethical Business Practice.

Nothing in these guidelines is meant to prohibit research, marketing or other uses of health-related data which are not personally identifiable, and which are used in the aggregate.

Comments:

- Think carefully about using a promotion implying or stating, for example, that your company knows what prescription medicine the consumer may be taking -- this would be considered overstepping the boundaries of confidentiality. Consumers are alarmed at the prospect of having sensitive health-related information out of their control, even if your intention is to benefit them by giving them information about other remedies.
- It is also important when using health-related information not to disclose potentially sensitive information on the outside of the mailing piece itself. For example, a consumer who has a thyroid condition may not want his family member or roommate (or postal carrier, or anyone else) to know this. Of course, what is sensitive to one person about his health may not be sensitive to another person. Nevertheless, it is best to be extremely careful with health-related information.
- If you collect or use information gained via surveys that ask questions about personal health conditions, make sure that the disclosure on the survey is easy to find, read and understand. In other words, visibly and clearly spell out what will happen if the consumer fills out and submits the survey, for example, "We will send you coupons to save money on useful products, and other carefully selected companies will also contact you with their offers of products you may find helpful." And, if pertinent, "If you only want the coupons and wish to restrict other uses of the information you have provided, please let us know by checking here."
- The DMA's Frequently Asked Questions fact sheet about rules implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (as well as legal counsel) should be consulted if your company is a health care provider (a "covered entity").
  See www.dmaresponsibility.org/HIPAA.

Questions to Ask:

- For what purpose is consumers' health and medical information collected, maintained and used?
- Do you take care not to collect more information than is necessary for the intended marketing purpose?
- Do you convey to consumers what information is being used and why?
- Are appropriate systems and procedures in place to remove consumers' information upon their request?
- Does your company carefully guard health and medical information?
- Are promotions regarding health and medical conditions designed and sent with sensitivity in mind?

PROMOTION OF MARKETING LISTS

Article #34

Any advertising or promotion for marketing lists being offered for rental, sale or exchange should reflect the fact that a marketing list is an aggregate collection of marketing data. Such promotions should also reflect a sensitivity for the consumers on those lists.

Comment:

- You should realize that policymakers and industry critics read direct marketing trade journals. Watch how you describe offerings; for example, marketing lists promising "to tell more about

individuals than their own mothers know" are misguided and really serve to attract negative attention to our industry.

- If you are a list provider, as another example, ask yourself whether a list promotion that describes people who may have financial difficulties as "desperate folks ripe for business opportunities" is a sensitive portrayal of prospective customers.
- Compilers and other list professionals should be especially careful to ensure that their promotions do not in any way imply that marketing data are used for non-marketing purposes, such as reference services. Data promotions should clearly note where information for "people-finding" and other such reference services is obtained.
- Media and critics also visit our industry's trade shows. Gimmicks that invite trade show attendees to "look up" individual or household data should be discouraged.

Questions to Ask:

- Does your data card or other listing clearly indicate that the list is an aggregate collection of consumer data?
- Do you use objective descriptions regarding the consumers that make up the lists?
- Do you promote the list in ways that respect individual consumer privacy?

MARKETING LIST USAGE

Article #35

List owners, brokers, managers, and users of marketing lists should ascertain the nature of the list's intended usage for each materially different marketing use prior to rental, sale, exchange, transfer or use of the list. List owners, brokers, and managers should not permit the rental, sale, exchange or transfer of their marketing lists, nor should users use any marketing lists for an offer that is in violation of these guidelines.

Comment:

- If you are a list provider, you should carefully analyze your own policies regarding acceptance of clients' intended promotion pieces. Problems can be avoided by not allowing potentially misleading or deceptive promotions to be sent to consumers. DMA's Guidance to List Industry on FTC Legal Interpretation discusses screening offers before list rental and should be helpful in this regard. See: www.the-dma.org/cgi/disppressrelease?article=603. [The *Commitment to Consumer Choice* also encourages suppliers to educate their customers as to fair information practices.]

Questions to Ask:

- How do you think the average consumer would view the sample promotion piece or telephone script or e-mail text presented to you?
- Do you believe the promotion is honest, complete, clear, believable and that it passes your internal "gut reaction" test?
- Does the marketer to whom you plan to provide the list practice fair information practices, too?

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.

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.

Comments:

- As a matter of clarification, database compilers are not responsible for providing notice to consumers regarding their information practices.
- The "written agreement" between a database compiler and a customer referred to in the guideline could be reached electronically (such as by voice recording, touch tone response, digital signature, or digital acknowledgement), but verbally would not be a strong enough standard. The point is that regardless of how databases are obtained (for example: online, telephone order, or CD-ROM retail purchase), database compilers and customers should have an agreement that states consumer data will be used ethically and legally.
- It should be noted that the agreement between database compilers and customers should include that a random monitoring process will be employed for consumer protection. It would be up to the parties themselves to spell out the specifics, including actions to be taken in case of a violation of the agreement.
- A "reasonable time" within which to suppress a consumer's information upon request is not defined by the guideline. As a guide, 30 days appears to be reasonable. The compiler should decide what is reasonable, taking the consumer's perspective into account. Compilers may also want to include language in their contracts advising how often suppression requests will be provided and encouraging their customers to honor those requests promptly.
- "Sensitive marketing data" means marketing data pertaining to children or older consumers, health care or treatment, account numbers, or financial transactions. For sensitive marketing data, the extra step of reviewing promotions should be taken.
- It is acknowledged that there are several different standards regarding at what age a person is an "older adult." Ages range from 50 (AARP) to 65 and up. We urge compilers to look at the totality of circumstances when deciding whether there is a duty to review promotions.
- The inclusion of "older adults" recognizes that younger and older Americans, in some instances, may be particularly susceptible to certain marketing practices. Promotions directed to them may require a higher degree of scrutiny.
- Compilers who sell, lease or trade lists that contain nonprofit data are covered under this guideline. Similarly, nonprofits that compile marketing lists or who hire third parties to do so are covered as well.
- Political data lists to be used for political purposes are <u>not</u> covered under this guideline. However, lists containing information of a political nature that will be used for marketing

purposes are covered by this guideline. For example, a list of contributors to a candidate that is to be used to market a political almanac would be covered.

- During discussions and review of this guideline it was noted that situations will not always present a clear and easy choice regarding the necessity to review the marketing use of a list. The guideline anticipates this by requesting that the compiler exercise its best judgment in determining the need to review the use of a list.
- Pre-screened credit offers may be used only as permitted by the Fair Credit Reporting Act (FCRA). Thus, for purposes of this guideline, "financial transactions" do not include pre-screened credit offers.

Suggested contract language:

The following is an illustration of appropriate language that database compilers may include in their written (or electronic) agreements and the points they should cover to help define the rights and responsibilities of the compiler and customer with respect to the use of marketing data:

> "It is an express condition of this agreement (1) that the Data rented or obtained from Database Compiler shall be used only for lawful marketing purposes and in compliance with the ethical guidelines of the Direct Marketing Association, and (2) that Database Compiler may, upon reasonable request, require Client or Client's agent or broker to provide Database Compiler with evidence showing that Client, Client's agent or broker, or other authorized user, is in compliance with this condition.

"Database Compiler reserves the right to immediately, and without further notice or refund or rebate, terminate this agreement if Database Compiler has reason to believe that this express condition is not being complied with."

This suggested language is just one option for defining rights and responsibilities concerning the use of marketing data. Contract language may be more or less strict, but should require compliance with applicable laws and DMA guidelines for DMA member customers (and require compliance with applicable laws and encourage adherence to DMA member guidelines for non-DMA member customers), and provide for a right of the database compiler to request proof of compliance and seek corrective action in the event of non-compliance by the customer.

INFORMATION SECURITY

Article #37

The protection of personally identifiable information is the responsibility of all marketers. Therefore, marketing companies should assume the following responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data:

- **Marketers should establish information security policies and practices that assure the uninterrupted security of information systems.**

- **Marketers should create and implement staff policies, procedures, training, and responsiveness measures to protect personally identifiable information handled in the everyday performance of duties.**
- **Marketers should employ and routinely reassess protective physical safeguards and technological measures, including data retention, destruction, and deletion practices, in support of information security.**
- **Marketers should contractually require all business partners and service providers that handle personally identifiable information to ensure that their policies, procedures and practices maintain a level of security consistent with the marketer's applicable information security policies.**
- **Marketers should, in the event of a security breach where there is a reasonable likelihood of material harm to consumers, inform those consumers who may be affected as soon as reasonably practical, unless requested by legal authorities to delay such notification.**

Comment:

- This guideline was originally developed in January 2003 for several reasons. Inasmuch as protecting *privacy* of personally identifiable information and maintaining *security* of information are closely intertwined, DMA believed that it was important to specifically address the ethics of information security within the *Guidelines for Ethical Business Practice*. In addition, DMA wanted to respond to challenges issued by the Federal Trade Commission and the Organization for Economic Cooperation and Development, which were increasingly concerned with this issue globally, and asked industry association leaders to be more involved in promoting security among industry members and encouraging them to factor security into the design of their systems. These guidelines are consistent with the OECD's revised security guidelines (see www.oecd.org).
- DMA produced, in cooperation with the FTC, a *Checklist of Information Security Procedures* based on these guidelines. *Information Security: Safeguarding Personal Data in Your Care* can be found at: www.dmaresponsibility.org/InfoSecurity.
- Marketers should also use the **DMA/Solutionary SecurCompass** security and compliance assessment tool – see www.the-dma.org/cgi/member/solutionary. This tool (available only to DMA members) consists of 42 questions that mirror the *Checklist of Information Security Procedures*. This internal self-assessment gauges where your organization has addressed security and privacy issues appropriately, and where you may need some assistance.
- The FTC's *Protecting Personal Information – A Guide for Business*, and other important resources are also available at www.ftc.gov/infosecurity.
- The original ethics guideline incorporated four main points as baseline requirements for marketers:
  1) creating policies for an overall "culture of security"
  2) developing security standards and training employees
  3) incorporating the use of appropriate technologies, and
  4) informing business partners of their responsibilities to adhere to the same

standards

- Without a corporate standard of security ethics and the proper training, structure and technologies, it would be difficult to reassure consumers of your intentions and ability to keep personally identifiable information secure.

The DMA Board of Directors, in May 2008, approved updates to the guideline, in three important ways:

Primarily, it added a new (fifth) bullet to address the important issue of security breaches and what a marketer's responsibility is to consumers if information has been compromised. The following factors include the reasoning for adding to the guideline in this way:

- Since the original guideline was approved, the issue of security breaches has emerged as an important concern. Over the past couple of years, breaches have occurred in numerous ways – through identity thieves posing as customers, stolen laptops, lost computer disks, and other means.
- The media attention serves to hurt consumer trust.
- Several states quickly passed "notice of security breach" laws.
- The federal government has been considering a law, but has not yet come to a consensus.

This addition is meant to convey that:

- Marketers should inform consumers when a breach occurs that involves sensitive information (generally defined as including financial account data, medically-related information, children's data, or Social Security numbers) that was not encrypted.
- In general, marketers should not have to advise customers of a security breach when the information lost or stolen was encrypted.
- Personally identifiable information such as name and address, and public or publicly available information would not normally be considered sensitive.
- *However,* in determining whether to inform consumers of a security breach, marketers should consider how the information about consumers was used. Even if the information is not normally thought to be "sensitive," its uses may be considered sensitive to some consumers. For example, consumers ordering certain health-related items or subscribing to adult magazines may be highly upset if their name and address and order information were misused as a result of a security breach.
- "Material harm" to the consumer generally means when unencrypted sensitive information was lost/stolen and such loss could lead to significant financial harm to the consumer, including identity theft.
- It would not make sense to require that marketers inform consumers of every incidence a file containing data may be temporarily misplaced, as that would be unnecessarily alarming to consumers.

The third bullet was revised to add that marketers should also employ and routinely reassess "data retention, destruction, and deletion practices." Such addition was meant to address this emerging issue (being discussed by Federal Trade Commission staff and legislators) as a consumer protection tool to fight identity theft.

Lastly, the fourth bullet added the terms "contractually require" in order to reinforce that marketers should require their business partners and service providers to handle personally identifiable information at an acceptable level of security. Entering into a contract that requires acceptable data handling is a stronger standard of care than merely "informing" business partners.

Questions to Ask:

1) In regard to **Establishing information security policies and practices:**

- Have you established an internal culture of security and its supporting infrastructure, including a formal written plan?
- Do you believe all employees understand the importance of keeping information secure?
- Do you maintain confidentiality statements signed by employees when they are hired?
- Do you regularly review your information security policies and practices?
- Does your company maintain an adequate budget for security tools?
- Have you considered employing network security specialists to assess your policies and practices, perform risk assessments and audits, and assist your company with compliance?
- Do you report cyber attacks to law enforcement agencies?
- Have you considered liability insurance coverage in case of any security breaches?
- Have you created and tested a data recovery plan in case of a natural disaster?
- Has your company established a dispute resolution plan in case of disputes arising out of security breaches or alleged misuse of personally identifiable information?

2) In regard to **Establishing staff policy and training measures:**

- Have you designated responsible staff to design written information security policies and practices and ensured their implementation throughout your company? Do you feel confident that you have sufficient full-time staff available for your security program?
- Have you developed documentation and training materials to educate appropriate staff on the importance of information security and their responsibilities related to it?
- Do you perform background checks as necessary before hiring employees who would handle sensitive information, such as financial or medical data, or data about children?
- Do you verify employee qualifications regarding information technology, to avoid security breaches due to employees' lack of technological ability?
- Do you review your information security policy with appropriate employees, as indicated by their position or function, promptly upon their being hired, and regularly thereafter?
- Do you routinely audit your information security practices or systems (including when changes to the practices or systems are made) to assure accurate execution and to assess vulnerabilities? Do you revise your practices as necessary?
- Have you decided what information is sensitive and who has access to such information? Have you established a process for classifying data, and appropriate levels of security for each data class?
- Do you routinely monitor employee access to and use of personally identifiable information?
- Have you set forth penalties for breaches of information security by employees and promptly implemented them upon discovery of any information security breach?
- Upon termination of employees, do you ensure that appropriate processes are changed?

3) In regard to **Employing physical safeguards and technological measures, including data retention, destruction, and deletion practices, to ensure security of consumer information:**

- Do you define information security specifications for all new technologies, products, and data uses, and for system developments?
- Have you considered diverse or redundant solutions for high-risk systems?

- Do you take steps to understand the security impact of any new technologies, products, or data uses?
- Do you use current virus protection programs to protect information and do you update them regularly?
- Do you pay attention to security "alerts" released by software vendors?
- Do you employ firewalls to protect personally identifiable information?
- Do you change passwords routinely and use passwords with multiple numbers and symbols?
- Do you put into place authentication measures, as they are available, in order to verify personnel and consumer use and access to personally identifiable information?
- Do you test information security systems to ensure that specifications are met and that data are secure in storage and in transit? Do you check with your software vendors to make sure they have tested their applications before public release?
- Do you compile and review audit logs for attempted intrusions?
- Are you able to identify potential security breaches before they occur? Do you use software patches as needed?
- Have you created an incident recovery/back-up plan, including backup software and a secondary site to maintain data, in case of any breaches in your information security systems?
- Do you have policies regarding how long customer data should be retained?
- Have you considered different retention and destruction standards considering the type of data, for example, typical personally identifiable data such as name, address, and what was purchased versus sensitive data such as credit card or other financial account information, health-related data, data about children, Social Security numbers)?
- How would your customers (and potential customers) view your data retention, destruction, and deletion practices (for example, is it a positive customer service when consumers do not have to give out credit card information they previously provided)?
- How are customer data protected?
- How should data be disposed of or destroyed? Have you put into place a system to eradicate data from equipment prior to disposal?
- Are sensitive data (specifically, financial, health, children's, Social Security) encrypted?

4) In regard to **Contracting with business partners and vendors to ensure consistency with the marketer's own security policies:**

- Do you consider security ramifications before sharing networks with your business partners and vendors?
- Do you assure yourself that you understand the nature of any intended use of a list and that the list does not violate any of the ethical guidelines?
- Do you decoy and monitor the data practices of your business partners?
- Do you take steps to avoid unusual or suspicious list requests?
- Have you considered a sample notice to your business partners and vendors, for example: *[Marketer's] security policies are set forth below. [Marketer] expects [partner/vendor] to ensure that its security policies are consistent with and do not compromise [Marketer's] protection of personally identifiable information in any way.*

5) In regard to **Informing consumers of a security breach:** (several points relevant to security breaches are also asked in 1 – 4 above)

- Do you have a plan for informing consumers in the case of a security breach that warrants disclosure (e.g., information was of a sensitive nature and was not encrypted)?
- Are there others (in addition to consumers) who need to be notified of the breach?

- Have you considered providing any assistance to consumers (in the form of credit report monitoring, etc) if sensitive information was breached?
- Have you taken steps to close off existing vulnerabilities and threats?

Online Marketing

This section of the guidelines covers Online Information, Commercial Solicitations Online, E-Mail Authentication, Use of Software or Other Similar Technology Installed on a Computer or Similar Device, Online Referral Marketing, and E-mail Appending. These guidelines are minimum standards DMA members are required to follow when marketing online. "Best practices" examples are given for those marketers wishing to exceed the basic standards.

Online Information

Article #38

Notice to Online Visitors

1. If your organization operates an online site, you should make your information practices available to visitors in a prominent place on your Web site's home page or in a place that is easily accessible from the home page. The notice about information practices on your Web site should be easy to find, read, and understand so that a visitor is able to comprehend the scope of the notice. The notice should be available prior to or at the time personally identifiable information is collected.

Comment:

- One of the best ways to provide notice to consumers is to have a privacy icon or symbol on your home page that would link to your company's privacy policy. The icon could note "click here for our privacy policy" or words to that effect.
- Notice does not have to be on every page of your Web site in order to be conspicuous to consumers, but linking at all points where personally identifiable information is collected is the best way to ensure consumers will see your notice.
- "Easy to find, read and understand" basically means that your policy notice is available from your Web site's home page in readable print, not obscured by design elements, and that your privacy policy is written in plain English.
- Marketers need provide notice only if information about consumers is personally identifiable information, not if you just use aggregate data to help make improvements to your site.

Questions to Ask:

- Do you have a link to your policy in a prominent place or places on your Web site?
- Do you believe that the average consumer would view your privacy policy as prominent and easily accessible from your Web site's home page?
- Have you written your policy in plain, easy-to-read English so that it is understandable at a high school level?
- Are the print, format, and design of the text easy to read?

2. Your organization and its postal address, and the Web site(s) to which the notice applies should be identified so the visitor knows who is responsible for the Web site. You also should provide specific contact information so the visitor can contact your organization for service or information.

Comment:

- It increases consumer confidence to know your company's address. If consumers know where a company is physically located, they can more easily verify that the site they are viewing is the authentic Web site of your company. (Fraudulent operators can copy sites of reputable companies, harming both consumers and legitimate businesses.)
- Listing a physical address separates legitimate businesses from those who may be disreputable and do not want to be found. Law enforcement is facilitated when a physical address is listed, thus helping legitimate businesses as well.
- Consumers may need to contact your company for any of the following: to inquire about the status of a purchase they made, to seek help with a service problem, to get more information about one of your services (or for other reasons). If your company has different contacts for different purposes, you should list all of them on your Web site. Online contact information should be available since the consumer is presumably disposed to do business online.

Questions to Ask:

- Does your Web site include your company's physical address?
- Is it clear to consumers who is responsible for your Web site?
- Does your site include specific contact information that consumers can use to get their questions or concerns answered or to get the service they require?

3. If your organization collects personally identifiable information from visitors, your notice should include:

- ***The nature of personally identifiable information collected about individual visitors online, and the types of uses you make of such information, including marketing uses that you may make of that information.***

Comment:

- Consumer confidence is increased if consumers know what information is collected and how that information will be used.
- DMA's Online Privacy Policy Generator can assist you with developing your privacy notice. Your notice is essentially completed after answering a series of questions based on your company's information practices. This online tool can be found at www.the-dma.org/privacy/creating.

- The DMA has also developed the Children's Privacy Policy Generator to meet the notice requirements of the Children's Online Privacy Protection Act (www.the-dma.org/privacy/childrensppg2), and the GLB Privacy Policy Generator to meet the notice and opt-out requirements of the Gramm-Leach-Bliley Act (www.the-dma.org/glb/createprivacy).
- Personally identifiable information would include, for example:
  - e-mail addresses of visitors to your Web site;
  - e-mail addresses of those who post messages to your bulletin board;
  - e-mail addresses of those who communicate with your company via e-mail;
  - e-mail addresses of those who make postings to your chat areas;
  - user-specific information on what pages consumers access or visit; and
  - information volunteered by consumers, such as survey information and/or site registrations. (Information obtained in this way could include gender, age range, presence of children, presence of pets, income range, etc.)
- Information collected could be used by you in many different ways, among them:
  - for internal review and then discarded;
  - to improve the content of your Web page;
  - to customize the content and/or layout of your page for each individual visitor;
  - to notify visitors about updates to your Web site;
  - by your company to contact consumers for marketing purposes; and
  - given to other marketers or to agents.

Questions to Ask:

- Does your Web site notice clearly describe what personally identifiable information is collected?
- Does your notice state, in easily understandable terms, how each type of information will be used by your company?

➢ ***Whether you transfer personally identifiable information to third parties for use by them for their own marketing and the mechanism by which the visitor can exercise choice not to have such information transferred.***

Comment:

- If it is the case, consumers should understand that other marketers, besides your company, are using data about them. In order to gain consumer confidence and trust, marketers should focus on providing clear notice to consumers, and the opportunity for consumers to opt out of having information about them transferred to other marketers.
- Third parties who could be the recipient of personally identifiable information and use the data for their marketing could be unrelated entities, but could also include company affiliates, marketing partners, and cooperative databases.
- Requests for opting out of having information transferred should be honored promptly.

Questions to Ask:

- Does your Web site notice clearly explain whether personally identifiable information is transferred to third parties?
- Does the notice explain what relationship the third party marketers have with your company, for instance, an affiliate, a marketing partner, or a member of a cooperative database?
- Does your notice explain how consumers may request that information not be transferred?

- Do you have systems in place for promptly acknowledging and processing opt-out requests to prevent transfer to other marketers?
- Are the staff who handle customer service properly trained to identify and respond to such requests?

➢ ***Whether personally identifiable information is collected by, used by or transferred to agents (entities working on your behalf) as part of the business activities related to the visitor's actions on the site, including to fulfill orders or to provide information or requested services.***

Comment:

- "Agents" are the people working directly for you to serve and support your relationship with your customers. They are not the same as third party marketers.
- Agents include such service entities as delivery companies, print and letter shops, computer service bureaus, ad servers, fulfillment houses, credit card processors, and other companies working on the marketer's behalf to provide information or service to consumers.
- Consumers should be told that information has to be transferred to other entities so their orders and requests can be fulfilled.
- Marketers need to give notice of information transfer to agents, but do not need to give consumers the opportunity to opt out of transferring data to support their own orders. That is because opting out could not be honored, since transfer must take place in order for fulfillment and customer service to take place.

Questions to Ask:

- Does your Web site notice clearly explain whether personally identifiable information is collected, used by or transferred to agents?
- Does the notice explain that these are entities working on your behalf to fulfill consumers' requests?

➢ ***Whether you use cookies or other passive means of data collection, and whether such data collected are for internal purposes or transferred to third parties for marketing purposes.***

Comment:

- "Cookies" tag information about individuals and what they do online: a "cookie" is a note your Web site feeds to the consumer's computer when the consumer visits your site. If that computer returns to your site, your site will "recognize" the computer and you can present a targeted message or offer, based on past behavior.
- Cookies and other passive data collection tools, including Web "bugs," "bots," and "spiders," are often portrayed negatively and as intrusive to consumers' privacy. When these tools are used without consumer knowledge, consumers can be concerned that information is collected and used without their knowledge. Therefore, it is important for marketers to explain to consumers the positive ways in which cookies are utilized, and how consumers can benefit from their use. For example, cookies are used to personalize their visits, remember their preferences, or help tag items for their shopping baskets.

- Your notice should include not only how your company uses cookies, but whether information gained from cookies is made available to others for marketing purposes.
- Your notice should also inform consumers that, if they choose to, they can stop cookies by a setting in their browser.

Questions to Ask:

- Does your Web site notice state whether you use cookies or other passive means of collecting personally identifiable information?
- Does your notice state what you use the personally identifiable information collected from cookies for?
- Do you state whether you use information gleaned from cookies for internal purposes only, or are the data transferred to other marketers?

➢ ***What procedures your organization has put in place for accountability and enforcement purposes.***

Comment:

- The Federal Trade Commission and the European Union, among others, have identified the concept of "accountability" as one of the main "Fair Information Practices." Accountability means that you have a process in place that you follow to make sure you adhere to your privacy policy. It also means that if there is a privacy breach, there is an enforcement mechanism in place to fix the problem.
- This process and mechanism could be either internal or handled by some other entity you use to oversee adherence to your privacy policy. Such third party entity could include the Council of Better Business Bureaus, TrustE, or DMA.
- Your Web site notice should include a specific contact within your company, and/or the third party entity, for a consumer to contact regarding a question or problem with your privacy policy.

Questions to Ask:

- Does your Web site's notice include a contact consumers can use internally if they feel you are not living up to your privacy policy?
- Does your notice include what, if any, third party enforces your privacy policy on your behalf, including how to contact that entity in case of a dispute regarding your handling of personally identifiable information?

➢ ***That your organization keeps personally identifiable information secure.***

Comment:

- One of the biggest barriers to consumers conducting commerce online is the fear that information about them, especially sensitive financial information, may not be secure, and that they could be harmed by such crimes as credit card or identity fraud. You should, therefore, reassure consumers for the benefit of your company as well as the general well-being of the industry, that your company places a high priority on data security.
- Without divulging the particulars of how your company keeps information secure, your notice should indicate that you use up-to-date security protocols, both internally, such as keeping data physically secure, and externally, as when data may be transmitted or shared with others.

Questions to Ask:

- Do you have in place reasonable protocols and technologies to protect data in storage and in transit?
- Does your Web site explain to consumers in a reassuring way that personally identifiable information is kept securely?
- Have you reviewed DMA guidelines on security and *Information Security: Safeguarding Personal Data in Your Care* (see www.dmaresponsibility.org/InfoSecurity)?

4. If you knowingly permit network advertisers to collect information on their own behalf or on behalf of their clients on your Web site, you should also provide notice of the network advertisers that collect information from your site and a mechanism by which a visitor can find those network advertisers to obtain their privacy statements and to exercise the choice of not having such information collected. (Network advertisers are third parties that attempt to target online advertising and make it more relevant to visitors based on Web traffic information collected over time across Web sites of others.)

Comment:

- Consumers should be informed about third party network advertisers that collect data on your Web site. Likewise, they should be informed whether such data collected are transferred to third parties for marketing purposes.
- Third party network advertisers (also known as ad servers) should be specifically named, so that a visitor to your Web site knows who to contact to get information about that network advertiser's privacy policy and to opt out, if desired.
- Third party network advertisers' privacy policies themselves do not have to be included on your company's Web site; a link to each company and its policy is a recommended way of accomplishing consumer notice.
- As with cookies, it is recommended that you explain to consumers the purpose of allowing third party network advertisers to collect information on your site. (Unlike cookies, which visitors cannot see, "banner" or "pop-up" ads are quite visible; they are, in fact, designed to attract visitor attention and have the visitor click through for more information on the subject of the ad.) Visitors should be informed of benefits to them, such as providing a more positive shopping experience.

Questions to Ask:

- If you have relationships with network advertisers who collect information from your Web site, does your notice clearly state that this is the case?
- Does your Web site notice disclose who the network advertisers are, and provide a contact point for visitors to read their privacy policies and have the chance to opt out of information collection by each ad server?
- Does your Web site contain a link to network advertisers' privacy policy notices?

5. If your organization's policy changes materially with respect to the sharing of personally identifiable information with third parties for marketing purposes, you will update your policy and give consumers conspicuous notice to that effect, offering an opportunity to opt out.

Comment:

- "Doing the right thing" when there is a major change in your privacy policy means alerting consumers to any change that would affect the previous choices they made, and giving them the opportunity to react to the new policy.
- A material change, from the consumer perspective, is one where there are fewer restrictions placed on sharing personally identifiable information with third parties for marketing purposes. For instance, your policy may change from not sharing information with other marketers, to renting lists of customer names to other marketers. Or, you may begin participating in a cooperative database, in which personally identifiable information is shared with other catalogers.
- Marketers immediately incur additional business risks if their policies become less restrictive. Therefore, you should be prudent in making sure that you let visitors know as soon as possible about any less restrictive privacy policy. Make sure that you do not use personally identifiable information collected under the new policy until you have provided notice and allowed a reasonable time period for consumers to opt out of having information shared from that time forward. Thirty days is a reasonable time for consumers to respond to your notice.
- Your policy cannot be changed retroactively; in other words, data collected under your old policy cannot be used as per your new policy without notice to the consumer.
- At a minimum, you should post clear and conspicuous notice on your Web site that alerts visitors to the policy change. Other ways of "conspicuously" notifying consumers include, for example, "pop-up" notices or flashing signs on your Web site which serve to inform returning visitors to click onto your new privacy policy, or sending e-mail notices to consumers.
- You can assume after a reasonable time period that consumers who have not opted out do not object to the new policy. Notwithstanding this, however, it may be more prudent to honor the consumer's choice regarding data collected under your old policy if you don't hear from the consumer.
- Requests for name removal should be honored promptly.

Questions to Ask:

- Do you have a mechanism or system in place for promptly notifying consumers of any material change in your privacy policy?
- Does your new notice clearly explain the nature of the change?
- Do you allow enough time (at least 30 days) for consumers to review the notice and respond with an opt-out request, if they desire?
- Do you have a system for tracking consumers who let you know that they do not want personally identifiable information shared under your new policy?
- Do you promptly honor requests for name removal?

Honoring Choice

You should honor a visitor's choice regarding use and transfer of personally identifiable information made in accordance with your stated policy. If you have promised to honor the visitor's choice for a specific time period, and if that time period subsequently expires, then you should provide that visitor with a new notice and choice. You should provide choices of opting out online. You may also offer opt-out options by mail or telephone.

Comment:

- Not adhering to your own privacy policy is a breach of industry self-regulation and consumer confidence, and of federal law.
- Time frames for honoring privacy choices can differ from marketer to marketer, including anywhere between a year and infinity, for example. Since consumers' e-mail addresses frequently change, many online marketers choose limited time periods.
- If your notice's stated time period is expiring, then the visitor should be furnished a new notice and choice.
- Notice should ideally be furnished by e-mail, but it could be furnished by posting a notice on your Web site. The Web site could indicate, for example, that visitors' requests not to have data about themselves shared one year ago are now expiring. The notice would ask visitors to register their preferences again.
- Most consumers would reasonably expect that if they do not register a new preference, information about themselves would not be used after the stated time period.

Questions to Ask:

- Does your Web site policy indicate a specific time for honoring visitors' privacy preferences?
- Do you have a mechanism or system for alerting consumers that the time has lapsed and they should re-register their preferences with you?
- Do you offer opt-out choices by e-mail?
- How do you track Web site visitors who saw the new notice and opt-out option?
- Do you discontinue the use of data provided by consumers before the time expiration if they do not register their choices again?

Providing Access

You should honor any representations made in your online policy notice regarding access.

Comment:

- Some companies offer the opportunity to consumers to check their transaction records and to correct inaccurate data. If your company makes any public statements about consumer access to information, the promises should be kept.
- Individuals usually request access to data, such as contact information, registration, application or enrollment information, consumer preferences regarding information exchange, and recent transaction/purchase information in order to assure their accuracy.
- DMA recommends that you give consumers "reasonable access" to the information that will answer these customer service questions. You should also take reasonable steps to verify the identity of the individual requesting access, indicate a time frame to the consumer in which the request will be honored, and make requested corrections as appropriate.
- Consumers should agree to any fees you may charge for data access before work is initiated to retrieve the requested data.

Questions to Ask:

- Does your company state in its privacy policy or elsewhere that consumers can have access to information about them?
- If so, does your policy state what your procedures are for releasing information to requesting individuals?

- Have you trained your customer service personnel to identify and properly handle or refer requests for access?
- Have you assigned particular staff to handle consumer requests for access to data (and correction, if appropriate)?
- What kinds of information do you make available, and how far back in time do you research your records?
- Do you make a reasonable effort to verify the identity of individuals before releasing information to them?
- If you charge a fee for accessing information, do you notify consumers of the fee and get their permission before proceeding?

Data Security

Your organization should use security technologies and methods to guard against unauthorized access, alteration, or dissemination of personally identifiable information during transfer and storage. Your procedures should require that employees and agents of your organization who have access to personally identifiable information use and disclose that information only in a lawful and authorized manner.

Comment:

- It is important to maintain data security, and to let your Web site's visitors know that your company keeps personally identifiable information secure, in order to build consumer trust.
- For assistance, see the security checklist developed by DMA in conjunction with the FTC at www.dmaresponsibility.org/InfoSecurity, and other resources listed under Article #37.

Questions to Ask:

- Has your company implemented measures to provide secure transactions for consumers?
- Are you confident that data are kept physically secure when in storage, and in the process of transfer?
- Do you use current security and encryption technologies to ensure that consumer data are secure?
- Do you have a security policy concerning employee and agent access to data?
- Are employees instructed on your security policy and routinely monitored to ensure their compliance?
- Are visitors to areas where personal data are stored and processed specifically authorized?
- Are your security practices routinely audited to assess any weaknesses and to assure that policies are followed?

Visitors Under 13 Years of Age

If your organization has a site directed to children under the age of 13 or collects personally identifiable information from visitors known to be under 13 years of age, your Web site should take the additional steps required by Article #16 of the Guidelines for Ethical Business Practice and inform visitors that your disclosures and practices are subject to compliance with the Children's Online Privacy Protection Act.

Comment:

- Article #16 of the *Guidelines for Ethical Business Practice* says, among other things, that marketers should not collect personally identifiable information online from a child under 13 without prior parental consent or direct parental notification of the nature and intended uses of such information online and an opportunity for the parent to prevent such use and participation in the activity.

Questions to Ask:

- Is your Web site directed to visitors under the age of 13, or does your company collect personally identifiable information from visitors who are under that age?
- Do you have systems in place and staff responsible for assuring adherence to the Children's Online Privacy Protection Act (COPPA)?

The DMA has tools you can use if you market online to children:

The Children's Privacy Policy Generator was designed to meet the notice requirements of the Children's Online Privacy Protection Act (COPPA). Like the Privacy Policy Generator, a marketer answers a series of questions online about its information collection and sharing practices, which generates a customized policy to be modified and reviewed and then posted on your Web site. The Children's Privacy Policy Generator can be found at: www.the-dma.org/privacy/childrensppg.

How to Comply with the Children's Online Privacy Protection Rule was developed in cooperation with the Federal Trade Commission to help marketers understand and comply with COPPA, a federal law implemented by the FTC. It is located online at: www.the-dma.org/privacy/HowtoComplywithCOPPA-PDFVersion.

Accountability

There should be a meaningful, timely, and effective procedure through which your organization can demonstrate adherence to your stated online information practices. Such a procedure may include: 1) self or third party verification and monitoring, 2) complaint resolution and 3) education and outreach. This can be accomplished by an independent auditor, public self-certification, a third party privacy seal program, a licensing program, membership in a trade, professional or other membership association or self-regulatory program, or being subject to government regulation.

Comment:

- You should advise visitors of procedures your organization has put in place for accountability and enforcement. Accountability means you have a process in place that you follow to make sure you adhere to your privacy policy. It also means that if problems occur, there is an enforcement mechanism to correct them.
- There are several ways in which you can be held accountable to your online privacy policies, including the following examples: being a member of a trade association, such as DMA, which administers a membership seal and the Commitment to Consumer Choice and has enforcement capabilities; applying for a third party privacy seal program, such as TrustE or the Better

Business Bureau's online seal; or having an independent firm audit your company on a yearly basis.

- Your company may also monitor itself and have an internal compliance and complaint resolution process.
- Whatever your accountability mechanism is, you should summarize it on your Web site in plain English so that it is easy for visitors to understand and use.

Questions to Ask:

- Do you have a procedure or program in place that holds your company accountable for its information practices?
- Are your employees knowledgeable as to what the procedure/program is?
- Do you notify Web site visitors about your procedure/program and how to access it if they have a dispute regarding your privacy practices? Does your notice include specific contacts, including at any third party organization you may be responsible to?
- Do you maintain records as to any monitoring program you have in place?

COMMERCIAL SOLICITATIONS ONLINE

Article #39

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 assurances 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 online suppression list.**

Comment:

- Marketers need to be in compliance with the federal CAN-SPAM law. DMA's FAQs (www.the-dma.org/cgi/member/spamfaq), and graphic representations of legitimate vs. misleading or fraudulent e-mail (www.the-dma.org/antispam/E-mail_Chart.pdf) should be consulted.
- "Affirmative consent" is when the consumer has to take an action before being added to an e-mail list, for example, through a check-off box. It is another way of saying "permission was granted" or "the individual said *yes*" or "the consumer opted in." The overriding principle here is that consumers on your lists, and on lists you received from others should have either agreed to receive e-mails, or, at a minimum, should have been given notice and the choice to opt out.

- Online "solicitations" are e-mails that are sales messages or advertisements. If you send an e-mail notifying a consumer on the status of an order, or any other customer service matter, such as updating account information, or acknowledging a transaction, payment, or communication, that is not a solicitation and these guidelines would not apply. When such customer service messages and sales messages or advertisements are combined within the same e-mail, these guidelines would apply.
- Point one is the principle that you can contact your own customers online, even if the prior relationship with them was conducted in another medium. This also allows for e-appending, for example, obtaining your customer's e-mail address from a directory or listing based on their physical address information. "Customers" include individuals with whom marketers have previously conducted business (e.g., they have made a purchase or donation) or individuals who have contacted a marketer or the marketer's agent and included their e-mail addresses. Examples of such contacts could include requests for information, responses to questionnaires or surveys, product registrations, or responses to sweepstakes or contests.
- Points two and three apply to your own actions: that consumers gave you permission to contact them by e-mail, or they did not opt out of receiving e-mail solicitations when you provided them notice. The guideline allows you to send individuals (customers or prospects) at least one e-mail solicitation, and if recipients do not ask you to stop, you can continue to send them solicitations online.
- Since point four relates to third party lists, permission would have been granted to the third party marketer (or the marketer's agent) who is sharing the e-mail list with your company. In other words, it is the original marketer's responsibility to provide the individual with notice and an opt-out opportunity (for example, a check-off box) before renting or exchanging the e-mail addresses with your company.
- Your responsibility is to ask the list provider whether permission was granted or opt-out notice was given, and to be reasonably reassured of the answer before proceeding to send e-mail solicitations to consumers on the list.
- Marketers should be aware that some Internet Service Providers (ISPs) have policies to block the receipt of unsolicited commercial e-mail. A marketer should take into account the e-mail policies of the destination ISP because that is one way of ensuring that your messages will be delivered.

Questions to Ask:

- Do you ask your customers whether they wish to receive e-mail communications, including solicitations, from your company and from other marketers? Do you provide a means for individuals to easily register their preferences?
- If you e-mail commercial solicitations to individuals who are not currently your customers, do you have their consent to receive solicitations? Or, have the individuals on your list previously been given notice and the opportunity to opt out of receiving commercial e-mail from your company?
- If you receive an e-mail list from another entity, have you asked that list provider whether the individuals on the list have given permission to receive e-mail solicitations? Or, do you know whether the individuals on the rented list have been provided notice and the opportunity to opt out of having their names transferred?
- Do you include a provision in your list rental contract stating that list providers must obtain consumer permission or give notice and opt out to consumers?
- If you rent your customer lists to other marketers, do you first ascertain how the lists will be used, to make sure they are not used for promotions that may violate any of the *Guidelines for Ethical Business Practice*?

- Do you know the policies of major destination Internet Service Providers concerning the sending of e-mails?

Best Practices:

- Include a link to your privacy statement at the point of collection of an e-mail address, as well as each subsequent e-mail, for easy access to your notice.
- At the point of collecting consumers' e-mail addresses (either online or offline), provide consumers with a clear and conspicuous way to find out how the marketer will use their e-mail address.
- Ask consumers whether they want to receive solicitations by providing an unchecked box for them to check their preferences.
- Send an e-mail acknowledging that you are in receipt of their agreement to receive e-mails from you and/or from third party marketers.
- Include some reference within the first e-mail message to remind customers how you obtained their e-mail address, what they signed up for, and why they are receiving the e-mail. When using a third party list, the source should be identified in your solicitation to remind the consumer of where the permission was granted.
- One way to be reasonably reassured as to whether permission was granted, or opt-out notice was given, to a list provider is to include a provision in your list rental contract that states the obligation of the list provider to obtain consumer permission or give notice and opt out.
- Test the mechanism third-party list providers used to obtain a list before using their list to make sure that consumers receive adequate notice and the opportunity to opt out. Test where and how e-mail addresses are collected to be sure that your intended list use is consistent with how it was advertised and that it abides by these online guidelines.
- Familiarize yourself with the e-mail policies of the top Internet Service providers before sending e-mails to their subscribers.
- Familiarize yourself with the e-mail policies of the top Internet Service Providers before sending e-mails to their subscribers.

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 ten 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.

Comment:

- This part of the guideline states that every commercial e-mail you send should allow consumers to tell you that they want you to stop sending such e-mails, and that their names should not be included on lists you transfer to other marketers.
- Specific instructions on how to opt out do not need to be included in the e-mail itself, though they could be. An example of unsubscribe language would be: "To unsubscribe from this e-mail list, reply to this e-mail with *unsubscribe* in the subject line."
- A link to a suppress mechanism with instructions as to how to opt out also fulfills this requirement. The link should say something to the effect of: "Click here for unsubscribe options." Note that simply providing a link marked *"Privacy Policy"* does not make clear to consumers how they can opt out of receiving future e-mails from your company.
- Any consumer requests for suppression should be honored, and action should be taken expeditiously. Consumers would reasonably expect that, in the online medium, you would be able to act on their requests quickly. The CAN-SPAM law requires that opt-out requests be honored within ten business days, and that the opt-out mechanism be active for at least 30 days from the date of the solicitation. (This and other relevant Guidelines were amended to reflect specific requirements of CAN-SPAM.)

Questions to Ask:

- Do all of your e-mail solicitations include a notice of how the recipient can request not to receive future e-mails from your company? Do the e-mails include notice of how the recipient can opt out of having his or her e-mail address transferred to other marketers?
- If your e-mails include a link to a suppress mechanism on your Web site, is the description of the link clear?
- Do you have in place a system for removing, as requested, individuals' e-mail addresses? Do you let individuals know their requests have been taken care of?
- Are you operating in accordance with CAN-SPAM?

Best Practice:

- To ensure that an e-mail address can be accurately matched and suppressed, a marketer should include the consumer's e-mail address in the unsubscribe instructions. For example, "You are currently subscribed as name@domain.com. Please reply with "unsubscribe" in the subject line if you no longer wish to receive your weekly updates."
- Provide a clear and easy method for consumers to opt out -- for example, a link to a one click away unsubscribe mechanism for your e-mails.
- Unsubscribe requests should be processed automatically and promptly, upon receipt. (Where a system is not in place for automatic suppression, a reasonable time frame -- which is required by law -- is to suppress the e-mail address within 10 business days.)

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.

Comment:

- Consumer notice of information exchange with third parties is not applicable in situations where you do not exchange or transfer information to other marketers.

Questions to Ask:

- If you transfer information to other marketers, do you provide notice and the opportunity to opt out to individuals on your list?
- Do you honor any opt-out requests within 10 business days, as required?
- Do you honor such opt-out requests permanently, per the CAN-SPAM Act?

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.

Comment:

- Following the same principle as with the Mail Preference Service, marketers must remove individual names before prospecting, according to the wishes of individuals who register for DMA's name-removal services.
- You do not need to remove your own customers who may be on e-MPS because you have a business relationship with them. Similarly, individuals who have checked opt-in boxes or otherwise gave permission to receive commercial e-mail can be contacted. (Although it is not required when the lists you use are permission-based, using e-MPS can provide an extra level of privacy protection for those consumers who are especially concerned about privacy.)
- Even if someone is given an opportunity to opt out of e-mail address sharing originally, any marketer who rents the e-mail address for prospecting should use e-MPS for suppression.

- Service providers that are DMA members are required to take steps to comply with these guidelines, including endorsing use of DMA's e-MPS file and documenting efforts to encourage their clients to comply.
- Subscriber information for e-MPS is available (in downloadable form) at **www.preference.the-dma.org/products/empssubscription**.

Best Practice:

You should use and/or inform all DMA member clients that they should use e-MPS when processing third party e-mail lists, and require all non-member clients who refuse to use e-MPS in connection with third party e-mail lists to sign an appropriate waiver acknowledging their refusal to use e-MPS as requested.

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.

Comment:

- Individuals should be able to easily understand who sent the e-mail they received. The subject line should not claim "your personal account information attached" if that is not the case or is not the primary purpose of the e-mail, for example, because such a heading has the potential to mislead. Likewise, a subject line should not state "Open this for your free gift" unless there is an attachment with a certificate for merchandise or service that can be obtained without conditions to the consumer.
- The use of invalid, forged, or fraudulent information used to direct messages (e.g., making it appear as though the e-mail were from a different entity), use of invalid or non-existent domain names, or any other means of deceptive addressing is not appropriate or acceptable, and is illegal. Legitimate marketers do not use techniques meant to obscure the source of the e-mail.
- If you use an agent to deliver your e-mail campaigns on your behalf, it is not considered fraudulent to publish the marketer's name in the "from" line.
- It should always be possible to send a reply to an e-mail, and the full e-mail headers should accurately identify the sender of the e-mail as specified in standard mail transfer protocol ("SMTP").
- This guideline does not mean that the e-mail or its subject heading must include "ADV" or "this is an advertisement" or similar terminology (unless such language is required by the laws of the states into which you are sending e-mail). However, it should be understood by the recipient that the e-mail is an advertisement.
- Consumer confidence is greatly enhanced if the e-mail includes specific contact information for your company. Your company's physical street address should be included in the e-mail.

- To assist e-mail marketers who wish to improve their response rates and best practices education, DMA has developed seminars, white papers, research, and regular educational opportunities. To find out more, refer to www.the-dma.org.

Questions to Ask:

- Do consumers reasonably understand that the e-mail is a sales message?
- Are consumers able to easily see that the e-mail is from your company? Is your company's physical street address on the e-mail itself?
- Does the e-mail include specific contact information so that the recipient can obtain information or service?
- Is the e-mail straight-forward in its message and unlikely to be misconstrued?
- Does the subject line reflect the actual content of the e-mail's message?
- Have legal counsel reviewed your e-mail for compliance with the CAN-SPAM law?

Best Practice:

Certain types of e-mail including fraudulent and deceptive marketing messages are regulated by the Federal Trade Commission (and some states) and marketers who violate these laws can be held accountable and fined accordingly. Marketers should help fight fraud by reporting what they believe to be deceptive e-mail solicitations to the Federal Trade Commission at *spam@uce.gov.*

E-MAIL AUTHENTICATION

Article #40

Marketers that use e-mail for communication and transaction purposes should adopt and use identification and authentication protocols.

Comments and Questions/Answers:

- DMA's Board of Directors approved this guideline in October 2005, with this member requirement taking effect February 1, 2006. The following explains what authentication is, and what DMA members should do to implement the guideline within their companies.
- Authentication improves the likelihood that legitimate e-mail will get through to the intended recipient. Additionally authentication reduces the likelihood of spam, spoofing and phishing attacks, thus protecting the integrity of marketers' brands. It is seen as one way of making the electronic marketplace more secure and improving consumer confidence in e-mail, thus preserving it as a valuable marketing communications tool.
- DMA's guideline requires marketers to choose and implement authentication technology into their e-mail systems. It is up to your company to decide what kind of authentication protocol to use. DMA does not require the use of any specific protocol, as there are several interoperable, inexpensive, and easy to implement solutions available on the market today.
- The guideline applies only to **outbound** e-mail that marketers send either from their own IP addresses or via the use of a service bureau. (It does not cover inbound e-mails.)

- The guideline applies to **ALL** outbound messages that marketers send or that their service bureaus send on their behalf (including transaction-related messages).
- DMA believes that the same care in e-mail deliverability for consumer promotions should be used for business-to-business campaigns.
- Nonprofit organizations, as well as for-profit businesses, should authenticate the e-mail messages they send.

E-Mail Authentication Technology Basics FAQs

Q: What is an E-mail Service Provider (ESP)?
A: An E-mail Service Provider is an entity that sends e-mail on behalf of a marketer.

Q: What is an Internet Service Provider (ISP)?
A: An Internet Service Provider is a service provider that provides access to the Internet and/or an e-mail account.

Q: What is the Difference Between IP-Based Authentication and Cryptographic Authentication?
A: There are currently two major types of interoperable e-mail authentication systems: IP-based solutions like Sender Policy Framework (SPF) and Sender ID Framework (SIDF), and cryptographic solutions like DomainKeys Identified Mail (DKIM). The goal of each is the same, which is to create a public record against which to validate e-mail messages so that the legitimacy of senders can be verified. Both technologies work to verify that the sender is authorized to send mail from a particular IP address. Authentication makes it difficult to forge IP addresses or the cryptographic signatures utilized by e-mail authentication systems.

A fundamental difference between IP-based and cryptographic authentication solutions is that cryptographic technology protects the integrity of the e-mail contents, while IP-based technology verifies or proves that the sender is authorized by the domain owner to send the mail.

Q: What is the Domain Name System (DNS)?
A: The Domain Name System (DNS) is an Internet directory service. DNS is where companies publish which IP addresses are allowed to send e-mail on their behalf.

Implementation FAQs: Three Complementary Types of E-Mail Authentication Systems: SPF, SIDF and DKIM

Sender Policy Framework (SPF)

Q: What is Sender Policy Framework (SPF) and How Does It Work?
A: SPF is an IP-based technology that verifies the sender IP address by cross-checking the domain in the e-mail address listed in the visible "Mail From" line of an e-mail against the published record a sender has registered in the Domain Name System (DNS). SPF technology is free to all users. An SPF record is a list of computer servers or IP addresses that senders indicate are "authorized" to send e-mail that claims to be coming from their domain. When you publish an SPF record for your domain, you declare which IP addresses are authorized to send out e-mail on your behalf.

SPF allows senders/marketers effectively to say, "I only send mail from *these* machines (IP addresses/servers). If any other machine claims that I'm sending mail from there, they are not telling the truth."

Q: How Do I Implement Sender Policy Framework (SPF)?
A: 1. Audit and make a list of all IP addresses that send e-mail on your behalf. Talk to your IT staff and any E-mail Service Providers you work with.

2. Create your SPF record:
Use this SPF Setup Wizard to publish which IP addresses and servers you use to send e-mail messages: http://www.openspf.org/wizard.html.

3. Publish your SPF record in DNS.

4. Verify that your SPF record is published and working:
a. Use the tool at: www.dnsstuff.com.
b. Copy all the information after the "@" sign in the "From" line of the domain you wish to verify (e.g., @yourcompany.com).
c. Paste this information into the look-up field on the far right column (DNS Lookup).
d. Select the "TXT" option from the drop down box directly next to where you just pasted your domain information.
e. Select "Lookup."
f. Under the "Answer" box you should see "v=spf…" This verifies that your record is SPF compliant.

Sender ID Framework (SIDF)

Q: What is Sender ID Framework (SIDF)?
A: Sender ID is basically "Caller ID for e-mail." SIDF, created by Microsoft, is very similar to SPF. Whereas SPF verifies the visible "Mail From" line of the e-mail, SIDF authenticates either the "Mail From" line or the non-visible "From" line of the e-mail header.

Using the U.S. Postal Service as an analogy, SIDF is akin to verifying the authenticity of both the outer envelope and the letterhead on the document inside the envelope.

Q: How Does Sender ID Framework (SIDF) Work?
A: 1. Sender sends an e-mail to Receiver.

2. Receiver's inbound e-mail server receives the e-mail and calls its Sender ID Framework.

3. Sender ID Framework looks up the Sender ID or SPF record of the domain that Sender is using in the Domain Name System (DNS).

4. The recipient's ISP determines whether the outbound Mail Server IP address matches any listed IP address authorized to send mail for the user.

Q: How Do I Implement Sender ID Framework (SIDF)?
A: 1. Audit and make a list of all IP addresses that send e-mail on your behalf. Talk to your IT staff and any E-mail Service Providers you work with.

2. Use this four-step wizard:
Go to:
http://www.microsoft.com/mscorp/safety/content/technologies/senderid/

wizard/

3. Verify that your SIDF record is published and working:
   Port25 Solutions has created an automated testing tool to verify Sender ID implementation. To use the tool, send an e-mail message from the sending environment you wish to verify to check-auth@verifier.port25.com. (Leave the "Subject Line" and the body of the message entirely blank.) In return, you will receive a reply containing an analysis of the authentication status of the message you sent.

DomainKeys Identified Mail (DKIM)

Q: What is DomainKeys Identified Mail (DKIM) and How Does it Work?
A: DomainKeys Identified Mail is a cryptographic, signature-based type of e-mail authentication. DKIM is a combination of Yahoo's DomainKeys (DK) and Cisco's Identified Internet Mail (IIM). DKIM is offered to all users free of charge.

DKIM is available at http://domainkeys.sf.net. DKIM requires more computing resources than IP based technologies. DKIM requires e-mail senders' computers to generate "public/private key pairs" and then publish the public keys into their Domain Name System (DNS) records. The matching private keys are stored in a sender's outbound e-mail servers, and when those servers send out e-mail, the private keys generate message-specific "signatures" that are added into additional, embedded e-mail headers.

ISPs that authenticate using DKIM look up the public key in DNS and then can verify that the signature was generated by the matching private key. This ensures that an authorized sender actually sent the message, and that the message headers and content were not altered in any way during their trip from the original sender to the recipient.

The DKIM authentication process involves checking the integrity of the message using the public key included in the e-mail signature header, in addition to verifying whether the public key used to sign the message is authorized for use with the sender's e-mail address. This step currently involves utilizing the DNS record of the sending domain. The authorization records in the DNS contain information about the binding between a specific key and e-mail address.

In the U.S. Postal Service analogy DKIM is like verifying a unique signature, which is valid regardless of the envelope or letterhead it was written on.

Q: How Does E-Mail Authentication Reduce and Protect Against Spam?
A: Spam causes problems for both consumers and marketers. The spam problem is not going away, and spammers quickly adapt to filters set up by Internet and Mailbox Providers thus blurring the perception in consumers' minds of which commercial e-mail is legitimate and which is spam. Authenticated e-mail will help ISPs and Mailbox Providers better identify legitimate e-mail. Spammers will then be distinguished from senders of legitimate e-mail and reliably deliver wanted mail to consumers with higher certainty, and at a lower cost.

Example:

Using SPF technology, suppose a spammer forges an ABC.com address and tries to spam you. The spammer connects from somewhere other than ABC's e-mail servers. When the message is sent, you see "Mail From: <e-mailcustsvc@ABC.com>".

ABC publishes an SPF record. That record tells your ISP or Mailbox Provider how to find out if the sending machine is allowed to send mail from ABC. If ABC says they recognize the sending machine, it passes, and your ISP or Mailbox Provider can assume the sender is who it says it is.

Authentication combined with e-mail reputation and accreditation programs will ultimately help e-mail receivers distinguish legitimate messages from spam.

Q: How Does E-mail Authentication Help to Reduce and Protect Against Spoofing and Phishing?

A: Spoofing, a method often used by spammers, is the forging of another person's or company's e-mail address to get users to open a message. Phishing is sending an e-mail that attempts to trick recipients into giving out personal information, such as credit card numbers or account passwords. The e-mail pretends to be from a legitimate source, such as a user's bank, credit card company, or online Web merchant. Most phishing attacks come from e-mail in which the sender's name in the "From Line" has been forged or spoofed.

Authentication is predicted to cause a significant reduction in spoofing and phishing attacks because those particular elements of e-mail fraud are identity-based. Therefore, identity authentication will either stop phishing and spoofing, make it easier for consumers to steer clear of them, or make it easier for law enforcement to go after them.

For well-known companies that commonly send e-mail to consumers, such as banks, utilities, remote retailers, and e-commerce services, the benefits of authentication are more profound, as authentication can help them protect their users from phishing attacks. For these companies, protecting their users from fraudulent e-mails translates directly into user protection, user satisfaction, reduced customer care costs, and brand protection and trust.

Example:

Implementing DomainKeys Identified Mail (DKIM) can protect companies that are susceptible to phishing and spoofing attacks. Companies can sign all of their outgoing e-mails with DKIM and publish their policies so that ISPs can watch and block any messages that claim to come from their domains that are unsigned.

If the company 'www.example.com' signs all of its outgoing e-mail with DomainKeys, Yahoo! can add a filter to its spam protection system that blocks any unsigned or improperly signed messages claiming to come from the domain www.example.com, thus protecting tens of millions of example.com's customers (or prospective customers) from these phishing and spoofing attacks. DKIM also examines the integrity of the message body.

Beyond Authentication FAQs: E-mail Reputation and Accreditation

Authentication, accreditation and reputation are fundamentally linked. Implementing authentication without at least one of the other solutions would be unproductive, as each one contributes to the ultimate success of the others. Authentication compliance alone is not sufficient for Internet Service Providers (ISPs) to make deliver/non-deliver decisions. Authentication verifies authorization to send, but it doesn't tell mailbox providers anything about whether the authorized sender is legitimate or a spammer. This is where solutions like reputation, accreditation and/or white listing come into play.

Q: What is a Company's E-Mail Reputation?
A: E-mail Reputation is a way for ISPs to combine the sender's identity with additional information about the sender's practices. Reputation is based on numerous factors: complaint rates, identity stability, unknown user volume, security practices, unsubscribe policies, and more. Most of these factors can be measured, quantified and weighted by Internet Service Providers (ISPs) and E-mail Service Providers (ESPs).

Q: What Metrics Should I Monitor to Ensure That My E-mail Reputation is Good?
A: There are a few simple steps marketers can take to ensure that their E-mail Reputation remains in good standing with ISPs.

1. **Good List Hygiene:** Sending e-mail to too many addresses that don't exist isn't only a trait of spammers—it is a trait of any entity that is considered to have poor marketing practices and is sending spam. ISPs acknowledge that there is a lot of churn in terms of consumers changing e-mail addresses, and because of that they do allow for some margin of error. However, it is generally accepted that marketers should aim to keep "invalid" addresses at **less than 10%** of each mailing. Of course, reducing these types of errors isn't just good for deliverability, but for Return on Investment (ROI) as well.

2. **Sound E-Mail Sending Infrastructure:** A common trait of spamming is to redirect e-mail bounces and replies to spoofed, non-functional or non-existent return addresses. Therefore, to differentiate themselves, legitimate senders are expected to be capable of receiving the volume of bounces that typically accompanies any high volume e-mail campaign. Most ISPs require that e-mail senders are capable of receiving at least 90% of messages that are bounced back to them when they attempt to e-mail to an invalid or unknown addresses. When an e-mail sender does not accept the bounce back error replies it is considered suspicious behavior and the sender may be identified as a spammer. If an ISP becomes suspicious of an e-mail sender it may ask high volume e-mail senders to adjust the number of simultaneous connections to their networks. Or it may institute mail volume throttling (spreading out the number of e-mails sent over a long period of time).

3. **High Relevance/Low Complaint Rate**: Having good list hygiene and sound delivery infrastructure are the foundation to having a good reputation—but keeping complaint rates low is where a company can significantly improve or damage its reputation. The key to having a low complaint rate is making sure that your e-mail is relevant and delivers value to the recipient. In general, ISPs believe there should be little to no reason for a consumer to complain about legitimate e-mail. Marketers should aim to keep their complaint rate **below 0.1 percent**. The complaint rate is calculated by dividing the total number of complaints by the total number of delivered e-mails in a specific mailing. A mere two or three complaints out of a thousand e-mails delivered could result in short-term blocking by ISPs that employ reputation systems, and severe long-term blocking if the sender does not bring the complaint rate under control.

Q: What is Accreditation?
A: For companies who have authenticated their e-mail systems, and have established good e-mail reputations, accreditation is the next key to reaching the inbox. Accreditation systems analyze a company's e-mail program against a strict set of best practice guidelines, and if a program is accepted, e-mail sent by the company is exposed to less filtering by e-mail receivers. While there is no way to guarantee e-mail delivery, accreditation is the closest to a guarantee there is that receivers will accept an e-mail message.

Q: What is a Whitelist?
A: A whitelist is a list or process that some ISPs use to allow e-mail marketers to send e-mails to their networks without being subjected to certain (potentially stricter) levels of anti-spam filtering, for example volume filters. E-mail marketers can apply on ISPs Web sites to be added to existing whitelists.

Q: What is Enhanced Whitelisting?
A: AOL officially introduced the industry's first accreditation and reputation-based solution, the enhanced whitelisting program, more than a year ago. Similar whitelisting, accreditation and reputation-based systems are now in place at virtually all of the major ISPs (e.g., Yahoo, Earthlink, and MSN Hotmail) and enterprise spam filtering companies (e.g., CipherTrust and Symantec Brightmail). Enhanced whitelists provide senders with deliverability benefits including bypassing certain levels of filtering, inbox placement, and guaranteed full image and link rendering/display.

Senders who wish to be placed on enhanced whitelists must submit a certification application (form of accreditation) beforehand in which they attest that they meet and abide by the ISPs requirements. The agreement relates to, but is not limited to, CAN-SPAM compliance, list hygiene, e-mail deployment infrastructure capabilities, and bounced e-mail acceptance. After a sender has submitted an application the ISP will track and make assessments of the senders reputation based on observed marketing behavior and complaint rates against the sender's IP addresses.

Q: What is the Difference Between Pass, Fail and Softfail of an E-Mail Message?
A: If a message **passes** an ISPs authentication check it means the e-mail meets the standards for a ISPs definition of a legitimate message and is delivered to the recipient's inbox. If a message **fails** an authentication check it did not meet the standards for an ISP's definition of a legitimate message and will not be delivered to the intended recipient's inbox. It will either directed to the recipient's spam/junk folder, or the message may be blocked. A **softfail** is a message that is a "probable fail" according to the ISP's standards; A softfail message usually comes from a sender or IP address that is not listed on the ISP's list of authenticated senders but is not an outright failed message.

Q: What Are Feedback Loops?
A: Feedback loops are a system where some ISPs share spam complaints with whitelisted senders in order to unsubscribe complainants from their lists. Feedback loops are essential for marketers to identify and resolve high complaint e-mail campaigns and messaging streams emanating from their IP address/computer networks.

Best Practices for Implementing E-Mail Authentication Protocols

- Assign an individual or group at your company to be responsible for working with other relevant departments and vendors to implement e-mail authentication.
- Authenticate using more than one technology. SPF, SIDF and DKIM are interoperable free technologies that have different deliverability success rates with different ISPs. For best results, authenticate your e-mail systems with one or more technologies.
- Know your customers and where you are mailing.
- Follow developments in the field, including technological white papers and industry or government-sponsored workshops.
- Research the major protocols to determine the best solution(s) for your Company.
- Develop a policy for assigning domain and sub-domain names.

- Develop a way to measure the impact of e-mail authentication, in terms of higher deliverability to those you wish to reach.
- Research ways to authenticate incoming e-mail to your company.

There are many resources available on E-Mail Authentication. See DMA's E-Commerce Integrity Resource Center: www.dmaresponsibility.org/Ecommerceintegrity for more information.

USE OF SOFTWARE OR OTHER SIMILAR TECHNOLOGY INSTALLED ON A COMPUTER OR SIMILAR DEVICE

Article #41

Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (e.g., relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

*Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar

- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including Web beacons, are not governed by this Guideline. Article #38 provides guidance regarding cookies and other passive means of data collection.

Comment:

- DMA's Board of Directors approved this guideline (in January 2006) in order to assist members in defining minimally acceptable marketing practices in the area of software installation practices. (The Board also approved a six-month phase-in period to allow for any programming changes companies may need to make for implementation.)
- Software by itself is neutral, and the use of software and other similar technology to assist consumers is beneficial. This guideline supports DMA's vigorous opposition to the fraudulent, deceptive or unscrupulous use of software or other similar technology to harm the interests of consumers. The guideline's focus, therefore, is to prohibit practices that are deceptive. (Not all possible deceptive practices are listed, as new ones will, unfortunately, be implemented by unscrupulous operators in the future.) Controlling a user's computer and preventing users from uninstalling unwanted software are examples of deceptive or harmful practices.
- The guideline does not use terminology such as "spyware" or "adware." It was decided that the terminology used should be neutral and broad (e.g., "software and other similar technology") because of the continuous evolution of online technology. ("Spyware" or "malware" generally refer to software that has negative consequences for computer users, while "adware" generally refers to software that places legitimate advertisements.)
- Federal and state legislators are extremely concerned about the negative consequences of "spyware," or applications that harm users' computers in various ways, and have introduced numerous legislative bills. DMA ethics guidelines are meant to get "ahead of the regulatory curve" by demonstrating effective self-regulation.
- The guideline refers to "software or other similar technology installed on a computer or similar device" because it is meant to encompass such things as PDAs and MP3 players, etc. (and future similar inventions) as well as computers.
- The guideline does not include "cookies," "Web beacons," or other such passive means of data collection. Rather, it focuses on the effects of software that is installed on computers.
- By stating: "Anyone that offers software or other similar technology that is installed on a computer…," the guideline is conveying that there is broad responsibility for who is responsible for the software offer. Responsibility belongs to both the marketer and the service entity it may employ.
- The standard of giving computer users "notice and choice" before the software begins operating (or at the point of joining a service) is the DMA guideline. However, marketers can go beyond the basic standard if they choose, for instance, by getting users' affirmative consent beforehand.
- Marketers should not be held responsible for inactive software that may inadvertently remain on a user's computer. The guideline reads: "Give the computer user an easy means to install

the software or other similar technology and/or disable all functionality" because it is difficult to assure that each and every component of an installation can be completely removed. In addition, some effects of software installation, including changes to registry settings (i.e., configuration files within Windows) may go unnoticed.

- Reference to the "significant effects" of having software installed is not meant to be all-inclusive because new applications are always emerging.
- It is essential that marketers make sure they provide an easily accessible link to their privacy policy so that computer users can review what information may be collected as a result of the software installation, and how it may be used. Such transparency serves to encourage consumer trust in your company.

Questions to Ask:

- Have you assessed whether any programming changes are needed for implementation of the guideline, and made such changes?
- Have you reviewed your online privacy policy to make sure it appropriately covers significant effects, as outlined, of software installations?
- Is notice and choice provided to computer users easy to find, easy to read, easy to understand and easy to act upon?
- Have you been sure to identify the software being installed, as well as your company name and information, in case the computer user wants to contact you?
- Have you given users an easy means to uninstall and disable the computer software?

Best Practices:

- Marketers should get users' affirmative consent before computer software is installed and/or begins operating.
- Marketers should help users in not only uninstalling software, but making sure users' computers are returned to their original settings (prior to software having been installed).

ONLINE REFERRAL MARKETING

Article #42

Online referral marketing is a technique marketers use to get new marketing leads. Typically, the online marketer:

1. **encourages an individual to forward a marketing piece on to another individual (personally identifiable information is not collected), or**
2. **asks an individual to provide the marketer with personally identifiable information about another individual so the marketer may contact that person directly.**

This guideline relates only to the second type of online referral marketing above, where personal information about a prospect is given to the marketer.

A marketer should not use personally identifiable information about a prospect provided online by another individual unless:

- **the marketer has first clearly disclosed to the referring individual the intended uses of the information;**
- **the marketer has disclosed to the referring individual that their own contact information will be provided to those they have referred to the marketer;**
- **the marketer discloses to the referred person the fact that their contact information was obtained from another individual. The marketer should make the referring person's information available in the first e-mail communication to the prospect. Or, the marketer can tell the prospect how to get the referring person's contact information at no cost; and**
- **the marketer provides, in the first and any subsequent e-mail communications, the ability to remove the referred person's name from future contact.**

Marketers should not contact referred individuals who are on their in-house e-mail suppression lists, and should not sell, rent, share, transfer or exchange a referred e-mail address unless they receive prior permission from the referred person to do so.

Comment:

- DMA developed this guideline to promote ethical standards for "viral" marketing, which has a negative connotation, and to provide assistance to members needing guidance in the online medium. "Friend Get a Friend" promotions in the print medium have been in existence for years and have proven to be beneficial for both consumers and marketers. *Online* referral marketing also can be beneficial: consumers who receive marketing messages that resulted from friends or colleagues passing their names on to your company may be much more receptive and trusting.
- Much of online referral marketing is in the form of forwarding e-mail or Web site news articles on to others. This guideline, as noted, applies only in situations where a *consumer's personal information* is forwarded to the marketer, who then contacts the consumer.
- The guideline states that you should make the referring individual's name and contact information available in the first e-mail communication to the referred person, *or* that your first e-mail should inform the referred person how to get the referring individual's contact information.
- Each e-mail communication you send to the referred consumer should contain an opt-out option to allow the person not to receive further e-mails from your company.
- Although the guidelines do not address how frequently a marketer may e-mail a referred consumer who has not opted out, you risk annoying consumers by continuing e-mail communications in the absence of any positive response to your message. In the spirit of keeping your e-mail list clean and responsive, you may want to consider asking non-responsive

referred consumers for permission to continue contacting them. Some marketers delete the referred person's contact information after the referral e-mail is delivered. Any referred person who responds is, of course, a new customer whose contact information is again captured.

- Permission from the referred consumer does not need to be granted in advance of sending your initial e-mail communication, as noted. However, you cannot contact the consumer if the consumer is on your in-house suppression list. Further, you cannot *transfer* the consumer's information to any other marketer without the consumer's *permission* to take such action. "Permission" means the consumer affirmatively is notified and says "yes."
- The obligation to receive permission before transferring a consumer's referred e-mail address to another marketer stems from the fact that the referring individual provided the information only to you, not to other marketers. It would be a violation of the referring individual's intent and trust if the referred friend's e-mail address was provided to unknown marketers, resulting in additional and unwanted e-mail communications.

Questions to Ask:

- Do you disclose how information about referred persons will be used? And, do you let referred persons know who referred them, or at a minimum, make that information available in your first message at no cost?
- Do you offer the opportunity to opt out in the first e-mail? Is opt out available in any subsequent e-mail communications?
- Do you obtain the referred person's prior permission before transferring their e-mail address on to another marketer?

Best Practice:

Marketers should personalize the referral and communicate in the subject line why the consumer is being contacted, for instance, "Your friend, Adam Abel, thought you'd be interested in our electronic equipment."

E-MAIL APPENDING TO CONSUMER RECORDS

Article #43

Definition of e-mail address appending: E-mail address appending is the process of adding a consumer's e-mail address to that consumer's record. The e-mail address is obtained by matching those records from the marketer's database against a third-party database to produce a corresponding e-mail address.

A marketer should append a consumer's e-mail address to its database only when the consumer gives a marketer permission to add his or her e-mail address to the marketer's database; or

1. **There is an established business relationship with that consumer either online or offline; and**
2. **The data used in the append process are from sources that provided notice and choice regarding the acceptance of receiving third-party e-mail offers and where the consumer did not opt out; and**
3. **Reasonable efforts are taken to ensure the appending of accurate e-mail addresses to the corresponding consumer records.**

Marketers should not send e-mails to appended e-mail addresses that are on their in-house e-mail suppression files. A marketer should not sell, rent, transfer or exchange an appended e-mail address of a consumer unless it first offers notice and choice to the consumer.

All messages to an e-mail appended address should include a notice and choice to continue to communicate via e-mail.

Marketers should have in place appropriate record keeping systems to ensure compliance with these guidelines.

Comment:

- This guideline was written in response to questions received from DMA members and the press concerning the association's position on e-mail append. It is an expansion of DMA's previous commentary that e-mail appending was permissible for obtaining an existing customer's e-mail address.
- Some consumers may reasonably assume that a customer relationship based on one medium, for instance, mail, should not extend to other media. DMA's position, however, is that a *customer is a customer* regardless of the media – unless the consumer asks to be removed from a marketing channel.
- Like DMA's other online marketing guidelines, this guideline addresses only consumer e-mail addresses for appending, not business-to-business applications.
- This guideline stresses that if the consumer did not give you permission to have his or her e-mail address added to your database, three other factors must be in place: 1) you have a relationship with the consumer already in some medium and 2) the source of the appended information gave the consumer notice and the chance to opt out of receiving third party offers, and 3) the addresses you are attempting to append are real – not "mathematically guessed" or fabricated.
- The third-party databases do not need to be "opt-in" or permission-based sources, but they need to have offered notice and choice to consumers. Similarly, consumers must be given notice and the opportunity to opt out prior to the marketer transferring an appended e-mail address to other marketers. The purpose of these requirements is to avoid consumer annoyance or perceptions of intrusion by the receipt of e-mail offers from unknown third parties. Controlling the amount of perceived "spam" is increasingly vital because of the large volume of unsolicited commercial e-mail most consumers now receive.
- Marketers do not specifically need to communicate with consumers before adding their appended e-mail addresses to their databases, although they could send an e-mail to the effect,

"Since you are a valued customer, we would like to provide special sales notices to you via e-mail. If you would prefer not to receive e-mail from us, please let us know."

- Likewise, a marketer could send a message prior to providing a customer's e-mail address to another marketer, for example, "We received your e-mail address from another company you do business with. Before we send you offers we think you'll be interested in, we wanted to give you a chance to object. If you do not want us to contact you by e-mail, please click here."
- If a consumer decides not to receive future messages from you, that also automatically means that you may not transfer the consumer's name and e-mail address to another marketer.
- When you send commercial e-mail to appended consumer names, the first, as well as all subsequent, e-mail communications must offer a notice and removal option.
- Be sure to honor any removal requests within ten business days, as required by the CAN-SPAM federal law.
- Marketers should apply all appropriate suppression files, including DMA's E-mail Preference Service name-removal file for prospects who wish to reduce the amount of unsolicited commercial e-mail.
- The guideline requires that the appending process use appropriate technologies and methods to ensure the accurate appending of e-mail addresses to the corresponding consumer's record. Matching should be performed at the individual level (first name, surname, address) to ensure a high degree of accuracy. This is to avoid consumer receipt of random or erroneous e-mail communications.
- You should be careful not to reach out excessively to consumers who have not been responsive. If a positive response is not captured within a reasonable amount of time, you may wish to consider suppressing that appended record.
- You should be able to verify how e-mail appending is performed, and keep appropriate records in case you need to document your systems and procedures.

Questions to Ask:

- Are your e-mail communications practices in line with the federal law, CAN-SPAM, keeping in mind that the law does not exempt e-mail to existing customers?
- Do you use DMA's E-mail Preference Service prior to contacting prospects whose e-mail addresses were obtained from a third party?
- Does each e-mail you send to appended names contain notice and choice to allow removal?
- Do you assure yourself that sources used for appending provided notice and choice to consumers?
- Do you offer notice and choice to consumers whose e-mail addresses have been appended prior to transferring their e-mail addresses to other marketers?
- Do you have a system in place for automatically removing consumers' e-mail addresses upon request, and does that system remove addresses within ten business days, as required by federal law?
- Do you use appropriate record-keeping practices to document e-mail appending, as well as maintain records securely?

Telephone Marketing

Marketing by telephone became the subject of intense scrutiny by federal and state government agencies, industry critics and the media. Most aspects of telephone marketing are now regulated, and marketers are referred to resources that explain the relevant federal regulations in detail. Specifically, telephone marketers and service entities working on their behalf should consult DMA's website, www.dmaresponsibility.org, for detailed information on the revised Telemarketing Sales Rule, implemented by the Federal Trade Commission (see also www.ftc.gov), and the revised Telephone Consumer Protection Act, implemented by the Federal Communications Commission (see also www.fcc.gov).

Some articles in this section have been revised in order to be consistent with amendments to the Telemarketing Sales Rule and the Telephone Consumer Protection Act. Other articles go beyond what is legally required in order to proactively address problematic telemarketing practices. It is recommended that industry members adhere to these guidelines for consumer protection measures, as well as for protection of their ability to market via this medium in the future.

***Please note that DMA began to gradually phase out the Telephone Preference Service (TPS), referenced throughout this section. New consumer registrations for TPS are no longer being accepted. However, members must continue to suppress prospective customers listed on TPS through December 31, 2011 (thus honoring TPS registrant requests for five years). Additionally, TPS continues to serve as the official registry for the states of PA and WY.**

REASONABLE HOURS

Article #44

Telephone contacts should be made during reasonable hours as specified by federal and state laws and regulations.

Comment:

- The Telephone Consumer Protection Act and the Telemarketing Sales Rule set the allowable calling hours from 8:00 am - 9:00 pm (the consumer's time). Days of the week are not restricted, but some consumers probably do not consider it to be reasonable to be called on a weekend. In fact, DMA's Teleservices Ethics Committee recommends that calls on the weekends should be limited as follows: Saturdays from 10:00 am - 9:00 pm and Sundays from 12:00 pm - 6:00 pm. (This is somewhat consistent with retail store hours.)

Questions to Ask:

- Are your telephone calling systems set to compensate for various time zones and daylight savings/standard times so consumers are not called outside the appropriate and recommended times?
- Are your service reps trained as to what the applicable rules and regulations are and how to comply with them?

TAPING OF CONVERSATIONS

Article #45

Taping of telephone conversations by telemarketers should only be conducted with notice to or consent of all parties, or the use of a beeping device, as required by applicable federal and state laws and regulations.

Comment:

- This article means, for example, that your customer service representatives or a recorded message should inform consumers that their call may be taped. You could say, where appropriate, "The following call may be taped for quality assurance purposes, or to verify purchase authorization."
- Monitoring employees through taping or listening in to a sample of calls is a positive action to take to help train employees, make sure your customers are well-served and applicable federal and state regulations are followed.
- Employees need to be informed in advance of why and how you monitor their calls in the workplace and the results of any monitoring.
- Refer to *Article #12 - Advance Consent Marketing* - for regulatory requirements to audio record telephone sales of advance consent marketing plans.

Questions to Ask:

- Are your customer service reps trained to comply with the applicable laws?
- Are procedures in place to give proper notice to consumers if taping will occur?
- Do you follow up with your employees about the results of monitoring?

RESTRICTED CONTACTS

Article #46

A marketer should not knowingly call or send a voice solicitation message to a consumer who has an unlisted or unpublished telephone number except in instances where the number was provided by the consumer to that marketer for that purpose. A marketer should not call consumers who are on the marketer's in-house Do-Not-Call list. A marketer should not knowingly place a call or send a voice or text message to a wireless telephone number for which the called party must pay the charge, in either business-to-consumer or business-to business marketing, except in instances where the number was provided by the consumer or business to that marketer for that purpose. A marketer should also use DMA's Wireless Suppression Service or another comprehensive wireless suppression service prior to calling or sending text solicitation messages.

***A marketer should use DMA's Telephone Preference Service as required in Article #31 and must use the federal Do-Not-Call registry and state Do-Not-Call lists when applicable prior to using any outbound calling list. Individuals with whom the marketer has an established business relationship do not need to be suppressed even if they are on the national registry. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services within the last 3 months. (Note: State laws may vary. DMA's Web site at: www.the-dma.org/government/donotcalllists attempts to provide current information on state Do-Not-Call lists.) Consumers who have given written permission to the marketer do not need to be suppressed by any Do-Not-Call list. Individuals can add or remove themselves from company-specific Do-Not-Call lists either orally or in writing.**

Marketers should not use randomly or sequentially generated numbers in sales or marketing solicitations.

Comment:

- The privacy of consumers with unlisted or unpublished numbers must be honored, especially since many consumers may have gotten unlisted numbers because they wanted to reduce the volume of unsolicited calls they were receiving.
- This revised guideline acknowledges new technologies, such as wireless telephone services and the fact that voice and text messages can be made to wireless numbers. Most recipients pay to receive calls to their wireless devices and would not welcome unsolicited marketing calls or messages, which is why such contacts should only be made when recipients have provided their numbers to the marketer for that purpose. Along with the new technology have come wireless suppression services, which should be used as an extra check against calling wireless numbers.

- *Using DMA's Telephone Preference Service (TPS) has long been a requirement when prospecting. It is still important to use it (and should be used through November 2011, as noted earlier), along with federal and state government Do-Not-Call registries, because TPS includes charitable organizations and other numbers that do not have to be suppressed by law.
- Although the guidelines are generally oriented toward consumer marketing, this article also states that businesses should not send other businesses unwanted voice or text messages.
- Calling numbers randomly or sequentially runs the risk that consumers who have asked marketers not to call them will be contacted.

Questions to Ask:

- Have steps been taken to remove unlisted, unpublished and wireless numbers from your calling lists, once those numbers have been identified?
- Are you careful not to exchange or transfer unlisted, unpublished or wireless numbers to others?
- Do you use the federal Do-Not-Call registry, any relevant state registry and *TPS before prospecting?
- If applicable, do you use DMA's Wireless Suppression Service or another such service?
- Do you maintain an in-house suppress service for consumers who request that your company not call them again?
- Do you train your reps to recognize in-house suppression requests and process them?

CALLER-ID/AUTOMATIC NUMBER IDENTIFICATION REQUIREMENTS

Article #47
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.

Comment:

- Many consumers who have Caller ID have expressed frustration to DMA and to regulators about non-identification of callers' names and numbers. It is fair to let consumers know who is calling (as long as it is technically feasible) and to provide a number where consumers can get information or service from your company.
- Blocking Caller ID purposefully or transmitting a false name are not fair practices.

- If you use ANI and plan to use the data received as a result, you need to first get consumer consent unless there is a prior business relationship (for related goods or services). Consent could be obtained, for instance, by asking consumers when they call your toll-free number to respond to your ad, if it would be okay to notify them of new product information. Or, you could provide a notice in the informational package you send, providing a toll-free number for them to call if they want to receive future updates.

Questions to Ask:

- Does your company make its name and number available on Caller ID (as per the FCC regulation requiring transmission of Caller ID, if feasible, which was effective as of January 29, 2004)?
- Do you have systems and procedures in place for notifying consumers about data collection and transfer and getting their permission if information collected via ANI is to be used later?
- Do you take care not to market to individuals who have not given their consent in this context?

USE OF AUTOMATED DIALING EQUIPMENT

Article #48
Marketers using automated dialing equipment should allow 15 seconds or 4 rings before disconnecting an unanswered call.

Marketers should connect calls to live representatives within 2 seconds of the consumer's completed greeting. If the connection does not occur within the 2-second period, then the call is considered abandoned whether or not the call is eventually connected.

For any abandoned calls, the marketer should play a prerecorded message that includes the seller's name, telephone number, states the purpose of the call, and provides a telephone number at which the consumer can request not to receive future marketing calls.

Repeated abandoned or "hang up" calls to consumers' residential telephone numbers should be minimized. In no case should calls be abandoned more than:

- **3% of answered calls within a 30-day period (unless a more restrictive state law applies), or**
- **twice to the same telephone number within a 48-hour time period.**

Marketers should only use automated dialing equipment that allows the telephone to immediately release the line when the called party terminates the connection.

When using any automated dialing equipment to reach a multi-line location, whether for business-to-consumer or business-to-business marketing, the equipment should release each line used before connecting to another.

Companies that manufacture and/or sell automated dialing equipment should design the software with the goal of minimizing abandoned calls to consumers. The software should be delivered to the user set as close to 0% as possible. Manufacturers should distribute these Guidelines for Automated Dialing Equipment to purchasers of dialing equipment and recommend that they be followed.

The dialers' software should be capable of generating a report that permits the user of the equipment to substantiate compliance with the guideline.

Glossary of Terms Used

Automated Dialing Equipment **- any system or device that initiates outgoing call attempts from a predetermined list of phone numbers, based on a computerized pacing algorithm.**

Abandoned Call **- a call placed by automated dialing equipment to a consumer which when answered by the consumer, (1) breaks the connection because no live agent is available to speak to the consumer, or (2) no live agent is available to speak to the consumer within 2 seconds of the consumer's completed greeting.**

Abandonment Rate **- the number of abandoned calls over a 30-day period divided by the total number of calls that are answered by a live consumer. Calls that are not answered by a live consumer do not count in the calculation of the abandonment rate.**

Report **– reportable information that should be made available which contains key points, including the percentage of abandoned calls.**

Comment:

- In the past, computerized calls caused consumers problems, such as recorded messages taking up all the space on a consumer's answering machine, tying up hospital and other emergency lines, or annoying people who would answer the phone to hear a strange-sounding computer "voice." You need to ensure that your automated equipment immediately releases the line when the called party ends the connection so that it does not tie up consumers' or businesses' lines.
- This revised guideline incorporates *Use of Predictive Auto Dialing Equipment* from the previous *Guidelines for Ethical Business Practice*, and revises certain essential points in keeping with revised federal regulations, including that the maximum rate for abandoned calls is 3% of answered calls within a 30-day period.
- It is important that your goal be to have as close to 0% abandonment rate as you can so that as few consumers as possible are bothered by the occurrence of answering their phones to find "dead air."

- The abandonment rate does not include reaching busy signals or answering machines; it is based on live consumers answering the phone expecting someone to be on the other end, and there is not someone there.
- Note the requirement to have a pre-recorded message in cases where your dialer abandons calls. This is to allay fears of consumers and let them know who called and to give them an opportunity to opt out, should they wish to.

Questions to Ask:

- Do you have adequate measurement systems and procedures in place to monitor the responsible use of predictive dialing software and equipment?
- Has your predictive dialing equipment been set so that this guideline can be adhered to in terms of the percentage of abandoned calls and other requirements?
- Has your staff been trained to operate the equipment so that as low an abandonment rate as possible is their goal, and so that the other requirements are also met?
- If your company manufactures and/or sells predictive dialing equipment, have you assured yourself that the equipment is always set as close to a 0% abandonment rate as possible before delivery to the buyer?
- If you sell this equipment, do you have a regular procedure in place for distributing these guidelines and for encouraging their use?

USE OF PRERECORDED VOICE MESSAGING

Article #49

Marketers who use prerecorded voice messaging should not automatically terminate calls or provide misleading or inaccurate information when a live consumer answers the telephone.

Prerecorded solicitations should include the name and telephone number of the seller, service bureau or customer service department where the consumer can call back during normal business hours to request not to receive future calls, ask questions or get service.

Comment:

- It is no longer a DMA requirement to have a live representative introduce a prerecorded message, as this practice is no longer easier for the consumer or the marketer.
- Purposefully hanging up on consumers in order to deliver a message to their answering machines, or saying "sorry, wrong number," practices examined by DMA's ethics committees, would violate this guideline. Also, contacting telephone numbers that were once disengaged to see if the line is now "live," and then hanging up, would be a violation.
- If your company leaves prerecorded messages, it is essential to leave your company name and a number for the consumer to call back. In addition, you should consider that consumers would most likely find it annoying to have lengthy prerecorded solicitations taking up message space on their answering machines, and keep messages targeted and brief.

Questions to Ask:

- If your company uses pre-recorded solicitations, is your prospecting targeted and are your messages meaningful and brief?

- Does any message always give your company's name and number where your company can be reached?
- What happens when a live consumer answers the telephone instead of an answering machine?
- Do you honor name-removal requests received as a result of pre-recorded messages to consumers?

USE OF TELEPHONE FACSIMILE MACHINES

Article #50

Unless there is an established business relationship with the recipient, or unless the recipient has given prior permission, advertisements, whether sent to a consumer or a business, should not be transmitted to a facsimile machine, including computer fax machines. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services/causes within the last 3 months.

Each permitted transmission to a fax machine must clearly contain on the first page, the date and time the transmission is sent, the identity of the sender which is registered as a business with a state and the telephone number of the sender or the sending machine.

Comment:

- Sending out fax broadcasts to prospects as a way to get new business is against this guideline article, and is also illegal. Detailed information on a new fax act and the revised rules of the Federal Communications Commission (FCC), including the allowance for an established business relationship, can be found at www.dmaresponsibility.org/FaxAlert. Of particular note are that (a) the Junk Fax Prevention Act of 2005 requires you to include an opt-out notice on the first page of each commercial fax you send and (b) the FCC has delayed indefinitely enactment of the requirement that you must get written permission to send commercial faxes, even to your own customers.
- The FCC passed its fax rules in 1991 to allow fax recipients, both businesses and consumers, to control the amount of paper used and the amount of time their machines were tied up receiving unsolicited faxes. The FCC's revised Telephone Consumer Protection Act (TCPA) applies whether you are transmiting a fax *from* a computer or *to* a computer (or e-fax service).
- The *Guidelines for Ethical Business Practice* are meant to promote ethical practices that affect consumers; however, this article (in keeping with the federal regulation) is applicable to business-to-business solicitations as well.
- Although listings of fax numbers may be readily available, you should not use them to market to consumers' and businesses' fax numbers, unless you are certain that those fax numbers were voluntarily placed on the list by the ultimate fax recipients. Otherwise such prospecting is illegal.
- Keep in mind that an opt-out notice must appear on the first page of each commercial fax you send. The telephone and fax numbers listed in the opt-out notice must be domestic numbers, and the recipient must be able to make an opt-out request at any time and any day of the week.

- In addition to providing a fax number and a toll-free telephone number for recipients to opt out of receiving future faxes, also consider providing an e-mail address and/or Web site address that recipients can use to make opt-out requests.
- Make sure the fax and toll-free telephone opt-out lines are properly staffed and/or set up so that all opt-out requests are captured. This means, for instance, making sure your lines are not busy when recipients call to opt out and that you have enough voicemail capacity to handle all calls.
- Keep in mind that the person or entity on whose behalf the fax is sent must be identified on the fax. If the service bureau has "a high degree of involvement" in preparing and sending your company's faxes (such as providing the phone numbers or designing the content), then the broadcaster must also include its name as registered with a state corporation's commission.

Questions to Ask:

- Do you have a business relationship with the intended recipient of your fax? If not, have you obtained express, prior consent from the intended recipient of your fax to fax him/her?
- Are you including a clear and conspicuous opt-out notice on the first page of all faxes you transmit?
- Does the opt-out notice clearly state that the intended recipient of the fax may opt out of any future faxes, provide clear instructions for doing so, and include a domestic telephone and fax number for the recipient to transmit an opt-out request free of charge?
- Is your company knowledgeable about the new federal fax regulations, and any state regulations (such as those that do not permit you to send faxes even to your own customers without prior express permission), that may be applicable to you?
- Do you have procedures in place to honor Do-Not-Fax requests, and do you maintain an internal Do-Not-Fax suppression list?

PROMOTIONS FOR RESPONSE BY TOLL-FREE AND PAY-PER-CALL NUMBERS

Article #51

Promotions for response by 800 or other toll-free numbers should be used only when there is no charge to the consumer for the call itself and when there is no transfer from a toll-free number to a pay call.

Promotions for response by using 900 numbers or any other type of pay-per-call programs should clearly and conspicuously disclose all charges for the call. A preamble at the beginning of the 900 or other pay-per-call program should include the nature of the service or program, charge per minute and the total estimated charge for the call, as well as the name, address and telephone number of the sponsor. The caller should be given the option to disconnect the call at any time during the preamble without incurring any charge. The 900 number or other pay-per-call should only use equipment that ceases accumulating time and charges immediately upon disconnection by the caller.

Comment:

- This article reflects federal law and regulations on how you have to operate if you use pay-per-call promotions. Regulations were put into place several years ago to stop problem situations, for example, consumers running up huge bills for calls they thought were free (800 number calls rolling into pay calls), or being misled about how much the calls would cost.
- The sponsor, address and telephone number also need to be disclosed because of problems with seemingly free calls that were actually international.

Questions to Ask:

- If you operate a pay-per-call number, have you made disclosure of the total price - or price per minute - easy for consumers to find, read and understand?
- Are all costs and other necessary information disclosed in the preamble part of the message?
- Can the caller hang up during the preamble and not be charged for the call?

DISCLOSURE AND TACTICS

Article #52

Prior to asking consumers for payment authorization, telephone marketers should disclose the cost of the merchandise or service and all terms and conditions, including payment plans, whether or not there is a no refund or a no cancellation policy in place, limitations, and the amount or existence of any extra changes such as shipping and handling and insurance. At no time should high pressure tactics be utilized.

Comment:

- Telling consumers they have to make an immediate decision to buy is one example of "high pressure." Consumers need to understand an offer and have the opportunity to check it out to their satisfaction before making a financial commitment.
- Although these guidelines generally apply to consumers, it is recommended that you honor them when marketing to businesses also. DMA, for instance, has received complaints from business people citing high pressure tactics from investment sellers who used misleading tactics to reach them.
- Some states have enacted "no rebuttal" provisions for telemarketers. It is essential to be aware of and follow such restrictions.
- See also *Article #12 - Advance Consent Marketing* - concerning disclosures to be made during telephone solicitations.

Questions to Ask:

- Are your telephone reps trained to disclose all important information to consumers before they ask for payment?
- Are your telephone reps trained to know when not to pursue the call at hand, and to courteously end the call?

Fundraising

This section, which contains only one article, is in regard to nonprofit organizations, a significant sector of the Association's membership. This article is in addition to the other applicable guidelines and the Commitment to Consumer Choice.

Article #53

In addition to compliance with these guidelines, fundraisers and other charitable solicitors should, whenever requested by donors or potential donors, provide financial information regarding use of funds.

Comment:

- Consumers want to feel assured that their charitable contributions will be used wisely and as represented, so you should freely give them the needed financial information that will help with their decision to give.
- Other specific questions concerning nonprofits can be addressed to DMA's subsidiary, the Nonprofit Federation, at nonprofitfederation@the-dma.org.

Questions to Ask:

- Do you have a prepared financial information sheet ready to be sent to inquirers?
- Do you cooperate with the Better Business Bureaus Wise Giving Alliance and other such organizations, in terms of providing information to them when they request, so that a publicly available report on your organization can be prepared?

Laws, Codes, and Regulations

This last section of the guidelines also contains only one article. Obviously, marketers should be in compliance with all applicable laws, codes and regulations. This guide has referenced many federal laws and rules that are essential for marketers to know about and follow. It should be noted that all federal laws referenced are U.S. laws, relevant only to the U.S. marketplace. It is strongly recommended that legal counsel be consulted to ensure your promotions respect federal and state limitations. And, if you market

internationally, you need to make sure you are in compliance with relevant laws of those countries. Finally, it is hoped that adherence to these self-regulatory principles will go a long way toward lessening the possibility of even more regulations in the future.

Article #54
Direct marketers should operate in accordance with laws and regulations of the United States Postal Service, the Federal Trade Commission, the Federal Communications Commission, the Federal Reserve Board, and other applicable federal, state and local laws governing advertising, marketing practices and the transaction of business.

Comment:

- Throughout these examples, several laws and regulations have been referenced, such as the *Mail or Telephone Order Merchandise Rule*, the *Telephone Consumer Protection Act,* the *Telemarketing Sales Rule,* the *Children's Online Privacy Protection Act and CAN-SPAM.*
- There are others as well, such as the *Textile and Wool Acts*, which requires your catalog to clearly disclose for any wool or textile product that the article is made in the USA, imported or both. (It is not enough to state generally that "all products are either made in America or imported.")
- Online marketing is subject to many of the same rules as other ways of marketing direct. Many consumers are still waiting and debating the benefits of transacting business in this relatively new medium; as their trust and confidence builds, the market will continue to grow.
- Laws and rules must, of course, be followed for consumer protection and to avoid legal actions being taken against your company, but ethics guidelines often go even further and should be the higher standard to reach for when striving *to do the right thing.*
- Refer to: www.dmaresponsibility.org for a listing of various guides and fact sheets developed to explain important regulations.

Questions to Ask:

- Do your company's promotions, policies and practices receive regular review by legal counsel to ensure that all legal requirements are followed?
- Do you maintain resource information on essential regulations?
- Do you have systems and procedures for making sure your information is up-to-date?
- Do you regularly train staff regarding advertising and marketing regulations they need to be familiar with?
- Do your online sites post relevant consumer protection information, both your own customer service policies and compliance with federal regulations; and do you provide links or references to other sites with consumer protection information?

OTHER DMA RESOURCES

For more complete information on resources, see www.dmaresponsibility.org.

- *Commitment to Consumer Choice* Member Compliance Guide and other CCC materials (www.DMACCC.org)
- DMA Preference Services Subscriber Information
- DMA's consumer website: www.DMAchoice.org
- Privacy Policy Generators
- Environmental Resources and Generator (The "Green 15")
- E-Commerce Integrity Resource Center
- Reports on Ethics Committee Findings
- Information Security: Safeguarding Personal Data in Your Care

DMA can also provide your organization with information on many federal laws and regulations affecting direct marketers, including:

- Mail or Telephone Order Merchandise Rule
- Telemarketing Sales Rule
- Telephone Consumer Protection Act
- Children's Online Privacy Protection Rule
- Do's and Don'ts - Sweepstakes for Marketers

The U.S. Postal Service's *Fighting Mail Order Fraud and Theft; Best Practices for the Mail Order Industry Reference Guide* is also available, as well as a variety of consumer education brochures. Contact the Department of Corporate & Social Responsibility in Washington, D.C. at ethics@the-dma.org for more information.

DMA'S DEPARTMENT OF CORPORATE & SOCIAL RESPONSIBILITY

In its continuing efforts to improve the practices of direct marketing and the marketer's relationship with customers, DMA sponsors several activities in its Department of Corporate & Social Responsibility.

- Ethical guidelines are maintained, updated periodically, and distributed to the direct marketing community.
- The Committee on Ethical Business Practice investigates and examines promotions and practices made throughout the direct marketing community that are brought to its attention.
- The Ethics Policy Committee revises the guidelines as needed, and initiates programs and projects directed toward improved ethical awareness in the direct marketing area.
- The Committee on the Environment and Social Responsibility is dedicated to environmental issues, and educating consumers about the "electronic highway."
- The *Commitment to Consumer Choice* (www.DMACCC.org) reflects DMA's continued emphasis on empowering consumers and strengthening their trust with the direct marketing community.
- "Dialogue" meetings between direct marketing professionals and consumer affairs and regulatory representatives facilitate increased communication between direct marketers and their customers.
- DMAchoice offers consumers assistance in managing their marketing preferences, and provides consumer education on a number of topics.

For additional information, contact DMA's Washington D.C. office.

Direct Marketing Association
1615 L Street, NW; Suite 1100
Washington, D.C. 20036-5624
Phone: 202-955-5030
Fax: 202-995-0085
www.dmaresponsibility.org
e-mail: ethics@the-dma.org

DMA
Direct Marketing Association
Department of Corporate Responsibility
1615 L St. NW, Suite 1100
Washington, D.C. 20036

EXHIBIT 4

Related Content:
Press Releases
DMA Press Room

DIRECT MARKETING ASSOCIATION ISSUES GUIDANCE FOR ESTABLISHING AND SUBSTANTIATING SHIPPING AND HANDLING CHARGES

SAN FRANCISCO, June 2, 2003 -- The Direct Marketing Association (The DMA) today issued guidance to assist catalogers and other direct marketers in establishing charges for shipping, handling, and other fulfillment costs.

The Guidance for Establishing and Substantiating Shipping and Handling Charges was released today at the 20th Annual Catalog Conference & Exhibition in San Francisco.

"In a marketplace of sophisticated consumers and close scrutiny by regulators, direct marketers must be very careful. Positive consumer perception of all charges, especially shipping and handling, is critical to the continued success and growth of the industry," said H. Robert Wientzen, president & CEO, The DMA.

"In short, shipping and handling costs should be fair, reasonable, clear, and justifiable," said Wientzen.

The guidance provides additional direction beyond article #11 of The DMA's Guidelines for Ethical Business Practice, which states: "Postage, shipping, or handling charges, if any, should bear a reasonable relationship to actual costs incurred."

The guidance recommends that companies do the following when establishing and substantiating shipping and handling charges:

- Companies should determine what costs will be covered, and substantiate their method so they can easily respond to consumers, regulators, or others who might inquire about charges. Ideally, a fulfillment cost study should be done with the assistance of an impartial outside expert. While most consumers understand paying for direct costs such as common carrier or delivery charges, semi-direct costs such as warehousing and returns processing or indirect costs such as item replacement costs are much more difficult to substantiate and should be clearly documented.

- more -

DMA ISSUES GUIDANCE ON SHIPPING AND HANDLING CHARGES/2

- Exact charges should be disclosed clearly and conspicuously in advance of the order. In catalogs and direct mail, charges should be prominently displayed and readily visible. When ordering online, shoppers should receive shipping information early in the order path.
- In continuity programs, in which shipping costs may differ from month-to-month depending on the order, marketers should provide an estimated range of costs before consumers sign up. When each order is shipped, the exact shipping and handling charge should be clearly stated.
- If a company eliminates a separate shipping and handling charge and concurrently builds the cost into the price of the product, the offer should include a term such as "shipping included" rather than "free" shipping.
- When a company offers free products and the consumer pays only for shipping and handling, the offer should disclose very clearly and close to the word "free" the costs of shipping, the entire plan for which the consumer is obligated and the total cost that consumers will pay.

To assist companies in understanding the new guidance and to address other issues regarding shipping and handling charges, The DMA will sponsor a seminar via conference call on Thursday, July 17, 2003 from 2 to 4 p.m. ET. The seminar will be conducted by George Isaacson of Brann & Isaacson, who consulted with The DMA in developing this new guidance. The cost for the seminar is $99 for DMA members and $150 for non-members. To register for the call-in seminar, e-mail The DMA's Ethics and Consumer Affairs Department at ethics@the-dma.org.

The complete text of the Guidance for Establishing and Substantiating Shipping and Handling Charges is available on The DMA Web site at www.the-dma.org.

The DMA is the leading trade association for businesses interested in interactive and database marketing, with nearly 4,700 member companies from the United States and 53 other nations. Founded in 1917, its members include direct marketers from every business segment as well as the nonprofit and electronic marketing sectors. Included are catalogers, Internet retailers and service providers, financial services providers, book and magazine publishers, book and music clubs, retail stores, industrial manufacturers, and a host of other vertical segments, including the service industries that support them. According to a DMA-commissioned study, direct and interactive marketing sales in the United States surpassed $2 trillion in 2002, including $126 billion in catalog sales and $34 billion in sales generated by the Internet. The DMA's Web site is www.the-dma.org, and its consumer Web site is www.shopthenet.org.

RSS Subscription

EXHIBIT 5

DMA Guidance for Establishing and Substantiating Shipping and Handling Charges

Most direct marketers charge consumers for delivery of products. What the actual charges are and how these charges are calculated are significant issues for consumers.

Setting shipping and handling costs is not as easy as it might, at first, seem. In a marketplace of sophisticated consumers and close scrutiny by regulators, direct marketers must be very careful. Positive consumer perception of your charges is critical to your success. Regulators are concerned about what they might view as unclear or unfair charges.

It's Important To Substantiate Your Charges

That way, if you receive an inquiry about the fairness of your shipping and handling charges, you will be able to respond easily and well, having done in advance the careful analysis that must go into such charges.

This fact sheet is intended to help you develop a sound approach to calculating and substantiating shipping and handling charges.

Although not required, you may consider doing a fulfillment cost study that can help you determine what your actual costs are so that you can charge consumers reasonably. Further, should your method of charging be questioned, you have the evidence to prove that you took all reasonable steps to set charges appropriately.

You should consider consulting your accounting department or internal audit department to help identify the costs involved in shipping and handling.

Unless you are confident that you have sufficient in-house expertise to do the job, it can be useful to have an impartial outside expert do this study. Any study done should clearly report details as to the information reviewed and the conclusions reached.

It's important to substantiate your method of charging for whoever may have a question about it. A fulfillment consultant or industry analyst would be an appropriate person. But whether an in-house or external person, the task is the same: to make fair, credible, objective and defensible decisions.

Some marketers take the position that so long as there is clear disclosure on how much the consumer pays in total for the shipped product, the amount the marketer charges for shipping and handling should not matter. There appears to be a trend by law enforcement agencies,

however, to insist that a consumer who is charged shipping and handling costs should be paying a fee reasonably based on the marketer's cost. The latter position is consistent with existing DMA guidelines.

Review Your Costs

When there is any significant change in your incurred costs or in your method of determining shipping and handling charges, it's time to review your costs.

Costs Included in Your Shipping and Handling Charges

This decision is, at the same time, a matter of consumer perception, a marketing issue and a legal issue.

The charges should be clearly understandable and fair to the consumer. From a consumer perspective, high shipping and handling charges can be a deterrent to customer purchases and customer satisfaction.

From the marketing perspective shipping and handling charges are a factor in your competitive stance and in your brand reputation.

Previous legal and regulatory actions have claimed that some marketers have been deceptive about setting their shipping and handling charges and should cause all direct marketing executives to take care in determining which costs to include and in substantiating shipping and handling charges.

Each consumer should be charged fairly. Your goal should be not to charge consumers as a whole more than you pay in total. No single or "correct" formula exists for calculating or charging shipping and handling. For simplicity, some marketers create an easy-for-the-consumer-to-understand method of charging based on price or weight or distance of delivery.

Some consumers think the price of shipping and handling should be limited to your actual common carrier cost. Of course, much more is involved and you must be prepared to explain the justification for the individual cost to an individual consumer inquiring about the fairness of his or her individual charge.

There are clearly risks associated with including certain categories of expense in your shipping and handling charge. Below we've identified some costs that some marketers have included. There may be others. In general, the more indirect your charge, the less consumers are likely to understand why you are charging them for it.

Direct Costs	• Common Carrier Costs • Land Delivery Costs • Express Delivery Costs

	• Extra Heavy Package Costs • Packaging Materials • Direct Labor Costs • Other Special Handling
Semi-Direct Costs	• Warehousing • Insurance for Assured Delivery, Loss, Damage • Rent • Returns Processing • Inbound Call Center Costs for Processing Returns • Depreciation of Distribution Center Equipment • Distribution Center Rent • Cost for Outsourcing Fulfillment • Overhead Costs, Conservatively Allocated
Indirect Costs	• General & Administrative Expenses • Inventory Carrying Costs • Item Replacement Costs • Aggressive Fixed Overhead Allocation

Disclosing Costs To Consumers

Shipping and handling costs should be disclosed clearly and conspicuously and in advance of the consumer's completing an order. Consumers should receive notice of the exact charge before the sale is finalized.

Providing consumers general information on how shipping and handling charges are computed can be easily done by your customer service staff or by reference to your Web site. For online shopping, consumers should get information on the actual cost early in the order path, so that they do not go through several purchase screens only to abandon their carts when they learn the cost at the end.

For catalogs and other direct mail channels, shipping and handling charges should be prominently displayed and readily visible to consumers. On the telephone, consumers should be told the applicable shipping and handling charge when the total cost of the order is given. Where shipping and handling charges may vary depending on the amount of the order, an easy method for consumers to determine their exact charges should be provided.

Special Disclosure Issues

Continuity, Negative Option Or Subscription Programs
In continuity or negative option marketing plans, an individual consumer's order may differ from month-to-month, causing a variation in shipping costs. In this instance it may be best to disclose an estimated range of shipping costs before they sign up, so that your customers are not unpleasantly caught by surprise. Of course, when the order is shipped, the exact shipping and handling charge should be clearly stated.

Free Products
In instances where you offer free products--where the consumer pays only for shipping and handling--it is critical that you disclose very clearly and close to the word "free" the costs of shipping, the entire plan for which the consumer is obligated and the total costs that consumers will pay. Consumers object strongly if they perceive that the cost of shipping and handling for an otherwise free product is too high.

Free Shipping And Handling
Nothing in this document should dissuade you from offering your customers free shipping and handling, or a decreased cost of shipping and handling when a consumer buys a larger order.

It is not appropriate, however, to eliminate your delivery charge and concurrently increase retail prices and still call it "free delivery." If you have in fact increased the price of the product to cover your shipping and handling charges then a term such as "shipping included" should be used instead of the word "free."

In Summary…

Shipping and handling costs should be fair, reasonable, clear and justifiable.

Additional Resources:

Federal Trade Commission, in conjunction with DMA, has additional information and helpful FAQs on how businesses can comply with the Mail and Telephone Order Rule: http://www.business.ftc.gov/documents/bus02-business-guide-mail-and-telephone-order-merchandise-rule.

This fact sheet was developed in consultation with attorney George Isaacson of Brann & Isaacson.

ClassAction.org