Direct marketing Q&A: US

by Alan Friel, Baker & Hostetler

Country Q&A | Law stated as at 30-Nov-2017 | United States

The regulation of unsolicited commercial communications

In the United States, federal and state laws limit and regulate the way in which companies communicate with individuals and other businesses for marketing, advertising, fundraising, and other related purposes. These laws affect the manner in which companies can call, text, mail, e-mail, or fax consumers.

Two of the most important federal laws governing this field are the:

- Telemarketing and Consumer Fraud and Abuse Act (Telemarketing Act), and the Telemarketing Sales Rule (TSR) regulations issued under it by the Federal Trade Commission (FTC).
- Telephone Consumer Protection Act (TCPA), enacted by Congress and regulated by the Federal Communications Commission (FCC).

Both laws apply to telemarketing calls, but the TCPA also contains provisions that apply to other types of calls, text messages, and fax advertisements. These rules often overlap, but they also contain key differences in scope including who can enforce them.

In addition, direct marketing by e-mail and direct mail is regulated in the United States most notably by the federal CAN-SPAM Act, which largely pre-empts state laws and covers e-mail, and the federal Deceptive Mail Prevention and Enforcement Act (DMPEA), which governs physical mail. US privacy and data security laws, and laws regulating false advertising, and promotions such as sweepstakes and contests, are also relevant to direct marketing. These laws are at both the federal and state level, often with great differences in the laws from state to state. Further, the marketing and promotion of various products and services (for example, foods and drugs, petroleum, automotive, financial services, age-restricted products and so on) have special requirements and restrictions that are beyond the scope of this note.

This Country Q&A is merely an overview. For a more detailed analysis, see Promotion & Marketing Law Book (Brand Activation Association, 8th ed. 2015) available at *www.baalink.org/dierson/show*.

Below is a list of important and commonly used terms referred to within this practice note, together with their abbreviations:

- Advertising Self-Regulatory Council of the Council of Better Business Bureaus: ASRC.
- Automatic Telephone Dialling System: ATDS.
- Children's Online Privacy Protection Act: COPPA.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act: CAN-SPAM.
- Act Deceptive Mail Prevention and Enforcement Act: DMPEA.
- Department of Justice: DOJ.

- Digital Advertising Alliance: DAA.
- Direct Marketing Association: DMA.
- Do Not Call: DNC.
- The Fair and Accurate Credit Transactions Act: FACTA.
- FCC-Issued 2012 TCPA Order (effective 2013): the 2013 FCC Amendment.
- FCC Omnibus TCPA Declaratory Ruling and Order: the 2015 FCC Order.
- Federal Trade Commission: FTC.
- Federal Trade Commission Act: FTC Act.
- Junk Fax Prevention Act: JFPA.
- Telemarketing Consumer Fraud and Abuse Prevention Act:Telemarketing Act.
- Telemarketing Sales Rule: TSR.
- Telephone Consumer Protection Act: TCPA.
- State “unfair or deceptive acts or practices” statutes: UDAPs.
- The Undertaking Spam, Spyware, and Fraud with Enforcers Beyond Borders Act: US SAFE WEB Act.
- Uniform Deceptive Trade Practices Act: UDTPA.
- Unfair Trade Practices and Consumer Protection Law: UTPCPL.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act: USA PATRIOT Act.

This note is intended for top-level issue spotting only and it is not intended as legal advice. Given the complexity of the issues, and how quickly the law is evolving in the US, consultation with local counsel is recommended.

1. How does national law regulate the making of unsolicited telephone calls for marketing purposes?

FTC Regulation of telemarketing
Telemarketing Consumer Fraud and Abuse Prevention Act (Telemarketing Act)

The Act:

- Prohibits specific deceptive and abusive telemarketing acts or practices.
- Requires disclosure of certain material information.
- Requires express verifiable authorisation for certain payment mechanisms.
- Sets record-keeping requirements.
- Specifies exempt transactions.

(see *15 USC. § 6101 et. Seq.*)

The Telemarketing Act establishes a private right of action in the federal courts.

Telemarketing Sales Rule (TSR)

The TSR was adopted by the FTC in 1995, and amended in 2003, 2008, 2010 and 2015 (see *16 C.F.R. Part 310*). As implemented, it applies to plans carried out to induce the purchase of goods or services, by the use of one or more telephones, and which involve more than one interstate telephone call (*16 C.F.R. §310.2(dd)*).

Under the TSR, telemarketing is defined as "a plan, program, or campaign which is conducted to include the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call." (*16 C.F.R. §310.2(dd).*)

With some exceptions, all businesses or individuals that engage in telemarketing must comply with the TSR, as well as applicable state laws. However, not all telemarketing activities are covered by the TSR, for example:

- Most business-to-business calls, and calls placed directly by a non-profit organisation (but not a for-profit solicitor working for a charity), or political candidate or organisation. (The only state with a do not call restriction applicable to calls to businesses is Texas, and that is limited to the regulation of electric utilities providers (*Texas Utilities Code §39.1025*).)
- Entities not covered by the FTC jurisdiction, and which are covered solely by the TCPA (for example, banks).

Some calls are partially exempt from the TSR. For example, calls to existing customers where there is an "established business relationship" are exempt from the Do Not Call (DNC) Registry provisions, a list of phone numbers of consumers who have registered a desire not to receive telemarketing calls (see below).

"Established business relationship" means a relationship between a seller and a consumer based on either:

- The consumer's purchase, rental, or lease of the seller's goods or services or a financial transaction between the consumer and seller, within the 18 months immediately preceding the date of a telemarketing call.
- The consumer's inquiry or application regarding a product or service offered by the seller, within the three months immediately preceding the date of a telemarketing call.

  (*16 C.F.R. § 310.2(q).*)

The caller must prove a prior existing business relationship or express written consent from a consumer it calls whose number is on the DNC Registry. There is an exemption for isolated or accidental violations but a caller who fails to keep its do-not-call list will not benefit from it. Companies must pay the FTC a subscription fee to access the national DNC Registry. Unsolicited inbound calls from customers are also excluded, although upselling during the call will bring it back within the scope of the rule with regard to disclosures, payment provisions and so on.

Compliance is required both of "telemarketers", entities that initiate or receive telephone calls to or from consumers, and "sellers", the entities that provide or arrange to provide the goods and services being offered. The TSR (*16 C.F.R. §310.4*) requires these organisations to:

- Engage in no deceptive or abusive telemarketing acts or practices.

- Call only between 8:00 am and 9:00 pm (same as under the Federal Communications Commission (FCC) Rule under the TCPA).
- Screen and "scrub" names against the national DNC Registry.
- Honour do not call requests and maintain an entity-specific do not call list.
- For pre-recorded calls, include an automated interactive opt-out mechanism that is announced and made available for the call recipient to use at the outset of the message and promotions.
- Respect requests to call back at a later time.
- Display telemarketer or seller's caller ID information.
- Identify themselves and what they are soliciting.
- Accurately disclose all material information and terms and make no misrepresentations (material terms may include such items as cost, quantity, restrictions, limitations, conditions, and no-refund policies).
- Not "abandon" any outbound calls to consumers (an outbound telephone call is "abandoned" under the TSR if a person answers it and the telemarketer does not connect the call to a sales representative within two seconds of the person's completed greeting (*16 C.F.R. §310.4(b)(1)(iv)*)).
- Comply with special rules for prizes.
- Never engage in unauthorised billing.
- Set payment restrictions for the sale of certain goods and services.
- Retain certain records for at least 24 hours and keep specific other records for two years.
- Include a description of any goods or services purchased in a tape recording of a consumer's express, verified authorisation to be charged (consent to the recording needs to be obtained to comply with other laws).

The types of payment methods that can be used when selling products or services via telemarketing are restricted (for example, no bank account debiting, money transfer services or pre-paid card cash loading).

For more information see *Federal Trade Commission: Complying with the Telemarketing Sales Rule*.

It should be noted that although companies often outsource telemarking to vendors, the advertiser is still responsible. Care should be taken to select competent vendors and obtain meaningful indemnity for compliance errors.

Debt relief services

The FTC has also issued additional rules for sellers and telemarketers of debt relief services (the new rules came into force in autumn 2010).

Debt relief service providers are prohibited from collecting a fee for services until a debt has been settled, altered or reduced. The providers are also prohibited from making specific misrepresentations about material aspects of the services. Certain disclosures must also be made in relation to calls marketing debt relief services.

In addition, the TSR has been extended to cover inbound calls made to debt relief companies in response to general media advertisements (see *16 C.F.R. Part 310*).

DNC Registry

This popular programme (established by the TSR) empowers consumers to stop calls from all companies within the FTC's jurisdiction, except when the consumer has an established business relationship (see above), or otherwise consents in writing. Over 210 million consumers have registered their telephone numbers with the national registry. Under the Do-Not-Call Improvement Act of 2007, registrations on the list became permanent, with no need to renew. The national DNC Registry does not cover calls:

- From organisations with which the consumer has an established business relationship.
- For which the consumer has given prior written consent.
- Which are not commercial or do not include unsolicited advertisements.
- By or on behalf of tax-exempt non-profit organisations.

However, a company that is acting for profit is covered by the TSR if it solicits charitable contributions on behalf of a non-profit organisation, and it must comply with the disclosure and other requirements of the TSR, as amended by the USA Patriot Act (see below), except for national DNC Registry requirements. For more information see *Federal Trade Commission: Q&A for Telemarketers & Sellers About DNC Provisions in TSR*.

State legislation

At a state level, many states have enacted opt-out legislation for telephone marketing, requiring the creation of state-wide registries containing the telephone numbers of consumers in the state who do not wish to be contacted by telephone for marketing purposes. The national DNC Registry does not pre-empt state do-not-call laws. The FTC was instructed by Congress in 2013 to work with those states that have enacted state do-not-call registry laws, as well as with the FCC, to articulate requirements and procedures during a transition period leading to one harmonised do-not-call registry system and a single set of compliance obligations. However, this process is not complete:

- At least nine states continue to maintain separate do-not-call lists which must be checked in addition to the national DNC Registry to avoid violating those states' laws (*Colorado, C.R.S. 6-1-905; Connecticut, Conn. Gen. Stat. § 42-288a; Florida, Fla. Stat. § 501.059; Indiana, Burns Ind. Code Ann. § 24-4.7-4-1; Louisiana, La. R.S. 45:844.14; Massachusetts, ALM GL ch. 159C, § 2; Missouri, Mo. R.S. §407.1098.1; Montana, 30-14-1602, MCA; Oklahoma, 15 Okl. St. § 775B.4, Pennsylvania, 73 P.S. § 2245.2, 73 P.S. § 2242 (*list maintained by *Direct Marketing Association; Tennessee, Tenn. Code Ann. § 65-4-405 (*requires the state list to include the names on the national registry, but does not substitute the national registry for the state*); Wisconsin, Wis. Stat. § 100.52*. See, Ruane, *U.S. Congressional Research Service: Telemarketing Regulation: National and State Do Not Call Registries*).
- Indiana, Missouri, Louisiana, and Oklahoma in addition to prohibiting commercial phone calls, also explicitly prohibit commercial text messages sent to numbers on the state do not call list, and Rhode Island and North Dakota prohibit commercial texts to numbers on the national DNC Registry. (However, as explained below, federal law, and many state laws, require express written consent to send commercial texts messages so getting that consent would result also in consent to text to numbers on these DNC lists).
- Several states require registration to engage in telemarketing to their residents (see, for example, *Arizona, A.R.S. § 44-1272; California, Cal Pub Util Code § 2871; Kentucky, KRS § 367.46971; New Jersey, N.J. Stat. § 56:8-121* which have adopted the national DNC Registry, but still require state registration for telemarketers, and the following states do not require compliance with the national DNC Registry, or have their own DNC lists, but do require the registration of telemarketers and otherwise regulate their activities: *Delaware, 6 Del.*

C. § 2503A; Ohio, ORC Ann. 4719.02; Washington, Rev. Code Wash. (ARCW) § 19.158.050; West Virginia, W. Va. Code § 46A-6F-301).

For sanctions, see *Question 7*.

USA PATRIOT Act

The USA PATRIOT Act 2001, among other things, amends the Telemarketing Act to extend its scope to include telemarketing calls made by profit-making entities soliciting donations on behalf of charitable organisations (non-profit entities are beyond the FTC's jurisdiction, except for trade organisations that represent for-profit interests). The amended TSR modifies various provisions to effectuate expansion of the TSR's coverage to include charitable solicitations (under section 1011 of the USA PATRIOT Act), and adds new mandatory disclosures and prohibited misrepresentations in charitable solicitations.

FCC Regulation of telemarketing

The Telephone Consumer Protection Act 1991 (TCPA) was adopted to reduce the number of nuisance calls by sellers and to protect consumers' right to privacy. It overlaps in many respects with the Telemarketing Act, but has broader and deeper coverage (including coverage of fax and text "calls", see *Question 2* and *Question 5*). For more information and FCC resources, see *www.fcc.gov/encyclopedia/telemarketing* .

The FCC has adopted rules to implement the TCPA (FCC Rule). The FCC Rule requires that all artificial or pre-recorded telephone messages:

- State clearly the identity of the entity initiating the call at the beginning of the message.
- During or after the message, state clearly the telephone number of the entity to which any residential phone recipient may make a do-not-call request during regular business hours.

  (*47 C.F.R. §64.1200(b)(1),(2).*)

Further, the FCC Rule prohibits telemarketers from:

- Disconnecting unanswered calls before at least fifteen seconds or four rings.
- Abandoning more than 3% of calls that are answered.

Consent requirements under the TCPA

The TCPA requires differing levels of consent to call a phone number (call includes both voice calls and SMS text messages), depending on the nature of the call and the number called (see table below).

	Wireless		**Landline**	
	Non- telemarketing	**Telemarketing**	**Non-telemarketing**	**Telemarketing**
ATDS (voice)	Prior express consent	Prior express written consent	No consent required	No consent required

ATDS (text message)	Prior express consent	Prior express written consent	No consent required	No consent required
Pre-recorded message	Prior express consent	Prior express written consent	No consent required	Prior express written consent
Live operator (no ATDS)	No consent required	No consent required	No consent required	No consent required

The definition of an ATDS includes any equipment that could be modified to "dial randomly or sequentially," not just equipment that has the current capacity to do so (*FCC 2015 Omnibus Declaratory Ruling and Order* (2015 FCC Order)). The FCC has indicated it would, and that courts should, apply an ad hoc approach to determining what level of human intervention would be required to remove a piece of equipment from the "automatic" category. Therefore, companies can no longer assume they are not using an ATDS simply by using a human operator in the dialing process. Anything other than a rotary phone is arguably an ATDS.

Internet-to-phone messages are considered the functional equivalent of SMS text messages and the equipment used to send them is considered an ATDS (*2015 FTC Order*).

Consent expires after 18 months of inactivity. To obtain written consent from recipients, sellers must satisfy a checklist of requirements, including informing the consumer that:

- They are authorising the seller to engage in advertising or telemarketing.
- Consent is not required as a condition of purchase of any good or service.
- The calls will be made using automated technology.

Automated calls and texts must also have an opt-out mechanism to quickly end the call, and a way to take the consumer's phone number off the caller's call list (that is, an individual entity DNC list).

Callers must allow recipients to revoke their consent at any time "using any reasonable method including orally or in writing." (*2015 FCC Order*.) Therefore, a caller cannot designate an exclusive means by which a recipient can revoke consent, such as texting back "STOP". This complicates how companies manage opt-outs. For instance, if a consumer were to text back "no more", "quit" or another term the platform is not programmed to recognise, the consumer may be deemed to have opted-out. It is therefore important to address this issue when managing opt-outs, including through vendor platforms or services.

Callers must obtain the consent of the current subscriber and not the intended recipient of the call, but callers are permitted one call to the reassigned number to "gain actual or constructive knowledge of the reassignment and cease future calls to the new subscriber." (*2015 FCC Order*.) However, according to the FCC consent for a telemarketing call made to a landline telephone remains valid even when that call is ported to a wireless service. Carriers provide lists of reassigned numbers, and there are services that sell lists that aggregate the various carrier lists. These lists need to be used to constantly weed out reassigned numbers from marketing lists

Seller's liability for third-party telemarketers

A 2013 FCC Declaratory Ruling has further clarified that, under the TCPA, a seller may be held vicariously liable for breaches of 47 U.S.C. §§ 227(b) or 227(c) that are committed by third-party telemarketers, even if the seller does not initiate the calls. To determine liability, courts look to whether an agency relationship between the seller and the third-party telemarketer has been established, which is a fact-intensive determination.

Exemptions to the consent requirements under TCPA

Some non-telemarketing or informational calls made using an ATDS do not require prior consent from landline recipients (callers are required to obtain consent from wireless recipients). This includes calls:

- Made for emergency purposes.
- Not made for commercial purposes.
- Made for commercial purposes but not including or introducing an advertisement.
- Made by or on behalf of tax-exempt or non-profit organisations.
- Containing a “health care” message.

The 2015 FCC Order allows exemptions to the TCPA consent requirements for calls made by the banking industry or healthcare providers that are categorised as “pro-consumer”. Pro-consumer calls are those that are made for certain specified purposes such as calling customers to prevent fraud, to provide security breach notification, or to inform patients about appointments or prescriptions. However, these exempt calls still face restrictions, including that the call or text must:

- Be concise and free to the consumer.
- State the name and contact information of the caller.
- Include an opt-out mechanism.
- Be free of any telemarketing, advertising or debt collection content.

Calls by government and government contractors

The TCPA does not apply to auto-dialled, pre-recorded, or artificial-voice phone calls, including text messages calls, made by or on behalf of the federal government in the conduct of official government business (*FCC declaratory ruling of 8 June 2016*, the ruling was requested by three petitions: Broadnet, National Employment, and RTI). However, the TCPA continues to apply to non-governmental activities including political campaign events conducted by federal officeholders (*FCC 16-72*).

Text "send-to-friend" tools

Following the 2015 FCC Order, there has been litigation surrounding whether companies offering text "send-to-friend" or invitation tools are a sender and required to obtain written express consent under the TCPA before the user sends the text, or if the user is the sender and thus the consent requirement does not apply to the mobile app or website publisher that enabled the sending of the text (see for example, *Reardon v. Uber Techs., Inc., 115 F. Supp.3d 1090 (N.D. Cal. 2015)* (holding that text messages sent to recruit drivers were not advertisements or a telemarketing effort on the part of Uber and individuals who provided their phone numbers during the application process “expressly consented” to those receive text messages pursuant to the TCPA)). The 2015 FCC Order suggests that if the user has complete control over the recipients and the message, the user, not the company, is the sender. However, giving consideration to the user to send the text could arguably change the analysis as plaintiffs in some current litigation contend.

Campaigns that have a pre-recorded call component, which are becoming popular as part of alternative reality interactive promotional games where the user interacts via voice and graphics, are subject to additional complex regulations intended to govern pre-recorded telemarketing calls.

For more information, see *Don't Call Us, We'll Call You, Data Privacy Monitor* (15 July 2015) and *FCC's New TCPA Order May Require Companies to Obtain Updated Consents for Marketing Calls and Texts, Data Privacy Monitor* (July 22, 2015).

For sanctions, see *Question 7*.

2. How does national law regulate direct marketing by fax?

Federal regulations

The TCPA prohibits the sending of unsolicited commercial advertisements to a person or business by fax (see *47 USC. § 227*). The FCC has adopted regulations under the TCPA (see *47 C.F.R. § 64.1200 et seq.;* see also *American Teleservices Association, Telephone Consumer Protection Act 1991 Compliance Guidelines*). Prior written consent is required except for where there is an existing business relationship. In this case, the Junk Fax Prevention Act 2005 (JFPA) states that consent can be inferred from the relationship, and it permits the sending of commercial faxes to recipients based on an existing business relationship, as long as the sender offers an opt-out in accordance with the Act.

Existing business relationship

An existing business relationship exists if the fax recipient has entered into a purchase or services transaction with the sender within the past 18 months or if the recipient has made an inquiry or application with the sender during the past three months. The JFPA permits faxes to both consumers and businesses. It also imposes requirements on how fax numbers can be obtained. Senders wishing to rely on the existing business relationship may only collect fax numbers from new customers either:

- Trough the voluntary communication of the fax number from the customer within the context of the business relationship.
- From a directory or internet site where recipients have voluntarily agreed to make fax numbers available for public distribution. Existing business relationship customer fax numbers possessed before the effective date are not subject to this requirement.

Opt-out information

All fax advertisements must include a notice and contact information on the first page of the fax that allows recipients to opt out of future faxes. The opt-out information must be easy to find, and include a cost-free way to submit the opt-out request to the sender, such as a toll-free phone number, local phone number, website address or e-mail

address. These opt-out contact options must be available 24 hours a day, seven days a week. Opt-out requests must be honoured within 30 days.

In addition, under the FCC regulations, the business or entity on whose behalf the fax is being sent must identify itself in the top or bottom margin of each page or on the first page of the fax message, and must include its telephone number and the date and time the fax is sent. If a facsimile broadcaster (the person or entity transmitting messages to a fax machine on another person's behalf) demonstrates a high degree of involvement in the sender's facsimile messages, such as supplying the facsimile numbers to which a message is sent, the facsimile broadcaster must provide its name on the fax. A facsimile broadcaster may be liable if it supplies facsimile numbers to a business or entity sending unlawful fax advertisements. Finally, faxes sent to fax servers and personal computers are covered by the faxing rules.

Seller's vicarious liability

Although the 2013 FCC Amendment clarified that a seller may be vicariously liable for a third party's telemarketing activity, it is unclear whether this also applies to faxes. At least one court has held that an entity is not a per se "sender" under the TCPA merely because its goods or services are advertised in the faxes at issue, where the faxes were not created by the defendant company (*Cin-Q Autos., Inc. v. Buccaneers Ltd. P'ship, No. 8:13–cv–01592–AEP, 2014 WL 7224943 (M.D. Fla. Dec. 17, 2014)*). However, the same case in selecting and contracting with vendors as is recommended for telemarketing should be taken for fax marketing service providers.

For sanctions, see *Question 7*.

State regulations

A majority of states have also enacted their own laws regulating unsolicited commercial fax transmissions. Notably, California attempted to eliminate the TCPA's exception for existing business relationships with legislation applicable to unsolicited faxes sent to or from a fax machine located within the state. The law, however, was declared unconstitutional when applied to interstate fax transmissions due to the TCPA's pre-emption of interstate regulation. Most of the state laws contain provisions that are more restrictive than, or different from, the federal rules in the following areas:

- Whether prior express invitation or permission is always required.
- How prior express invitation or permission may be conveyed.
- The content of notices that must be provided to recipients.
- The format of requisite notices (for example, minimum font size).
- The deadlines for complying with an opt-out request.
- Permissible opt-out methods.

These greater state-level protections will apply to intra-state faxes, and applicable state laws must be consulted for such fax marketing communications.

3. How does national law regulate direct mail advertising?

There is no national prohibition of direct mail advertising. The Deceptive Mail Prevention and Enforcement Act (DMPEA) (*39 U.S.C. Section 3001*), however, provides for certain types of non-mailable matter. It is unlawful for a non-governmental entity to send solicitations that imply a federal government connection for the purchase of, or payment for, a product or service. In addition, the US Postal Service can prevent the use of the US mail system for the carrying out of a scheme for obtaining money or property through the mail by means of false representations, or of a lottery for the distribution of real or personal property. Additionally, it is unlawful to mail sexually-oriented advertisements to persons who notify the postal service that they do not want to receive such material.

The DMPEA also addresses promotion of sweepstakes and contests. It requires the following information in all direct mailings that contain sweepstakes or contest entry materials:

- A disclosure that no purchase is necessary and a purchase will not enhance the participant's chances of winning.
- The sponsor's name and street address.
- The complete official rules and entry procedures, which must disclose all the material terms and conditions of the sweepstakes or contest, the nature and value of the prize and the numeric odds of receiving the prize, if applicable.

Direct marketers who send such sweepstakes or contest mailings must maintain a name removal system, which allows the recipients to opt out of receiving future sweepstakes or contest mailings. The direct mail piece must disclose the existence of this name removal system to recipients.

Direct mail solicitations not in compliance with the Act are deemed non-mailable matter and are subject to mail detention and prosecution by the United States Postal Service. For sanctions, see *Question 7*.

Direct mail solicitations involving sweepstakes or contests are also regulated by all 50 states, as well as some US territories, but these laws apply to in-state activities and recipients (see *Question 8*).

Direct Mail advertising, like all advertising, must also be in compliance with the Federal Trade Commission Act (FTC Act) (*15 U.S.C §§ 41-58*), as amended, which allows the FTC to protect against unfair or deceptive acts affecting commerce through regulating such acts and practices, and by seeking redress for injuries caused to consumers, as well as state consumer protection laws.

4. How does national law regulate direct marketing by e-mail?

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (*15 USC 7701*):

- Establishes requirements for those who send commercial (that is, promotional) and transactional e-mail (though transactional e-mails are less regulated).
- Provides penalties for violators and companies whose products are advertised in spam in violation of the law.
- Gives consumers the right to opt-out of commercial e-mails.

It applies equally to e-mails to consumers and to business recipients and there is no business-to-business exception.

The law primarily covers e-mail, the primary purpose of which is advertising or promoting a commercial product or service, including content on a website (which the Act designates as a “commercial” e-mail). A transactional or relationship message e-mail may not contain false or misleading information, but otherwise is exempt from most provisions of the CAN-SPAM Act. "Transactional or relationship messages,” are messages whose primary purpose is to:

- Facilitate or confirm an agreed-upon commercial transaction.
- Provide warranty or safety information about a product purchased or used by the recipient.
- Provide certain information regarding an ongoing commercial relationship.
- Provide information related to employment or a related benefit plan.
- Deliver goods or services to which the recipient is entitled under the terms of an agreed upon transaction.

The message's primary purpose would likely be commercial and therefore subject to the CAN-SPAM Act if either:

- The recipient would interpret the subject line to mean that the message contains commercial advertising.
- A substantial part of the transactional or relationship content does not appear at the beginning of the message.

The law’s basic provisions include:

- A ban on false or misleading header information (an e-mail’s from and to routing information, including the originating domain name and e-mail address).
- A prohibition on deceptive subject lines.
- A requirement that those who send commercial e-mail must give recipients a free, easy-to-use opt-out method. Consumers can be given options to unsubscribe to less than all commercial e-mails, but there must be an option to unsubscribe to all.
- A ban on commercial e-mails to consumers who have opted out, unless they subsequently opt-in.
- An express opt-in requirement (that meets certain requirements) for e-mails to mobile domains.
- A requirement that commercial e-mail be identified as an advertisement and include the sender’s valid physical postal address.

- A requirement that commercial e-mails contain a functioning, clearly and conspicuously displayed return e-mail address that allows the recipient to contact the sender.
- A requirement of warning labels on commercial electronic mail that contains sexually oriented material.

The CAN-SPAM Act authorises the FTC to adopt and enforce rules related to commercial e-mails sent to computers, while the FCC is authorised to adopt and enforce rules regarding commercial e-mails sent to wireless domains (for example, Alan@phonecompany.com).

E-mails and text messages sent to wireless domains

The FCC Rules and Regulations Implementing the CAN-SPAM Act, and Rules and Regulations Implementing the TCPA (Implementation Rules (*69 FR 55765*), issued on 16 September 2004) clarify the applicability of the CAN-SPAM Act to e-mails and text messages sent to mobile domains.

Under the Implementation Rules, the CAN-SPAM Act does encompass e-mails sent via mobile telco specifically to mobile handheld wireless devices (that is, to a mobile domain or e-mail to text). Additionally, to facilitate implementation of the CAN-SPAM Act provisions for handheld devices, the FCC rules also established a wireless domain registry and the requirement that wireless service providers supply the FCC with wireless mail domain names. According to the Implementation Rules, any commercial message sent to an e-mail address that is on the registry is prohibited unless the recipient provided express prior authorisation (therefore, opt-in as opposed to the opt-out scheme that otherwise applies to traditional commercial e-mails). Even if the recipient has provided express prior authorisation, the sender must allow the recipient to opt-out of receiving additional messages.

Requirements applicable to the sender

The CAN-SPAM Act contains a number of requirements generally applicable to the sender of a commercial e-mail message. A "sender" is anyone who initiates an e-mail message and whose product or service is advertised or promoted by the message. More than one person may be deemed to have initiated a message. A 2008 FTC regulation clarifies a number of statutory definitions in the Act, including that the entity identified in the "from" line can generally be considered the single sender, so long as there is compliance with the other provisions of the Act (*16 C.F.R. Part 316, Federal Trade Commission: CAN-SPAM Act: A Compliance Guide for Business*; *Federal Trade Commission: FTC Approves New Rule Provision Under the CAN-SPAM Act*).

The 2008 regulation also provides additional detail on:

- A prohibition on having the e-mail recipient pay a fee to opt out.
- The definition of "valid physical postal address" to include a post office box.
- The application of the term person to apply beyond natural persons.

A company will not be deemed the sender of an e-mail it facilitates or encourages a consumer to send, such as a promotional "invite-a-friend" message, except if it gives the consumer anything of value to do so (including a sweepstakes entry). In this case it will be responsible for ensuring the consumer does not send to anyone that has opted-out from commercial e-mails from that company, and that the consumer's e-mail includes a mechanism for the recipient to opt-out from future commercial e-mails from that Company. Accordingly, companies will either need to avoid giving consideration to those it encourages or assists in sending promotional messages, or design a

facilitation tool that enables compliance with the CAN-SPAM Act's opt-out and other sender compliance obligations, and suppresses e-mails to mobile domains.

Enforcement

The FTC is authorised to enforce the Act, including seeking injunctive relief and civil penalties. Internet Service Providers can bring a private right of action. The Act also gives the Department of Justice (DOJ) the authority to enforce it and, in certain circumstances, seek criminal sanctions. The DOJ can seek criminal penalties, including imprisonment, for commercial e-mailers who do or conspire to:

- Use another computer without authorisation and send commercial e-mail from or through it.
- Use a computer to relay or retransmit multiple commercial e-mail messages to deceive or mislead recipients or an internet access service about the origin of the message.
- Falsify header information in multiple e-mail messages and initiate the transmission of such messages.
- Register for multiple e-mail accounts or domain names using information that falsifies the identity of the actual registrant.
- Falsely represent themselves as owners of multiple internet Protocol addresses that are used to send commercial e-mail messages.

Deceptive e-mail campaigns

In addition to the CAN-SPAM Act (*15 USC. § 45(a)*), the FTC has exercised its authority under section 5(a) of the FTC Act to pursue deceptive commercial e-mail. Section 5(a) prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC can initiate federal district court proceedings to enjoin such violations of the Act and secure such other equitable relief as appropriate (including disgorgement and redress). For sanctions, see *Question 7*.

A 2 June 2016, FTC lawsuit against a Florida-based marketing operation is a good example of the types of CAN-SPAM and deceptive e-mail marketing campaigns the FTC goes after. The FTC complaint in that case alleges that the “defendants have initiated unsolicited commercial electronic mail messages to include consumers to click on links in the messages.” The operation attempted to sell consumers bogus weight-loss products through a number of deceptive tactics. According to the FTC’s complaint, the corporation used hacked e-mail accounts to send consumers e-mails that appeared to be from the family or friends of the consumer. The e-mail messages had misleading FROM: addresses and lured customers to click links that directed them to websites that were deceptive in their promotion of the defendant’s weight-loss products. For example, the links sent consumers to what looked like a news site. The FTC complaint also alleges that they were not real news sites but rather paid advertisements with links to the defendant’s diet products. See *Federal trade Commission: FTC Charges Marketers Used Massive Spam Campaign To Pitch Bogus Weight-Loss Products*.

Before the CAN-SPAM Act, most of the specific legislation enacted against unsolicited e-mail was at the state level. The CAN-SPAM Act pre-empts all state and local laws that directly regulate commercial e-mail, except that it expressly does not pre-empt state laws to the extent they deal with fraud or deception or "computer crime." Accordingly, more restrictive state laws, many of which permit a private right of action (including class action claims), may still potentially be used where there is a fraud or deception involved in the sending of the email (for example, disguised sender) or the content.

5. How does national law regulate direct marketing by text messaging (SMS)?

There are no federal regulations expressly addressing direct marketing by text messaging, although a "call" as used in the TCPA has been held by the courts and the FCC to govern text messaging. Accordingly, the requirements under the TCPA for calls to wireless numbers apply (see *Question 1*).

The TCPA provides a private right of action for those seeking injunctive and monetary relief in state court for violations of its provisions, making improper campaigns attractive for class action litigation. This has resulted in hundreds of class action lawsuits, frequently ending in eight figure settlements. To reduce the risk of becoming the target of a plaintiff's class action claim for TCPA, companies wanting to use text messaging for direct marketing should undertake the following:

- Determine whether they are using an ATDS and if the TCPA applies to them.
- Obtain verifiable, express, prior, written consent (even from those with whom they have an established business relationship) if the purpose or content is promotional (for non-telemarketing or informational messages, consent need not be written) and keep good records to prove they have the consent.
- Understand and comply with all the TCPA operational rules (for example, termination of consent) and do so.
- Obtain advance consent to send one final text message confirming cancellation of a text messaging campaign.
- Examine their existing databases and those of their vendors, and understand how the database was created, and whether the consent was adequate to meet the new rules.
- Eliminate any numbers that they cannot confirm comply with the rules.
- Review their agreements with third party vendors to ensure they are required to comply with the new rules and provide for adequate indemnification.

Text messages may also be covered by the CAN-SPAM Act which requires the FCC to issue rules with regard to mobile service commercial messages. The Implementation Rules issued by the FCC address the CAN-SPAM Act's applicability to SMS messaging (*69 FR 55765*). An SMS message is covered by the CAN-SPAM Act if it is an internet-to-phone SMS, which involves addresses that reference internet domains. The Act prohibits senders from sending mobile service commercial messages without the recipient's express prior authorisation. By contrast, if the SMS messaging does not involve addresses that reference to the internet, as in phone to phone text messaging, then the CAN-SPAM Act does not apply.

The TCPA and the CAN-SPAM Act apply generally regardless of whether the recipient phone number is registered to a business (non-profits are not generally covered when they act on their own behalf, with certain exceptions such as the need to get express consent (need not be written) for calls and texts to wireless numbers) or an individual, but the TCPA has certain provisions that only apply to residential landlines and provisions that treat wireless (and fax) differently than landlines.

For sanctions, see *Question 7*.

Many states have either express laws governing text messaging, or more general laws against consumer deception that may apply.

6. How do your national data protection regulations impact on direct marketing campaigns?

EU-US Privacy Shield

There is no omnibus national data protection regulation in the United States and its patchwork of privacy and data protection laws are considered inadequate by the European Union and some other territories worldwide.

In the past, personal data could be transferred to companies in the United States which had signed up to the safe harbor principles agreed between the European Commission and the US Department of Commerce (DoC). The Safe Harbor framework was declared invalid in October 2015 by the European Court of Justice (CJEU) (*Maximillian Schrems v. Data Protection Commissioner, C-362/14 (Oct. 6, 2015)*). It has now been replaced by the EU-US Privacy Shield. The Privacy Shield will function as a similar self-certification process to its predecessor but promises to be able to withstand legal challenge, guarantee EU citizens their fundamental right to protection of personal data, ensure legal certainty for businesses, and help build a Digital Single Market in the EU.

US Organisations wishing to self-certify under the Privacy Shield will have to pledge their compliance with its seven core and 16 supplemental principles, which are based on European Data Protection Law. The Privacy Shield is monitored by the DoC and Department of Transport (DoT) and enforced by the Federal Trade Commission (FTC) or the DoT. The DoC began accepting applications from 1 August 2016 and the framework has been fully functional since late 2017. Organisations may no longer rely on the Safe Harbour. In addition to the privacy shield, companies may continue to implement alternative mechanisms of transferring personal data from the EEA to the United States, such as data subject consent, Model Contractual Clauses, or Binding Corporate Rules. However, an EU court has recently found Model Contractual Clauses to be inadequate, calling into question their continued validity

The following US data protection laws may have an impact on direct marketing:

Driver's licence and social security numbers

The Drivers Privacy Protection Act (*18 USC. § 2721-2725*) restricts the sale or release of a driver's personal information. It allows state Departments of Motor Vehicles (DMVs) to distribute personal information only to law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses. The Act generally prevents these agencies from distributing information for direct marketing and other uses.

Most states have similar laws, many of which further restrict collection or use of driver's licence information from other sources as well as from DMVs.

There are many laws regulating social security numbers, including those limiting collection, use and publication, and those requiring security and notification in the event of security breach.

Children and students

Collection of personal information

The federal Children's Online Privacy Protection Act 1998 (*15 USC. § 6501 et seq*) (COPPA) restricts collection of personal information by commercial parties from individuals under 13 years of age (child or children) absent certain statutory exceptions.

FTC regulations adopted under the Act state that an operator of a website, mobile app or online service directed at children, or an operator that has actual knowledge that it is collecting information from a child or a child-directed service, may not collect personal information (including device identifier, IP address, photos or audio of children, geolocation data, name, email, and physical address) from a child in a manner that violates the FTC's regulations. Services that target children, but not primarily so, may age screen people and apply the regulations based on self-reposted age. Services otherwise directed to children must assume all visitors are children, until otherwise verified. The operator must:

- Post a notice regarding what personal information is collected from children, how the operator uses the information, and the operator's disclosure practices for the information.
- Generally obtain parental consent (in most cases in verified form, using exacting methods) for the collection, use, or disclosure of personal information from children, unless an exception applies. Certain exceptions apply that relate to direct marketing, such as certain internal operations, responding to an inquiry and a one-time use exception that can be used for contest and sweepstakes winner notification purposes. Send-to-friend e-mail tools need to be implemented to avoid sending personal information. The FTC regulations establish the requirements for appropriate parental consent and the various exceptions to it.

For additional discussion on COPPA, see Alan L. Friel , *FTC Clarifies New Federal Privacy Rules that Affect Companies Targeting Kids, Adults and a Mix of Kids and Adults, but Questions Remain*, Edwards Wildman Client Advisory (April 2013).

Restrictions on advertising

In California, the Privacy Rights for California Minors in the Digital World Act, effective 1 January 2015 (*Cal. Bus. & Prof. Code §§22580-22582*), prohibits websites and online services from advertising certain items to minors if the "marketing or advertising is specifically directed to that minor based on information specific to that minor" (*Cal Bus. & Prof. Code §22580(b)(1)*). Among the prohibited items are alcoholic beverages, firearms, ammunition, spray paint, tobacco and cigarettes, fireworks, tattoos, drug paraphernalia, and obscene material (*Cal Bus. & Prof. Code §22580(i)*). An operator can comply with such restrictions by taking reasonable actions in good faith to avoid such marketing and advertising (*Cal Bus. & Prof. Code §22580(b)(2)*

The new law also implements what has been described as a "Social Eraser". This provision requires operators of websites and online services directed to minors or with actual knowledge that minors are using the website or online service to:

- Permit registered users who are minors to remove, or request removal of, content posted by the user (but not third parties).

- Provide notice that the information may be removed.
- Provide clear instructions as to how to remove.
- Provide notice that such removal mechanisms do not ensure complete or comprehensive removal .

(*Cal Bus. & Prof. Code §22581(a).*)

The operator however does not have to erase or remove content if:

- Federal or state law requires its retention.
- It was posted by a third party.
- It is anonymous data.
- The minor does not follow the instructions provided regarding how to remove or request removal.
- The minor received compensation for the content.

(*Cal Bus. & Prof. Code §22581(b).*)

Lastly, the operator is deemed to be in compliance if:

- It renders the information no longer visible to third parties (even if still on the server).
- Even after removing the public post, it remains visible because a third party has copied or reposted the content.

(*Cal Bus. & Prof. Code §22581(d).*)

Delaware's Online Privacy and Protection Act (*Del. Code Tit. 6 § 1204C(b)*) similarly prohibits marketing directed to a child "based upon information specific to that child" and prohibits marketing of the same items covered by California's law, as well as tanning equipment, dietary supplement products, lottery games, and other items. Delaware's law also includes a good faith compliance provision.

Privacy of school records

In the United States, any school or institution that provides educational services or instruction and receives funds under any programme administered by the US Department of Education is subject to the privacy requirements of the Family Educational Rights and Privacy Act (FERPA) (*20 U.S.C. §1232g*).

Subject to certain limited exceptions, such as for directory information, FERPA gives students (or in some cases their parents) the right to inspect and challenge the accuracy of a student's own education records, while prohibiting schools from disclosing those records, or any personally identifiable information about a student contained in those records, without the student's (or in some cases the parent's) consent (*Id*).

Students' privacy

Various state laws also govern students' privacy. Much of this legislation addresses the governance of data use, including the use of student data by online service providers for advertising purposes. Notably, in 2016, at least 42 bills introduced would require certain student data privacy and security contract provisions for third-party service providers and vendors. Many of the proposed bills also addressed the capacity and resource needs of school districts, which have increasingly been made responsible for student data privacy and protection in recent years.

In September 2014, California passed one of the first state laws prohibiting any commercial use of student data by educational online services marketed to K-12 students, even if these services are not licensed by schools, and would prohibit advertising on such sites or apps (*Cal. Bus. & Prof. Code §22584*). This law, known as the Student Online Personal Information Protection Act (SOPIPA), effective as of 1 January 2016, further requires that all operators, broadly defined as service providers whose applications or services are designed, marketed, and used primarily for K-12 school purposes, must take affirmative steps such as "implement[ing] and maintain[ing] reasonable security procedures and practices" (*Id. at §22584(d))*.

Another California state law requires that contracts between California school districts and businesses to provide digital data storage and management and/or digital educational software must contain certain provisions ensuring the safety of students' personal data and compliance with FERPA (*Cal. A.B. No. 1584, Cal. Educ. Code §49073.1 (2014)*).

California is not alone in comprehensively regulating students' data privacy beyond regulatory schools themselves, as many other states have passed similarly comprehensive student privacy laws that restrict the use of student data for marketing. (See for example, *Colo. Rev. Stat. §22-2-309 (2014); Idaho Code §33-133 (2014); Ky. Rev. Stat. §365.734. (2014); La. Rev. Stat. §17:3913 (2014); N.C. Gen. Stat. §115C-402.5 (2014); N.Y. Educ. Law §2-D (2014).*)

Federal legislation based on California's SOPIPA was proposed by President Barack Obama in 2015 (introduced as H.R. 2902 (114th Cong., 2015-2016)) .

Financial services, credit and credit cards

The Gramm-Leach-Bliley Act (*15 USC. §§ 6801-6810*) regulates the disclosure of non-public personal information by financial institutions.

The Act:

- Requires financial institutions to disclose their privacy policies to their customers.
- Allows customers to opt-out of sharing of personal information.
- Prohibits the institutions from sharing account numbers with non-affiliated telemarketers and direct marketers.
- Describes the conditions under which those financial institutions may disclose personal financial information about consumers to non-affiliated third parties.
- Provides a method by which consumers can prevent financial institutions from sharing their personal financial information with non-affiliated third parties by opting out of that disclosure.

The Act does not prevent a financial institution from providing non-public personal information to a non-affiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services. In 2015, an amendment to GLBA created an exception to the annual privacy notice requirement. Under the amendment, financial institutions do not need to provide annual notice to their customers if both:

- The sharing of customer information with unaffiliated third parties does not require an "opt out" right.
- They have not changed their policies and practices with regard to customer information from the previous privacy notice that was sent to their customers.

(*Fixing America's Surface Transportation Act of 2015, Pub. L. No. 114-94 (2015), 129 Stat. 1312 (2015).*)

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) may apply to direct marketing campaigns. The legislation provides consumers, companies, consumer reporting agencies and regulators with tools that expand access to credit and other financial services, enhance the accuracy of consumers' financial information, and help fight identity theft. For example, a provision of the law requires that account numbers on credit card receipts be shortened or truncated so that merchants, employees, or others who may have access to the receipts do not have access to consumers' names and full credit card numbers. The FTC is also working with banking regulators to develop a rule that will require appropriate disposal of sensitive credit report information.

Many states have enacted laws to protect consumer credit card information from being misused and seventeen US jurisdictions have laws that restrict collection of personal information in connection with a credit card transaction. Some states prohibit merchants from requiring that customers' personal information be recorded in connection with their credit card transactions, such as addresses, telephone numbers, driver's licence numbers, and even zip code (that is, regional postcode). Some, but not all states, have certain exceptions such as for shipping purposes, to prevent fraud, or for a deposit on rental equipment. None have a marketing use exception and consumer class actions have been brought when retailers have requested e-mail or other personal information for a loyalty program or marketing list at check-out. For example, California's Song-Beverly Credit Card Act (*Cal. Civil Code 1747.08*) prevents retailers from requiring a consumer to record personal identifying information as a condition for using a credit card to make a purchase, with the exception of allowing the collection of information when necessary for fulfilment, such as a shipping address. Retailers are permitted to require forms of identification such as a driver's licence, as long as the information is not recorded. Accordingly, care must be taken when collecting personal information for things like marketing and loyalty programs at point of sale.

7. What sanctions exist for breach of unsolicited marketing communications legislation?

FTC Act

Under the FTC Act, those that breach the false advertisement provisions regarding food, drugs, devices, services, or cosmetics may be liable to a fine of not more than USD5,000 or by imprisonment for not more than six months, or both (*15 U.S.C. § 52 and 54*). If there has been a prior conviction of the same violation, then the punishment is by a fine of not more than USD10,000 or by imprisonment for not more than one year, or both (*15 U.S.C. § 54*).

Other deceptive and unfair practices related to advertising and promotion, under the FTC's more general section 5 authority, are subject to remedial, equitable and injunctive action, which may include disgorgement and restitution of earnings arising out of those practices.

CAN-SPAM Act

Each breach (that is, each non-compliant e-mail) of the CAN-SPAM Act is subject to civil penalties of up to USD11,000. Injunctive relief is also available.

The Department of Justice (DOJ) may seek criminal penalties, including imprisonment, for commercial e-mailers who do or conspire to engage in certain activities (see *Question 4*).

There is no private right of action under CAN-SPAM, other than for Internet Service Providers. However, deceptive commercial e-mail is also subject to laws banning false or misleading advertising, including state laws that permit a private right of action and class action claims.

Telemarketing Act

The Telemarketing Act is enforced by the FTC, which can seek civil penalties of up to USD16,000 per violation, may seek injunctive relief to prevent further violations as well as financial and other equitable redress for injured consumers. In addition, each violation of the Telemarketing Act gives private persons a right of action against violators of the Telemarketing Act if the amount in controversy exceeds USD50,000 in actual damages. The court may also award litigation costs and attorney fees to the prevailing party.

TCPA and TSR

Enforcement TCPA is achieved through an administrative proceeding by the FCC for civil forfeiture. If the forfeiture is not paid, the DOJ may initiate a collection action in federal court. Its "do-not-call" provisions are enforced by both the FCC and consumers.

The FTC may directly bring a federal court action for injunctive relief for a breach of the Telemarketing Sales Rule (TSR) and may bring an action for civil penalties in conjunction with the Department of Justice. Violators of the TSR are subject to civil penalties of up to USD16,000 per breach.

In addition, the TCPA and the TSR both provide for private rights of action for a consumer. Under the TSR, a private citizen may bring an action if they have suffered USD50,000 or more in actual damages. The TCPA, on the other hand, does not have a damages threshold for private citizens and allows a plaintiff to recover the greater of USD500 per breach or actual damages. A breach occurs every time a caller sends an automated or pre-recorded call or text to a recipient without the required form of prior consent.

The TCPA also provides for treble damages for willful or knowing violations, while the TSR does not. The TCPA allows state attorneys general to bring actions on behalf of their residents against persons breaching the law and class actions are common, with thousands of cases brought or pending in recent years. Settlements are often in the tens of millions of dollars.

DMPEA

The Deceptive Mail Prevention and Enforcement Act (DMPEA) authorises the postal service to impose stop-mail orders and monetary penalties of:

- Up to USD25,000 for each mailing up to 50,000 pieces
- USD50,000 for each mailing from 50,000 to 100,000 pieces.
- An additional USD5,000 for each additional 10,000 pieces above 100,000, not to exceed USD1 Million.

The Postal Service may double the penalty if the mailer is in violation of a prior order (*39 USCA 3012(c)(1)*).

COPPA
A court can hold operators who breach the law liable for civil penalties of up to USD16,000 per breach. The amount of civil penalties a court assesses may turn on a number of factors, including the seriousness of the breach, whether the operator has previously breached the law, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company.

Settlements with the FTC of COPPA violations are frequently in the hundreds of thousands and millions of dollars. There is no private right of action, but state Attorneys General can also enforce COPPA. Since 2000, the FTC has brought over 20 actions under COPPA.

8. Please list additional national rules that may apply to direct marketing campaigns.

Deceptive acts or practices
The Federal Trade Commission Act

Under the Federal Trade Commission Act (*15 U.S.C. §§ 41-58, as amended*) (FTC Act) the FTC is empowered, among other things, to:

- Prevent unfair or deceptive acts or practices in or affecting commerce.
- Seek monetary redress and other relief for conduct injurious to consumers.
- Prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices. (The FTC typically issues guidance documents that explain what it believes is necessary to avoid deception or unfairness in particular circumstances (for example, use of influencers in social media and use of native advertising) which do not have the force of regulations and are more of an advisory nature.)

In interpreting section 5 of the FTC Act, the Commission has determined that a representation, omission or practice is deceptive if it is likely to mislead consumers and affect consumers' behaviour or decisions about the product or service. In addition, an act or practice is unfair if the injury it causes, or is likely to cause, is substantial, not outweighed by other benefits and not reasonably avoidable.

The FTC Act prohibits unfair or deceptive advertising in any medium, including direct marketing and online advertising, marketing and promotion. An advertisement, whether through direct mail or otherwise, must tell the truth and not mislead consumers. An advertising claim can be misleading if relevant information is left out or if the claim implies something that is not true. Often, reasonable consumers can interpret the advertisement as making several statements. Advertisers are responsible for reasonable consumer interpretations made about their products

and services through their advertisements. The FTC will look for the net impressions(s) a reasonable consumer could take from an advert.

In addition, advertising claims must be substantiated in advance. What is deemed appropriate substantiation will vary depending upon the claims being made, the product and what the FTC and its experts believe necessary to substantiate the claim. The level of appropriate substantiation may be high. For example, claims made regarding the health effects or safety of a product require competent and reliable scientific evidence to substantiate the claim. If an ad specifies a certain level of support for a claim, such as "tests show X", then the advertiser must have at least that level of support. Third parties, such as advertising agencies or direct mail designers, also may be liable for making or disseminating deceptive representations if they participate in the preparation or distribution of the advertising, or know about the deceptive claims. The FTC is empowered to seek injunctive relief through administrative actions or actions brought in federal district court against advertisers who make unfair or deceptive claims. Monetary relief in the form of consumer redress or disgorgement is also possible. Consumers do not have a private cause of action under the FTC Act.

The FTC offers numerous guidelines and advisories of business at *www.ftc.gov*.

The FTC Endorsement Guidelines

The FTC has given guidance on what it thinks is necessary for use of endorsements and testimonials to avoid being deemed deceptive under section 5 of the FTC Act. In September 2017, the FTC updated its Frequently Asked Questions guidance (2017 FTC FAQ) to the FTC's 2009 revised Endorsement and Testimonial Guidelines (Guidelines) (see Alan L. Friel, *Growing Promotional Use of Social Media in the Government's Crosshairs: The New FTC Guidelines*, AMEC M/E Insights (Winter 2009-2010).

Generally, the purpose of the Guidelines is to make sure that when third parties promote on behalf of sellers or advertisers, consumers are made aware that these statements are to be treated as advertisements, and sellers or advertisers are held accountable. Parties receiving anything of value from a seller or advertiser to discuss it, or its products or services, must disclose that connection and meet the same deception and unfairness standards as would be applied to the seller or advertiser.

The FTC also changed its prior position that an atypical consumer experience could be qualified by a "Results Not Typical" disclosure, and now requires instead a disclosure of the typical consumer results, based on sound substantiation. A newly updated 2017 FTC FAQ issued by the FTC provides further guidance on how the Guidelines should be applied to social media and native advertising, including how to give disclosures in a clear and conspicuous manner.

With regard to social media, the 2017 FTC FAQ clarified that promotional statements made by employees about their company or its products or services, or by third party influencers with a material connection to a company, must meet non-deceptive and fair advertising standards and must disclose the nature of their relationship to the company (for example, employee, paid spokesperson, got free merchandise to review, sweepstakes entrant and so on). The newly updated FAQ also provides guidance on the types of statements that would be sufficient for a speaker to show a material connection to the promoted company. With regard to native advertising, the FAQ provides for stricter requirements for promotional videos on websites or the use of products on television shows.

Companies are also tasked with training and monitoring their employees and influencers (for example bloggers and affiliate marketers) regarding this policy. Where the FTC has found evidence of sound policies, training and monitoring, it has in several cases dropped its investigation. However, it takes the position that companies are strictly liable for their influencers and such election not to prosecute is discretionary.

The FTC recently filed the first complaint against individual social media influencers for failing to disclose their material connection to a website. In September 2017, the FTC settled the complaint against two social media influencers who were owners and officers of an online gambling website, CSGOLotto, for failing to disclose their personal involvement in the website while posting on their Youtube channels and Twitter about how to win cash by gambling on the site. The settlement forbids the influencers or their company from misrepresenting that endorsers are independent users of the site and also requires them to clearly and conspicuously disclose any connections they maintain with endorsers of the site. Based on this recent FTC action, advertisers and influencers are now on notice that the FTC will enforce action directly against individuals for failure to comply with the FTC Act.

To view a copy of the new FAQ and the underlying Guides, please see *Federal Trade Commission: FTC's Endorsement Guides*.

State UDAPS

Similar to the FTC Act, states have also enacted "unfair or deceptive acts or practices" (UDAP) statutes, which supplement the FTC's section 5 authority. Some state UDAP laws are based on the Uniform Deceptive Trade Practices Act (UDTPA), which was aimed at protecting businesses from harm caused by competitors. Other state UDAP laws are based on the Model Unfair Trade Practices and Consumer Protection Law (UTPCPL), which is more focused on consumers.

These state laws vary in the degree that they follow the FTC Act and its interpretations, with some states giving it great weight and other simply being guided by it. Unlike the FTC Act, however, UDAP statutes usually provide for private enforcement by consumer-plaintiffs. In most states, the attorney general can also file a lawsuit on behalf of consumers to seek injunctive relief, restitution for deceived customers, and or disgorgement of unlawfully acquired profits.

Regulation of promotional marketing: sweepstakes and contests and cause marketing

Direct mail solicitations involving sweepstakes or contests are regulated by federal law under the Deceptive Mail Prevention and Enforcement Act (DMPEA)(*39 U.S.C. § 3001, et. seq*).

Additionally, all 50 states regulate contests and sweepstakes.

These two forms of consumer promotion differ from a lottery, which is generally prohibited by the states with very few exceptions. Lotteries have three elements:

- Prize.
- Chance.
- Consideration.

One of the three must be eliminated for the promotion to be legal. A sweepstakes eliminates consideration, such as through a free alternative method of entry, while a contest eliminates chance by determining the outcome on bona fide skill or knowledge.

Every state, the FTC, the FCC and the Postal Service have jurisdiction over some or all promotional marketing. The states have complex and differing rules on how lawfully designed sweepstakes and contests may be administered

and promoted. New York and Florida require registration and bonding if prize value exceeds USD5000, and Rhode Island requires registration of sweepstakes with in-retail elements if prizes have a value of USD500 or more.

Print ads, point of sale collateral and other promotional material for sweepstakes and contests are required to provide certain disclosures, depending on the state, which typically include the full official rules (or where they can be located and short form rules), the beginning and end date, eligibility restrictions, odds, prize value, and, for sweepstakes, that no purchase is necessary.

Also regulated by some states is charitable co-venture, or cause marketing, where a brand represents that a purchase will result in some sort of charitable contribution. Promotion terms must be clear and conspicuous not misleading. Some states require registration and bonding.

For more detailed information on the differences in state law, see Promotion & Marketing Law Book (Brand Activation Association, 8th ed. 2015).

Cross-border communications

9. Under the laws of your country, is a direct marketer bound by the laws of the country of the recipient of unsolicited commercial communication (EU principle of the country of destination)?

Decisions of US courts on choice-of-law issues relating to unsolicited commercial communications are inconsistent and no clear trend has yet emerged. Most decisions are, however, consistent with the general principle that the laws of the country of origin will apply, absent sufficient contacts with the US. What are sufficient contacts, especially related to websites where no servers are located in the US remains an evolving question. If a company is found to have sufficient contacts with the United States, however, a court may find jurisdiction over that company in the US and apply US law to a dispute relating to unsolicited commercial communications. Indeed, the FTC may claim jurisdiction where a foreign marketer has directed marketing or sales activities, including via the world wide web, to US consumers. The Children's Online Privacy Act specifically gives jurisdiction to the FTC over any online service operator that knowingly collects information from a US child, or directs its service toward US residents.

The FTC fights cross-border fraud and deception through its enforcement and policy making initiatives. On 22 December 2006, the Undertaking Spam, Spyware, and Fraud with Enforcers Beyond Borders (US SAFE WEB) Act of 2006 was enacted. The purpose of the Act was to bolster FTC's authority to pursue cross-border cases involving spam, spyware, and internet fraud and deception. Some of the significant provisions of the US SAFE WEB Act include:

- Provisioning of additional resources for the FTC and DOJ to co-operate in foreign litigation.
- Confirming the FTC's remedial authority to redress harm, including restitution to domestic or foreign victims.
- Authorising the FTC to make criminal referrals for prosecution when FTC law violations also violate US criminal laws.

- Authorising the FTC to co-operate with foreign law enforcers in investigating cases, and reciprocal information sharing.
- Protecting certain entities from liability for reporting suspected fraud or deception.

With the additional authority granted by the US SAFE WEB Act, the FTC has more enforcement power in cross-border cases. (*15 U.S.C. §§ 41 et seq*).

The FTC enters internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel®, a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide. On 24 April 2001, responding to the challenges of multinational Internet fraud, and working to enhance consumer protection and consumer confidence in e-commerce, 13 countries unveiled econsumer.gov, a joint effort to gather and share cross-border e-commerce complaints. The group now covers over 30 countries and its website can be found at *www.econsumer.gov*. The project has two components:

- A multilingual public website.
- A government, password-protected website.

The public site provides general information about consumer protection in all countries that belong to the ICPEN (International Consumer Protection Enforcement Network), contact information for consumer protection authorities in those countries, and an online complaint form. All information is available in English, French, German, and Spanish. The ICPEN, formerly known as the International Marketing Supervision Network (IMSN), is a membership organisation consisting of the trade practices law enforcement authorities of more than two dozen countries, most of which are members of the Organization for Economic Cooperation and Development (OECD). Using the existing Consumer Sentinel network (a database of consumer complaint data and other investigative information operated by the FTC), the incoming complaints will be shared through the government website with participating consumer protection law enforcers.

10. Under the laws of your country, can an individual seek redress in their own courts against a foreign company who targeted them in breach of that individual's laws against unsolicited communications?

Yes, a citizen of the United States may seek redress against a foreign company in US courts. The citizen will generally, however, be required to serve process upon that foreign company where it is located. It also will be required to demonstrate that the foreign company has sufficient contacts with the United States such that fundamental notions of fairness will not be offended by forcing the foreign company to defend against such an action in the United States.

There is no clear direction among US courts on how actions against foreign direct marketers may be received. But some US federal and state court decisions concerning efforts by residents of one of the 50 states against direct marketers in distant states have found that local residents are entitled to sue in their home jurisdiction when marketers' actions indicate that the marketers make concerted efforts to contact residents of those states. If a US plaintiff obtains a judgment by a US court against a foreign company, it can seek to collect amounts owed from the company's US-based assets. Otherwise, the plaintiff must seek enforcement of the judgment in a foreign

jurisdiction, where that country's laws will apply to whether or not, and under what circumstances, the judgment will be recognised and enforced.

Self-regulation

11. Through which organisations is direct marketing self-regulated in your country?

Advertising and marketing

The Advertising Self-Regulatory Council (ASRC). The ASRC is the primary self-regulatory body in the US for advertising, marketing and promotions. It establishes the policies and procedures for advertising industry self-regulation, including the:

- National Advertising Division (NAD).
- Children's Advertising Review Unit (CARU).
- National Advertising Review Board (NARB).
- Electronic Retailing Self-Regulation Program (ERSP).
- Online Interest-Based Advertising Accountability Program (Accountability Program.)

The self-regulatory system is administered by the Council of Better Business Bureaus and governs national advertisers. ASRC has guidelines that advertisers must comply with, and monitors and enforces them. Children's advertising is particularly regulated. It adjudicates claims between advertisers and those initiated by consumers or as a result of its own monitoring. Codes and procedures are available at: *www.asrcreviews.org*. Where companies refuse to comply with an ASRC ruling, the ASRC may refer the matter to the FTC for investigation of potential breach of section 5 of the FTC Act, or of other laws.

Direct Marketing Association. The DMA is a trade organisation of companies involved with database marketing. The DMA maintains ethical guidelines for traditional and online direct marketers. The DMA's Personal Information Guidelines, applied by the DMA to all direct marketers:

- Require fair and lawful collection methods and a direct marketing purpose for the data collection.
- Limit the scope, use, and retention of the personal data.
- Address the accuracy and upkeep of the personal data.
- Address the sale, transfer, or licence of personal information between direct marketers.
- Require that consumers be given notice and an opportunity to prevent the use of their personal information by direct marketers, and require that list providers honour such consumer requests and ensure that other industry members comply with the Guidelines and respect consumer privacy.

All DMA members are required to adopt the Association's Privacy Promise which ensures that all DMA members adhere to certain prescribed Guidelines. These Guidelines require members to provide notice (in some cases annually) to consumers that they may opt out of having their personal information rented, sold, or exchanged with third parties and that consumers can subscribe to the DMA's Mail Preference Services (see below). DMA has created the Internet Alliance, a trade association for the internet industry, which has also focused on privacy in the internet arena. The Internet Alliance has published a series of online privacy guidelines. The guidelines address issues raised by the collection of personally identifiable information by online service providers and by parties operating websites.

The Mail Preference Service of the DMA, also known as DMAchoice™, is a service that assists consumers in decreasing the amount of national non-profit or commercial mail they receive at home. A person may register with the DMAchoice name-removal file online or via the mail. The name is then placed in a delete file which is made available to companies four times a year (in January, April, July and October) and made available to direct-mail and telephone marketers. Two to three months after the name is entered on the file, a decrease in the number of solicitations will occur. Registration lasts for five years. Registration will not stop mailings or calls from organisations not registered with the DMA's Mail Preference Services. The DMA's Telephone Preference Service, also part of DMAchoice, was largely discontinued in November 2006, except for the residents of the states of Pennsylvania and Wyoming. For those states the DMA manages the states' do-not-call registries. For all other states, the DMA refers residents to the national DNC Registry. For more information on DMAchoice, see www.dmachoice.org. For more information on the national DNC Registry, see *Question 1*.

For more information on the DMA, see *www.thedma.org*.

Word of Mouth Marketing Association (WOMMA). WOMMA describes itself as the official trade association dedicated to word of mouth and social media marketing. It is the leader in ethical word of mouth marketing practices through its education such as WOMMA Summit, professional development opportunities and knowledge sharing with top industry marketers. WOMMA's membership is made up of the most innovative companies committed to progressing the word of mouth marketing industry through advocacy, education, and ethics. WOMMA members commit to following its Code of Ethics located at *www.womma.org/ethics*. WOMMA has also issued privacy guidance and social media disclosure guidance.

Interactive Advertising Bureau (IAB). The IAB is an industry trade association for the media and marketing industries. It is comprised of more than 650 leading media and technology companies that are responsible for selling, delivering, and optimising digital advertising or marketing campaigns. Together, they account for 86% of online advertising in the United States. Working with its member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organisation is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of its public policy office in Washington, D.C., the IAB advocates for its members and promotes the value of the interactive advertising industry to legislators and policymakers (see *www.iab.com*). For useful guidance on social media and native advertising best practices, see *IAB: Social Advertising Best Practices* and *IAB: Native Advertising*.

Mobile Marketing Associates (MMA). The MMA is a global non-profit trade association. Its mission is to *"accelerate the transformation and innovation of marketing through mobile, driving business growth with closer and stronger consumer engagement"* (see *www.mmaglobal.com*).

Although not mandatory, before engaging in a mobile marketing campaign it is recommended to review and comply with the MMAs US Consumer Best Practices for Messaging, which attempts to reflect applicable law and offers best practices guidance on text-message advertising and solicitations, including the disclosure of "fine print" on

cell phone advertisements, and summarises the specific requirements imposed by the major US carriers. The MMA guide notes that standard text-messaging rate programs require single opt-in and recommends double opt-in for premium text-message rate promotions. The guide, which is regularly updated, also recommends double opt-in for standard or premium rate subscription programs and a renewal or billing reminder. Additionally, the MMA has a *Code of Conduct for Mobile Marketing*, specific guides in connection with mobile promotions and *Mobile Advertising Guidelines*.

Online advertising

Digital Advertising Alliance (DAA). The DAA is a consortium of the leading national advertising and marketing trade groups who work together to establish and enforce privacy practices for digital advertising. This self-regulatory programme is dedicated, in part, to enforcing standards for the protection and education of consumers regarding online behavioural advertising (OBA). OBA is the practice of collecting data from a particular computer or device, which reveals a user's online behaviour across time and services, and using the data to deliver advertisements to that user based on the user's predicted preferences or interests. The DAA has released a suite of principles, "Self-Regulatory Principles for Online Behavioral Advertising" "Multi-site Data Guidance" and "Mobile Guidance," which promote transparency, compliance, and accountability across the marketing and advertising community. Since 2009, DAA has been working to implement these principles industry-wide and its principles are enforced by the DMA, for DMA members, and the ASRC for national advertisers and other national ad industry participants. See also Cross-Device Tracking below.

Network Advertising Initiative. This organisation is one of the participating associations in the DAA. It was established by third-party network advertisers who are in the business of delivering targeted advertising. On 1 February 2001, the seven leading internet advertising firms, including DoubleClick and 24/7 Media, announced that they had signed the Network Advertising Initiative Self Regulatory Principles Compliance Program, which implements an agreement that the companies entered into with the FTC in the summer of 2000. The Program requires various protections for privacy and regular audits. Under the terms, network advertisers shall not use personally identifiable information about sensitive medical or financial data, sexual behaviour or sexual orientation, nor social security numbers for online preference marketing. Network advertisers or organisations acting on their behalf may also not, among other things, merge previously collected non-personally identifiable data with personally identifiable data for Online Preference Marketing without the consumer's prior affirmative consent (opt-in) to any such merger. It also administers a programme for consumers to opt-out of Online Preference Marketing from its members which is similar to the DAA's OBA opt-out programme. It uses the Watchdog Dispute Resolution Program of a third party organisation called TRUSTe for consumer complaints.

Advertising Self-Regulatory Council (ASRC) Accountability Program. The Interest-Based Accountability Program is administered by the Council of Better Business Bureaus and regulates OBA. The Accountability Program provides objective and independent oversight and enforcement of the DAA's Self-Regulatory OBA principles which businesses are required to follow and that are developed by leading industry associations (see above). The goal of the program is to promote compliance with the principles by all companies that are in the advertising system. Any organisations that collect data on a non-affiliated website or mobile app and/or use the data for online advertising, such as ad networks, data aggregators, website publishers, and advertisers, are subject to the principles as are publishers that permit such tracking or OBA ad serving, and advertisers that use OBA-enabled ads. The principles give consumers greater control over whether advertisers can use their information for targeted advertisement. For consumers who prefer not to receive interest-based ads online, they can use the AdChoices Program. When consumers see an advertisement that has an AdChoices icon or message, then can click on it to opt-out from future interest-based ads. See *www.asrcreviews.org* .

On 4 November 2015, the Online Interest-Based Advertising Accountability Program published its first cases requiring the AdChoices icon sponsored "native advertising" is targeted to consumer's personal interests. Native ads are promotional messages that look like editorial content. The cases also show that the OBA principles apply to both ad formats that are traditional and to those that are the latest trend. See *ASRC: Advertisers Must Tell Consumers When Sponsored-Content is Tailored to their Specific Interests*.

In August 2017, the Accountability Program brought an enforcement action against two digital advertising companies for not complying with the online advertising industry's requirements for interest based advertising. Under these recent actions, the Accountability Program stated that first parties (typically website and mobile application publishers) and third parties (typically advertising technology companies) share the responsibility of providing enhanced notice when collecting data for interest-based advertising from non-affiliate websites. The actions also cited the importance of providing an easy mechanism for consumers to exercise choice with respect to the collection and use of cross-application data or the transfer of such data to a non-affiliate for interest based advertising. For further information on the recent enforcement actions, please see Alan L. Friel & Sara Goldstein, *Industry Watchdog Reminds Digital Advertisers of the Importance of Providing Consumers With Transparency and Choice in Latest Enforcement Actions* (August 28, 2017).

Other

Messaging industry. Messaging Anti-Abuse Working Group (MAAWG) is an organisation that brings the messaging industry together to address issues relating to messaging abuse (see *www.m3aawg.org*). MAAWG works with the ISPs to develops industry best practices guidelines and standards.

Credit Bureaus. The credit bureaus offer a toll-free number that enables a consumer to opt-out of having pre-approved credit offers for two years. Contact 1-888-5-OPTOUT (567-8688) for more information. In addition, a consumer can notify the three major credit bureaus that he or she does not want personal information about them shared for promotional purposes. The three major credit bureaus are:

- Equifax, Inc. Options PO Box 740123 Atlanta, GA 30374-0123 (see *www.experian.com/privacy/opting_out.html*).
- Experian Consumer Opt-Out PO Box 80128, Lincoln, NE 68521 (Attn: Consumer Services Dept) (see *www.experian.com*).
- TransUnion Name Removal Option PO Box 505 Woodlyn, PA 19094 (see *www.transunion.com*).

Cross-device tracking. Cross-device tracking is the process of tracking a single consumer across all of the consumer's devices. On 16 November 2015, the FTC hosted a workshop to address issues stemming from cross-device tracking and on the same day the DAA issued its Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (DAA Guidance) on how its self-regulatory principles apply to cross-device tracking. To better understand how the principles of transparency (consumer notice) and control (consumer choice) are applied to cross-device data and how they are evolving in relation to US legal and self-regulatory privacy schemes, companies that participate in cross-device tracking, or plan to engage in cross-device tracking, should read the transcript from the FTC's 16 November 2015 workshop and the DAA's Guidance. The FTC workshop had five takeaways, including that companies need to work on providing more transparency and choices for consumers, such as giving consumers the choice to opt-out of targeted advertising. According to the DAA Guidance, the DAA's current principles of transparency and control are applicable to cross-device data. See more at: *www.dataprivacymonitor.com/behavioral-advertising/the-ftc-and-daa-set-their-sights-on-cross-device-tracking*. In January 2017, the FTC released a new staff report workshop on cross-device tracking as a series of efforts to explore emerging issues in the area of online behavioural advertising. The purpose of the Report is to

put industry on notice of the FTC's reviews regarding data tracking and disclosure practices which could be deemed unfair or deceptive to consumers. See *FTC Staff Report on Cross-Tracking*.

International Association for the Wireless Communications Industry (CTIA). CTIA has issued a set of best practices that provide for, among other things, consumer notice and consent for location-based marketing, and consumer choice for sharing of location information with third parties. These guidelines also address retention and security of location-based information, abuse reporting, and public self-certification of compliance with the best practices (see *CTIA: Best Practices and Guidelines for Location-Based Services*).

12.What obligations or standards do codes of practice for direct marketing impose upon marketers?

See *Question 11*.

13. Are there any opt-out lists in your country?

For DNC Registry, see *Question 1*. For the CAN-SPAM Act opt-out provisions, see *Question 4*. For sweepstakes and contests, see *Question 8*.

The Gramm-Leach-Bliley Act allows customers to opt-out of sharing of personal information in the hands of financial institutions. The FTC Telemarketing Rule allows consumers to register their telephone number on the national DNC Registry. Under the CAN SPAM Act, recipients of unsolicited commercial e-mail must be given the opportunity and mechanism by which they may opt out of receiving future commercial e-mail solicitations. The TCPA, which is an opt-in scheme, allows for withdraw of that consent. Finally, direct mailings containing sweepstakes or contest entry materials must disclose the requirement that the advertiser maintain a name removal system, which allows the recipients to opt out of receiving future sweepstakes or contest mailings

14. What procedures exist for complaining to organisations against unsolicited communications?

The FTC provides complaint forms for consumers for all types of complaints. It maintains on its *website* complaint forms concerning general complaints and for violations of the CAN SPAM act and the national do-not-call registry. Similarly, the FCC (*www.fcc.gov*) provides complaint forms for unsolicited fax advertisements and violations of its telemarketing rules. The ASRC (and its subdivisions), the DMA and other self-regulatory bodies also solicit and act to resolve consumer complaints (see *Question 11*).

The author would like to thank Baker & Hostetler LLP associates Stephanie Lucas and Moustafa Badreldin for their help in updating this piece.

END OF DOCUMENT

