THOMSON REUTERS
PRACTICAL LAW™

Direct Marketing in the US: Overview

by Practical Law Commercial Transactions, with Alan L. Friel, Katy Spicer, and Kyle R. Dull, Squire Patton Boggs

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/5-500-4203**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Practice Note providing a general overview of the legal issues surrounding direct marketing in the United States. This Note considers the statutes, regulations, and voluntary codes of practice that apply to direct marketing activities, including marketing by telephone, fax, email, text message, and mail. It also discusses means of consumer recourse and regulatory enforcement.

Direct marketing consists of communications by which the sender tries to sell or market certain goods or services directly to consumers, without the use of traditional forms of third-party publishers (such as radio, newspapers, and television) as intermediaries. In a direct marketing campaign, the sender communicates directly with a targeted consumer group through telephone, fax, email, text message, or mail. These communications are often unsolicited. For a discussion of issues that apply to advertising generally, see Practice Note, Advertising: Overview.

Direct marketing is a powerful business tool because of its low cost of entry and potentially immediate consumer response to a direct marketing campaign, which often translates into real-time revenue growth. However, if used in an irresponsible way, it can cause substantial nuisance, cost, and inconvenience to consumers and internet service providers, whose networks can be slowed down considerably by mass unsolicited email. Direct marketing campaigns involve complicated legal issues arising from several statutes, regulations, and voluntary codes of practice, the various provisions of which are not always consistent.

Although online behavioral advertising and other targeted online messaging may be considered forms of direct marketing, those tactics are beyond the scope of this Note (for a discussion of those topics, see Practice Notes, Online Advertising and Marketing and Advertising and Promotions in Social Media).

This Practice Note focuses on the legal issues relevant to direct marketing by telephone, fax, email, text message, and mail and considers, in particular:

- The laws and regulations that govern commercial communications by those methods.
- Additional federal laws and regulations that may apply to direct marketing campaigns.
- Policies on cross-border communications.
- The application of self-regulation and codes of practice.
- Consumer complaints and regulatory enforcement.

This Note also includes best practices to help make informed legal risk decisions (see Direct Marketing Campaign Best Practices).

Regulation of Unsolicited Commercial Communications

Nearly all direct marketing activities are affected by federal regulations. In recent years, advertisers have moved quickly to exploit the potential of newly developed media to sell their products and services. These sales techniques, mostly in the form of unsolicited commercial communications, have led to a variety of statutory responses. Current rules and regulations address communications by telephone, fax, email, text message, and mail.

Telephone

Federal rules that cover unsolicited commercial communication by telephone include:

- The Telemarketing Consumer Fraud and Abuse Prevention Act (see Telemarketing Consumer Fraud and Abuse Prevention Act).
- The Telemarketing Sales Rule (see Telemarketing Sales Rule).

- The Telephone Consumer Protection Act (see Telephone Consumer Protection Act).
- The National Do-Not-Call Registry (National DNC Registry) (see National DNC Registry).

Telemarketing Consumer Fraud and Abuse Prevention Act

The Telemarketing Consumer Fraud and Abuse Prevention Act (Telemarketing Act):

- Prohibits specific deceptive and abusive telemarketing acts or practices.
- Requires disclosure of certain material information.
- Requires express verifiable authorization for certain payment mechanisms.
- Sets record-keeping requirements.
- Specifies exempt transactions (like certain business-to-business calls).

(15 U.S.C. §§ 6101 to 6108.)

The Telemarketing Act directs the Federal Trade Commission (FTC) to implement the statute. The Act also establishes a private right of action in the federal courts, as well as a right for any state Attorney General to bring a civil action in federal court. For more information on FTC enforcement, see Practice Note, FTC Consumer Protection Investigations and Enforcement.

Telemarketing Sales Rule

The FTC established the Telemarketing Sales Rule (TSR) under the Telemarketing Act (16 C.F.R. §§ 310.1 to 310.9). The TSR applies to companies that sell goods or services by telephone and which involve more than one interstate telephone call. It covers:

- "Telemarketers," which are the entities that initiate or receive telephone calls to or from consumers.
- "Sellers," which are the entities that provide or arrange to provide the goods and services being offered.
- Calls by these entities originating outside the US made to consumers in the US.

The TSR prohibits deceptive and abusive telemarketing acts or practices and requires these entities to:

- Limit calls only between 8:00 a.m. to 9:00 p.m. recipient's time (same time under FCC rule).
- Screen and scrub names against the National DNC Registry (see National DNC Registry).
- Honor do-not-call requests and maintain an internal 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's or seller's caller ID information.
- Identify themselves and what they are selling or 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.
- Comply with special rules for prize promotions.
- 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 authorization to be charged (consent to the recording needs to be obtained to comply with other laws).
- Not to engage in unauthorized billing.

(16 C.F.R. §310.4.)

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act), amended the Telemarketing Act and brought charitable solicitations by for-profit telemarketers within the scope of the TSR (non-profit entities are beyond the FTC's jurisdiction, except for trade organizations that represent for-profit interests). As a result, most of the TSR's provisions, including mandatory disclosures and prohibited misrepresentations, apply to for-profit companies that solicit charitable contributions on behalf of non-profit organizations. These calls are exempt from the National DNC Registry requirements (see National DNC Registry), but the companies must keep their own do-not-call lists and honor requests not to be called.

Some types of calls are not covered by the TSR, regardless of whether the entity making or receiving the call is covered. These include:

- Unsolicited calls from consumers.
- Calls placed by consumers in response to a catalogue.

- Business-to-business calls that do not involve retail sales of non-durable office or cleaning supplies.
- Calls made in response to general media advertising, except those relating to credit card loss protection, credit repair, recovery services, advance-fee loans, investment opportunities, and certain business opportunities.
- Calls made in response to direct mail advertising, provided that the advertising is truthful, not misleading, and contains all of the disclosures required by the TSR. However, there is no exemption for calls responding to any direct mail advertising relating to credit card loss protection, credit repair, recovery services, advance-fee loans, investment opportunities, prize promotions, and certain business opportunities.
- Entities not covered by the FTC's jurisdiction who call consumers directly (but companies hired by these entities to provide telemarketing services are covered), including:
  - financial institutions, like banks, federal credit unions, and federal savings and loans;
  - common carriers, like telephone companies and airlines when they are engaging in common carrier activity; and
  - non-profit organizations.

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

Telephone Consumer Protection Act

Administered by the Federal Communications Commission (FCC), the Telephone Consumer Protection Act of 1991 (TCPA), as amended, has a much broader scope than the TSR, governing calls, texts, and faxes for both telemarketing and informational purposes. Covered calls even include ringless voicemails left on wireless lines (see Legal Update, FCC Rules That Ringless Voicemails to Consumer Wireless Phones Are Subject to TCPA Robocall Restrictions). In addition, unlike the TSR, the TCPA applies to all business-to-business calls.

The TCPA restrictions depend on the type of equipment used and the content of the message. For example, it prohibits:

- Telemarketing calls and texts to wireless lines using artificial or prerecorded voice recordings or an automatic dialing system (ATDS) without receiving prior express written consent, which consent must include certain specific language.
- Informational calls and texts to wireless lines using artificial or prerecorded voice recordings or an ATDS without receiving prior express consent (does not need to be written).
- Telemarketing calls (but not informational calls) to residential landlines using artificial or prerecorded voice recordings without receiving prior express written consent.

(47 U.S.C. § 227.)

There are some exemptions to the TCPA, including certain pro-consumer informational calls and texts for:

- Urgent healthcare matters.
- Emergency purposes.

In a 2016 declaratory ruling, the FCC had also exempted calls and texts made by or on behalf of the federal government for government debt collection purposes. In 2020, however, the Supreme Court ruled that the debt-collection exception to the TCPA's robocall restrictions unconstitutionally favored debt-collection speech over political and other speech (in violation of the First Amendment). It invalidated and severed the government debt-collection exception from the remainder of the TCPA. For more information on this ruling, see Legal Update, SCOTUS Strikes Down TCPA Government Debt Exception.

The FCC has authority to prescribe rules under the TCPA (FCC Rule), as well as to collect complaints and institute enforcement actions. Over the years, the FCC Rule has provided guidance on the FCC's interpretation of the TCPA. For example, 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; and
  - 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.
- Prohibits telemarketers from:
  - disconnecting unanswered calls before at least fifteen seconds or four rings; and
  - abandoning more than 3% of calls that are answered.

The FCC adopted regulations similar to the FTC's, prohibiting sellers and telemarketers from calling consumers who have stated that they do not wish to be called. Sellers and telemarketers must establish their own internal do-not-call lists and refrain from calling consumers on those internal lists as well as the numbers listed on the National DNC Registry.

There have been several FCC rulings and much litigation over what type of equipment comprises an ATDS. In *ACA International v. FCC*, the DC Circuit set aside the FCC's 2015 ruling on its interpretation of the definition of ATDS (885 F.3d 687 (D.C. Cir. 2018)). After that decision, the Circuit Courts split over the definition in the absence of the FCC guidance.

The Supreme Court brought closure to this split in its decision in *Facebook, Inc. v. Duguid* (141 S.Ct. 1163 (2021)). Pursuant to this decision, a device must have the capacity to use a random or sequential number generator to either store or create phone numbers to be an ATDS. Predictive dialers and other devices that store set lists of phone numbers and dial from these lists without using a random or sequential number generator do not qualify as an ATDS. For more information on the *Duguid* decision and its implications, see Legal Update, Supreme Court Reverses Ninth Circuit and Defines ATDS Under the TCPA.

The FCC has also clarified that if a calling platform is incapable of dialing numbers without a person "actively and affirmatively manually dialing each one," that platform is not an ATDS. It remains to be seen how courts will interpret this ruling after *Duguid* (see Legal Update, FCC Issues Declaratory TCPA Ruling: Certain P2P Text Messaging Platforms Are Not Autodialers). Nonetheless, some states (such as Oklahoma) have TCPA-like telemarketing laws where the definition of ATDS has not been as narrowly defined (see State Telemarketing Laws).

For more information on the evolution of the ATDS definition, see Practice Note, Telephone Consumer Protection Act (TCPA): Overview: Defining an ATDS.

For more information on the TCPA generally, see Practice Notes, TCPA Litigation: Key Issues and Considerations and Telephone Consumer Protection Act (TCPA): Overview.

National DNC Registry

The National DNC Registry was established by the 2002 DNC Registry Act. The National DNC Registry empowers consumers to stop calls from almost all companies within the FTC's and FCC's jurisdiction. Telephone numbers on the registry are only removed when they are disconnected and reassigned, or when consumers choose to remove them. Telemarketers covered by the registry have up to 31 days from the date a consumer registers to stop calling.

Under both the TSR and the TCPA, telemarketers are prohibited from calling consumer landline and wireless number that consumers add to the National DNC Registry unless an exception applies. The TSR and TCPA, however, have different exceptions. For example, under the TSR, the National DNC Registry does not cover calls where there is an established business relationship (EBR). An EBR is defined as an existing, voluntary relationship between the two parties, among other requirements established by the TSR or TCPA. The TCPA does not have an EBR exception for calls (including texts) to either residential landlines or wireless numbers, but does for fax solicitation.

There are stiff penalties for violating the DNC Registry Act, including civil penalties and a private right of action. The National DNC Registry restrictions are not tied to use of an ATDS, so plaintiffs are now concentrating on claims under this regime for unsolicited calls where an EBR is lacking rather than having to address the ATDS issue under the TCPA.

State Telemarketing Laws

The TSR and the TCPA do not preempt state laws that govern intrastate telemarketing. In the wake of the federal narrowing of what is an ATDS (see Telephone Consumer Protection Act), some plaintiffs are electing to bring claims under state laws where the ATDS definition has not been narrowed. Many states have enacted their own telemarketing laws that create additional legal requirements for telemarketers. For example, some states require that telemarketers:

- Limit their calls to certain hours that are different than those set by the TCPA.
- Obtain a license or register with the state.
- Identify themselves at the beginning of the call.
- Terminate a call without rebuttal at the request of the recipient.

Several states have recently expanded their telemarketing restrictions. See Legal Update, New York Expands Telemarketing Definition to Include Text Messages.

Many states have enacted opt-out legislation for telephone marketing, instead requiring the creation of statewide do-not-call registries. The National DNC Registry does not preempt state do-not-call laws. In 2013, Congress tasked the FTC to work with those states that have enacted do-not-call registry laws, to transition to one harmonized do-not-call registry system and a single set of compliance obligations. The process is not yet complete. Under some state laws, compliance with the FTC's do-not-call regulations is deemed to be compliance with that state's laws. At least twelve 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.

Fax

The TCPA prohibits sending unsolicited commercial advertisements to a person or business by fax. The FCC has adopted regulations under the TCPA regarding unsolicited fax advertisements (47 C.F.R. § 64.1200). Prior written consent is required except for where there is an EBR. In this case, the Junk Fax Prevention Act of 2005 (JFPA) states that consent can be inferred from the relationship, and it permits the sending of commercial faxes to recipients based on an EBR if the sender offers an opt-out in accordance with the TCPA.

An EBR exists if the fax recipient has either:

- Entered into a purchase or services transaction with the sender within the past 18 months.
- Made an inquiry or application with the sender during the past three months.

The JFPA permits unsolicited faxes to both consumers and businesses under an EBR exception. It also imposes requirements on how fax numbers can be obtained. Senders wishing to rely on an EBR may only collect fax numbers from new customers either:

- Through 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. EBR customer fax numbers possessed before the effective date of the JFPA are not subject to this requirement.

All unsolicited 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.
- Include a cost-free way to submit the opt-out request to the sender (like by email or a toll-free phone number) that is available 24 hours a day, seven days a week.

Opt-out requests must be honored within 30 days.

In addition, the business or entity on whose behalf a 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 with the date and time the fax is sent. If a fax broadcaster (the person or entity transmitting messages to a fax machine on another's behalf) demonstrates a high degree of involvement in the sender's fax messages, such as supplying the fax numbers to which a message is sent, the fax broadcaster must provide its name on the fax. A fax broadcaster may be liable if it supplies fax numbers to a business or entity sending unlawful fax advertisements.

On March 31, 2017, the US Court of Appeals for the District of Colombia Circuit invalidated FCC rulings that required opt-out language on solicited fax advertisements. The court held that although the TCPA gives the FCC the authority to regulate unsolicited fax advertisements, the law does not grant the FCC authority to require opt-out notices on **solicited** fax advertisements (fax advertisements sent with the recipient's prior express invitation or permission). (*Bais Yaakov of Spring Valley v. FCC,* 852 F.3d 1078 (D.C. Cir. 2017).) For more information on the DC Circuit's decision in *Bais YaaKov of Spring Valley*, see Legal Update, Updated: Supreme Court Declines to Review D.C. Circuit's Decision Overturning FCC's Solicited Fax Rule.

State Fax Laws

A majority of states have also enacted their own laws regulating unsolicited commercial fax transmissions. 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 apply to **intrastate** faxes and applicable state laws must be consulted for these communications.

Email

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

- Establishes requirements for those who send commercial (that is, promotional) and transactional email (though transactional emails are less regulated).

- Provides penalties for violators and companies whose products are advertised in commercial email in violation of the law.
- Gives consumers the right to opt out of commercial email.

(15 U.S.C. § 7701.)

It applies equally to emails to consumers and to business recipients.

CAN-SPAM covers email messages that aim to advertise or promote a commercial product or service, including content on a website (which CAN-SPAM designates as commercial email). An email message that facilitates an agreed-on transaction or updates a customer in an EBR (which CAN-SPAM designates as transactional email) may not contain false or misleading routing information, but otherwise is exempt from most provisions of CAN-SPAM. CAN-SPAM does not eliminate unsolicited commercial email, but instead provides an opt-out structure. Companies can send emails to prospects, but must respect the right of recipients to opt out of unwanted communications.

The law's main provisions:

- Ban false or misleading header information in commercial and transactional emails (an email's routing information, including the originating domain name and email address).
- Prohibit deceptive subject lines in commercial and transactional emails.
- Require that those who send commercial email must give recipients a free, easy-to-use opt-out method that is clearly and conspicuously disclosed.
- Require commercial emails to clearly and conspicuously display a functioning return email address that allows the recipient to contact the sender.
- Require a sender to cease sending commercial emails to any individual who has asked not to receive future commercial emails within ten business days of the request.
- Require that commercial email be identified as an advertisement and include the sender's valid physical postal address.
- Require that warning labels be added to commercial email that contains sexually oriented material.

CAN-SPAM authorizes the FTC to adopt and enforce rules regarding commercial email sent to computers, but authorizes the FCC to adopt and enforce rules regarding commercial email sent directly to wireless phones and mobile devices such as using wireless domains and email to text tools (see Text Message).

CAN-SPAM preempts all state and local laws that directly regulate commercial email, except that it expressly does not preempt 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 taking over a user's address book to send to all without clear indication that this would occur) or the content.

For more on CAN-SPAM and email marketing, see Practice Note, CAN-SPAM Act Compliance and Email Marketing Campaign: CAN-SPAM Act Compliance Checklist.

Text Message

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 also apply to texts (see Telephone Consumer Protection Act). In addition, state telemarketing laws typically apply to text messages (see State Telemarketing Laws).

Text messages may also be covered by CAN-SPAM which requires the FCC to issue rules and regulations related to mobile service commercial messages (Implementation Rules) (69 Fed. Reg. 55765 (Sept. 16, 2004)). The FCC's Implementation Rules address CAN-SPAM's applicability to messaging to wireless devices and provide that the technology employed to send the message determines whether it is covered by CAN-SPAM. If the text message is from internet-to-phone and involves a recipient address that reference an internet domain (like "customername@wirelesscompany.com"), then it is covered by CAN-SPAM.

The Implementation Rules create an opt-in structure for sending mobile service commercial messages (MSCMs) to wireless devices (as opposed to the opt-out structure established by CAN-SPAM for traditional commercial emails). Senders are prohibited from sending MSCMs to wireless devices without the recipient's express prior authorization. The FCC has issued detailed requirements for obtaining and revoking express prior authorization, including that:

- Express prior authorization only occurs when the consumer has taken an affirmative action to give

authorization. Authorization may not be obtained in the form of a negative option, like a pre-checked box. If the authorization is obtained via a website, the consumer must take an affirmative action, such as checking a box or hitting a button.

- The authorization must be given prior to the sending of any MSCMs.
- Consumers must not bear any cost with respect to the authorization or revocation processes.
- Each authorization must include certain required disclosures stating that the subscriber:
  - is agreeing to receive MSCMs sent to their wireless device from a particular (identified) sender;
  - may be charged by their wireless provider in connection with the receipt of such messages; and
  - may revoke the authorization at any time.
- The required disclosures must be clearly legible and in sufficiently large type (or volume, if given via audio). They must be presented in a manner that is readily apparent to the consumer and must be separate from any other authorizations contained in another document.
- The authorization must be specific to the sender and must clearly identify the entity that is being authorized to send the MSCMs. The Implementation Rules prohibit any sender from sending MSCMs on behalf of other third parties, including affiliates and marketing partners. Each entity must obtain separate express prior authorizations for the messages it sends.
- Authorization may be obtained in any format, oral or written, including electronic. Although writing is not required, the FCC requires that each sender of MSCMs must document the authorization and be able to demonstrate that a valid authorization (meeting all the other requirements) existed prior to sending the commercial message. The sender bears the burden of proof that it received compliant authorization.
- Senders must enable consumers to revoke authorizations using the same means that the consumers used to grant authorizations. (For example, if a consumer authorizes MSCMs electronically, the sender must permit the consumer to revoke the authorization electronically).
- The MSCMs themselves must include functioning return email addresses or another internet-based mechanism that is clearly and conspicuously displayed for the purpose of receiving opt-out requests.
- Consumers must not be required to view or hear any further commercial content during the opt-out process (other than institutional identification).

(47 C.F.R. § 64.3100.)

To facilitate implementation of the CAN-SPAM Act for wireless devices, the Implementation Rules also established a wireless domain registry and the requirement that wireless service providers supply the FCC with wireless mail domain names (see FCC: Domain Name Downloads). Wireless carriers are required to update this list periodically.

Mail

There is no national prohibition of direct mail advertising. However, certain types of non-mailable matter are prohibited under the Deceptive Mail Prevention and Enforcement Act (DMPEA) (39 U.S.C. § 3001). Under the DMPEA, for example:

- A non-governmental entity cannot send solicitations that imply a federal government connection for the purchase of, or payment for, a product or service.
- The US Postal Service can prevent the use of the 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.
- It is unlawful to mail sexually oriented advertisements to persons who notify the US Postal Service that they do not want to receive that material.

The DMPEA also requires certain information in all direct mailings that contain sweepstakes or contest entry materials, including:

- A disclosure that no purchase is necessary and that 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.

(39 U.S.C. § 3017.)

Direct marketers who send sweepstakes or contest entry materials must maintain a name removal system, which allows recipients to opt out of receiving future

sweepstakes or contest mailings. The mailing must disclose the existence of the name removal system to recipients. For more information, on the DMPEA regulation of direct mail sweepstakes and contests, see Practice Notes, Sales Promotions, Contests, and Sweepstakes: DMPEA and Running a Sweepstakes or Contest in the US: Direct Mail.

Direct mail solicitations involving sweepstakes or contests are also regulated by state laws that govern the conduct of lotteries, sweepstakes, and contests generally. Direct mail sweepstakes and contests must comply with the DMPEA requirements in addition to these state laws. For more information on these state laws, see Practice Notes, Sales Promotions, Contests, and Sweepstakes and Running a Sweepstakes or Contest in the US.

Additional Federal and State Laws

Consumer Protection Laws

All advertising, including direct advertising and marketing, must be in compliance with the Federal Trade Commission Act (FTC Act) (15 U.S.C. §§ 41 to 58). The FTC Act empowers the FTC to:

- Prevent unfair or deceptive acts or practices in or affecting commerce.
- Seek monetary redress and other relief for conduct injurious to consumers under certain circumstances.
- Prescribe trade regulation rules that specify which acts or practices are unfair or deceptive, and establish requirements designed to prevent these acts or practices.

In interpreting Section 5 of the FTC Act (15 U.S.C. § 45), the FTC determines whether a representation, omission, or practice is deceptive if it is likely to mislead consumers and affect consumers' behavior or decisions about a product or service. An act or practice is unfair if the injury it causes, or is likely to cause, is substantial, and is neither outweighed by other benefits nor reasonably avoidable.

The FTC Act prohibits unfair and deceptive advertising in any medium, including direct marketing solicitations. For more information on the FTC's standards for determining unfair and deceptive practices, see Practice Note, FTC Policy Statements on the Scope of Unfair and Deceptive Practices Overview.

An advertisement must be truthful 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 all reasonable consumer interpretations of their advertising for their products and services, and the FTC applies a "net impression" standard. For more information on advertising claims, see Practice Note, Advertising Claim Fundamentals.

In addition, advertising claims must be substantiated. Appropriate substantiation varies depending on the claims being made, the product being advertised, and the evidence that experts believe is 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 advertisement specifies a certain level of support for a claim, 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. For more information on substantiating advertising claims, see Practice Note, Substantiation of Advertising Claims.

All of the states have unfair and deceptive trade acts and practices (UDAP) laws prohibiting misrepresentation, deception, and unfairness in advertising. Sometimes referred to as "Little FTC Acts," the state UDAP laws vary in the degree that they follow the FTC Act and its interpretations, with some states giving it great weight and others simply being guided by it. Direct marketing campaigns must also comply with these state laws, some of which allow for a private right of action by consumers. For information on these state laws, see Practice Note, Key Elements of State Unfair and Deceptive Practices (UDAP) Acts.

Automatic Renewal and Negative Option Laws

Negative option contracts contain a term or condition that allows the seller to interpret a customer's failure to act, or silence, as acceptance of an offer. Negative options come in many forms, but automatic renewal plans in particular have caught the attention of state regulators. Several federal statutes and regulations and an increasing number of state laws specifically address negative option contracts and automatic renewals. These laws and regulations to varying extents impose disclosure, consumer consent, and cancellation requirements on businesses offering negative option programs. For detailed information on the

regulation of automatic renewal and other negative option programs, see Practice Notes:

- Automatic Renewal State Laws Charts: Overview.
- Automatic Renewal State Laws.
- Negative Option Offers: Positive Practices to Keep Them Compliant.

Federal Data Privacy Laws

Although the US does not have a national comprehensive privacy law, some targeted federal legislation related to data protection could impact direct marketers, including:

- The Drivers Privacy Protection Act (see Drivers Privacy Protection Act).
- The Children's Online Privacy Protection Act (see Children's Online Privacy Protection Act).
- The Gramm-Leach-Bliley Act (see Gramm-Leach-Bliley Act).
- The Fair Credit Reporting Act (see Fair Credit Reporting Act).

Drivers Privacy Protection Act

The Drivers Privacy Protection Act (DPPA) restricts the sale or release of a driver's personal information (18 U.S.C. § 2721). It allows state Departments of Motor Vehicles (DMV) to distribute personal information only to law enforcement officials, courts, government agencies, private investigators, insurance underwriters, and similar businesses. The DPPA generally prevents these agencies from distributing information for direct marketing and other uses. States have passed various other laws restricting use of DMV data and documents, including drivers' licenses.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) authorizes the FTC to prescribe rules governing the online collection of information from children under 13 (15 U.S.C. § 6501), which it has done in the form of the COPPA Rule. 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, may not collect personal information from a child in a manner that violates the COPPA Rule. The operator must post a notice detailing what information is collected from children, how the operator uses the information, and the operator's disclosure practices for the information. The operator must generally obtain verifiable parental consent for the collection, use, or disclosure of personal information from children, subject to certain exceptions. The COPPA Rule establishes the requirements for appropriate parental consent and any exceptions to it.

For more on COPPA, see Practice Note, Online Advertising and Marketing: Children's Online Privacy Protection Act.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) regulates the collection, use, and disclosure of non-public personal information by "financial institutions" (15 U.S.C. § 6801). If a direct marketer falls within the GLBA's definition of a financial institution, the GLBA would require it to provide a clear and conspicuous written privacy notice describing its privacy practices to its customers at the time the customer relationship is established and thereafter through an annual notice.

Customers may opt out of non-affiliate sharing of non-public personal information for marketing and the institutions may not share account numbers with non-affiliated telemarketers and direct marketers. However, the GLBA 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 the financial institution's products or services.

The FTC, the Consumer Financial Protection Bureau (CFPB), other federal regulatory authorities, and state insurance authorities enforce the GLBA and, in most cases, their own regulations promulgated under it, with respect to financial institutions over which they have jurisdiction. However, the FTC would have enforcement authority over a direct marketer subject to the GLBA, and may seek injunctive and ancillary equitable relief. The FTC also has authority under Section 5 of the FTC Act to examine privacy policies and practices for deception and unfairness related to the financial institutions' notices and practices.

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, may apply to direct marketers as users of consumer reports (Pub. L. 108-159, 117 Stat. 1952). The FCRA provides consumers, companies, consumer reporting agencies, and regulators with important tools that:

- Enhance the accuracy of consumers' financial information.
- Help fight identity theft.
- Regulate the creation, use, and disposal of consumer reports.
- Outline consumer disclosure requirements.

As a user of credit reports and potentially other types of consumer reports, a direct marketer has certain legal obligations under the FCRA. At a high level, its material obligations are:

- To use consumer reports only for identified, statutorily-permitted uses (such as credit evaluation or employment screening) and no other.
- To provide a notice containing statutorily-prescribed information to an individual if the direct marketer takes an "adverse action" against the individual based in whole or in part on the contents of a consumer report.
- In the event that the direct marketer is obtaining an "investigative consumer report," to provide a written disclosure to the subject of the report that an investigative consumer report may be obtained, which disclosure is delivered within three days of the date the report was first requested (an "investigative consumer report" is defined to mean a consumer report in which information is obtained through personal interviews with neighbors, friends, or associates of the consumer).

The FTC and the CFPB are the two federal agencies charged with overseeing and enforcing the provisions of the FCRA, though the CFPB typically is much more active in enforcing the FCRA. Many states, like California, also have their own laws relating to credit reporting that can be more restrictive with fewer exceptions than the FCRA.

State Data Privacy and Protection Laws

Several states have enacted data privacy laws which affect how direct marketers can collect, use, and share personal information of consumers. All states and territories have laws requiring reasonable security of personal data, provide for data subject notice, often require regulatory notice, and the potential for penalties, in the event of a security compromise.

California Consumer Privacy Act

California became the first US state with a comprehensive consumer privacy law when it enacted the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199).

The CCPA provides extra protections for the personal information of California residents. It defines personal information broadly and includes any information that either directly or indirectly:

- Identifies, relates to, or describes a particular consumer or household.
- Is reasonably capable of being associated with or could reasonably be linked to a particular consumer or household.

(Cal. Civ. Code § 1798.140(v)(1).) This definition of consumer personal information is expansive and includes unique identifiers like IP addresses and mobile ad IDs.

The CCPA grants California residents several rights, including:

- **General notice rights.** California consumers have the right to know what personal information a business collects, sells, or discloses about them, including the categories of third parties who purchased or received their data, both at or before collection and in a comprehensive, enterprise-wide annual notice.
- **Specific information rights.** This access right gives residents the right to know the individualized personal information that a business has collected, sold, or disclosed about them.
- **Data portability rights.** This access right gives residents the right to obtain a copy of individualized personal information a business has collected about them.
- **Deletion rights.** Subject to some exceptions, residents have the right to request that a business and its service providers delete their personal information.
- **Personal information sale prevention rights.** California consumers at least 16 years old have the right to opt-out of the sale of their personal information by a business. Personal information of California consumers under 16 years old may not be sold unless the child, or in the case of children under 13 years old their parent, has expressly opted-in to the sale of their personal information by a business. The definition of sale is very broad and encompasses sharing or transferring personal information in exchange for any valuable consideration (not just money).
- **Right of freedom from discrimination.** Residents have the right to equal service, meaning that businesses are prohibited from discriminating against residents who exercise their rights under the CCPA, such as giving them lower quality goods or services, unless the value of the incentive can be shown to be a fair measure of the value of the applicable data.
- **Protections against waivers of rights.** The CCPA expressly prohibits any agreement or contract provision that aims to waive or limit a resident's rights under the CCPA.

California subsequently passed the California Privacy Rights Act (CPRA) which amended the CCPA and went into effect on January 1, 2023. Many of the CCPA obligations and restrictions remain in place under the CPRA's amendments. The CPRA amendments, however, provide some additional consumer rights, including the rights to:

- Correct inaccurate personal information held by the business about the consumer.
- Opt-out of the sharing of personal information to third parties for cross-context behavioral advertising.
- Limit the use and sharing of their sensitive personal information.

It also provides for regulation (to come) of automated decision making and data retention and minimization requirements. The first, partial set of regulations became effective on March 29, 2023. Under the CPRA amendments, human resources and business-to-business data subjects are considered consumers and have the same sets of rights as traditional consumers.

California has been very active in bringing enforcement actions, including seeking civil penalties. For more information on California's privacy laws, see Practice Notes, California Privacy and Data Security Law: Overview and Online Advertising and Marketing: California Law.

Other State Consumer Privacy Laws

Other states have recently enacted CCPA-inspired privacy laws that impact direct marketing, including:

- **The Virginia Consumer Data Protection Act.** Virginia's consumer privacy act gives Virginia residents the rights to know, correct, delete, and opt out of the sale of their personal data, targeted advertising, and certain profiling. Like the CPRA, it went into effect on January 1, 2023.
- **The Colorado Privacy Act (CPA).** Signed into law on July 7, 2021, this consumer privacy legislation gives Colorado residents, among other things, the right to opt out of having their personal data sold or processed for targeted advertising or profiling. Companies that are subject to the CPA need to comply beginning July 1, 2023. In March 2023, Colorado finalized regulations that provider greater detail on rights and obligations.
- **Connecticut and Utah.** These two states have also recently passed consumer privacy laws that go into effect on July 1, 2023 and December 31, 2023, respectively.
- **Iowa.** Iowa passed a law in March of 2023, effective January 1, 2025, that is most similar to the Utah law.
- **Florida, Montana, Tennessee, and Indiana.** These four states passed consumer privacy laws in the spring of 2023. These laws go into effect in 2024, 2024, 2025, and 2026, respectively.
- **The Nevada Sale Law.** This narrower law gives Nevada residents the right to opt out of the sale of their covered information and was expanded in 2021.

For more information on state privacy laws that affect the collection, sharing, and use of personal information in the context of advertising and marketing, see Practice Note, Online Advertising and Marketing: State Privacy Laws.

State Data Security and Breach Laws

All 50 states, plus the District of Columbia and US territories have laws that require reasonable security of personal information and notifications to impacted individuals. With respect to state data security and breach laws, personal information is defined by statute and varies by state. Some states and territories require notification to the appropriate regulator, often in a set number of days.

Typically, organizations must comply with the law of the state where the impacted individual resides. Violations of these laws are enforceable by the state regulator, but many of these laws include private rights of action, meaning that impacted individuals, including in a class-wide basis, may be able to sue the breaching organization and seek statutory damages and other relief. Even when the state law does not contain an express private right of action, plaintiffs have alleged that violations of data security and breach laws is an unfair or deceptive trade practice and may attempt to bring the claim under the applicable UDAP laws (see FTC Act and State UDAP Laws). For more information on state data breach laws, see Practice Notes, US Privacy and Data Security Law: Overview and State Data Security Laws: Overview.

Cross-Border Communications

Effective enforcement of the rules governing unsolicited commercial communication is particularly difficult for messages originating in foreign countries. These actions present choice-of-law and other jurisdictional issues. The Undertaking Spam, Spyware, and Fraud with Enforcers Beyond Borders Act of 2006 (US SAFE WEB) was enacted to address cross-border issues involving spam (Pub. L. No. 109-455).

Jurisdictional Issues

If a foreign company is found to have sufficient contacts with the US, a court may find jurisdiction over that company in the US and apply US law to the dispute.

A US citizen may seek redress in US courts against a foreign company that targeted the individual in breach of US laws against unsolicited communications. The individual is generally required to serve process on the foreign company and to demonstrate that the company

has sufficient contacts with the US so that fundamental notions of fairness are not offended by forcing the company to defend against an action in the US. Some federal and state court decisions involving lawsuits by residents of one state against direct marketers in distant states have found that local residents can sue in their home jurisdiction when the marketers make concerted efforts to contact residents of those states. Even so, extending this principle to foreign direct marketing presents complex issues because of difficulties in obtaining jurisdiction over foreign companies.

Because the US does not have a national data protection regulation like the European Union (EU), it has had to work out mechanisms with the EU for cross-border data transfers to the US. Until July 16, 2020, the EU-US Privacy Shield Framework allowed participating organizations to transfer personal data from the EU to the US under the EU's General Data Protection Regulation. However, the European Court of Justice invalidated the Privacy Shield as inadequately protecting EU data subjects' rights (in a case commonly referred to as the Schrems II decision). Despite the court's decision, organizations must continue to meet their publicly stated Privacy Shield obligations for previously transferred EU personal data unless and until they formally withdraw from the framework.

The Schrems II decision did not invalidate other EU cross-border data transfer mechanisms, like model contractual clauses known as Standard Contractual Clauses (SCCs). In 2021, the European Commission adopted new SCCs for personal data transfers from the EU to the US (and similarly-situated countries). The UK has done so as well pursuant to their post-Brexit version of GDPR. For more on the court's decision, see Legal Update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ). For more information on the new SCCs, see Legal Update, European Commission adopts final versions of standard contractual clauses under EU GDPR.

In October 2022, President Biden issued an Executive Order to help pave the way for a new mechanism to transfer personal data subject to EU data protection law from the EU to the US. It is unclear when the new mechanism will be available for US businesses to use.

The FTC continues to fight cross-border fraud and deception through its enforcement and policy-making initiatives. Examples of cross-border cases filed by the FTC include one involving worthless medical discount packages peddled by Canadian telemarketers to elderly consumers throughout the US and another relating to phony international drivers' licenses advertised through spam email by defendants in the Bahamas, Israel, and Romania.

US SAFE WEB

US SAFE WEB bolsters the 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:

- Providing additional resources for the FTC and the DOJ to cooperate in foreign litigation.
- Confirming the FTC's remedial authority to redress harm, including restitution to domestic or foreign victims.
- Authorizing the FTC to make criminal referrals for prosecution when FTC rule violations also violate US criminal laws.
- Authorizing the FTC to cooperate with foreign law enforcers in investigating cases and sharing information.
- Protecting certain entities from liability for reporting suspected fraud or deception.
- Granting additional enforcement power to the FTC in cross-border cases.

Self-Regulation and Codes of Practice

Various voluntary regulations and codes of practice provide guidance for direct marketers. Although they do not have legal force to direct marketing activities, a self-regulatory body may refer cases to state and federal agencies. Direct marketing is self-regulated through a number of organizations, including:

- BBB National Programs, Inc. (BBBNP) (see BBBNP).
- The Association of National Advertisers (ANA) (see ANA).
- The Mobile Marketing Association (MMA) (see MMA).
- The Credit Bureaus (see Credit Bureaus).
- The Messaging Malware Mobile Anti-Abuse Working Group (MAAWG) (see MAAWG).

Besides their individual efforts, some of these organizations have collaborated to implement a broad industry self-regulatory program to protect consumer privacy.

For self-regulatory programs and codes related to online behavioral advertising, such as those offered by the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA), see Practice Notes, Online Advertising and Marketing: Voluntary Regulations and Codes of Practice and Advertising Self-Regulation in the US: Overview: Online Advertising.

BBBNP

BBBNP administers several important advertising self-regulatory programs, including:

- The National Advertising Division (NAD). Resolves challenges regarding truth and accuracy in national advertising.
- The Children's Advertising Review Unit (CARU). Enforces its guidelines on advertising to children and children's online privacy protection.
- The National Advertising Review Board. The appellate body for NAD and CARU decisions.
- The Direct Selling Self-Regulatory Council.
- The Digital Advertising Accountability Program. Enforces the DAA's self-regulatory OBA principles.

BBBNP establishes the policies and procedures for the programs it administers. Each program has guidelines that advertisers must comply with, and BBBNP monitors and enforces them. Each program adjudicates claims between advertisers, those initiated by consumers, or those resulting from its own monitoring. Where companies refuse to comply with a ruling, the program may refer the matter to the FTC for investigation of potential breach of section 5 of the FTC Act, or of other laws. For more information on the programs administered by BBBNP, see Practice Note, Advertising Self-Regulation in the US.

ANA

When the ANA acquired the Data & Marketing Association (DMA) in 2018, it became the keeper of the DMA's programs, guidelines, and responsibilities related to data-driven direct marketing. It adopted and enforces the Guidelines for Ethical Business Practice applicable to all direct marketers and originally developed by the DMA. These guidelines are intended to provide individuals and organizations involved in direct marketing with generally accepted principles of conduct. For more information on the Guidelines for Ethical Business Practice and the ANA's self-regulatory role, see Practice Note, Advertising Self-Regulation in the US: The ANA's Self-Regulatory Role.

The ANA maintains various consumer education programs and services originally created under the DMA and are free services for consumers who do not want to receive unsolicited communications, including:

- The DMAchoice mail preference service.
- The Telephone Preference Service (TPS).
- The Email Preference Service (eMPS).

DMAchoice, a program that grew out of DMA's Mail Preference Service, helps consumers decrease the amount of promotional mail they receive at home. A person may register with DMAchoice's name-removal file online or by mail. The individual's name and address are placed in a delete file which is made available to participating companies on a quarterly basis, with additions updated monthly. The DMAchoice mail service currently divides direct mail into four categories:

- Credit offers.
- Catalogs.
- Magazine offers.
- Other mail offers (including nonprofit mailings).

Consumers can request removal from any or all of the categories. Once registered, consumers remain on file for ten years. Registration does not stop mailings from organizations that do not subscribe to the DMAchoice mail service list.

The TPS was designed to help consumers decrease the number of commercial calls they receive at home. However, since November 2006, most registrations for TPS have been discontinued, directing consumers to the FTC's National DNC Registry instead (see National DNC Registry). TPS continues to accept and include current consumer registrations for the states of Pennsylvania and Wyoming, which are the only two states where companies must subscribe to the TPS file to remain in compliance with state-mandated do-not-call requirements.

The eMPS helps consumers decrease the amount of unsolicited commercial email they receive. To stop receiving this type of email, consumers can register their email addresses on an opt-out list. The list is updated daily and registration is effective for six years. Although registration with eMPS helps reduce the number of emails a consumer receives, it does not stop all commercial email. A consumer may continue to receive email from groups or advertisers who do not use eMPS to clean their lists and business-to-business email received at an individual's place of employment.

MMA

The MMA is a non-profit global trade association established "to accelerate the transformation and innovation of marketing through mobile, driving business growth with closer and stronger consumer engagement." It has more than 800 member companies. The last version of its U.S. Consumer Best Practices for Messaging (Version 7.0) dates back to 2012 and is still available on its website. Though no longer updated, it remains a useful guide.

The MMA now directs its members to another industry group, the International Association for the Wireless Communications Industry (CTIA), for guidance. The CTIA publishes Messaging Principles and Best Practices, last updated in 2019. The CTIA represents wireless carriers, and failure to follow its best practices can lead to termination of short codes by carriers.

Credit Bureaus

The credit bureaus offer a toll-free number (1-888-5-OPTOUT) and a website (optoutprescreen.com) that enables a consumer to opt-out of receiving pre-approved credit and insurance offers for five years or permanently. In addition, a consumer can contact the three major credit bureaus to stop personal information from being shared for promotional purposes:

- Equifax.
- Experian.
- TransUnion.

MAAWG

The MAAWG is a global organization that brings the industry together to deal with issues related to internet abuse, such as botnets, malware, spam, viruses, and denial-of-service attacks. MAAWG focuses on operational practices to fight internet abuse in three primary areas:

- Industry collaboration.
- Technology.
- Public policy.

MAAWG works with ISPs, telecom companies, email service providers (ESPs), social networking companies, leading hardware and software vendors, and major antivirus and security vendors to develop industry best practices, guidelines, and standards.

Consumer Recourse and Regulatory Enforcement

Consumers have various options for lodging complaints against a business for non-compliant direct marketing campaigns. Consumers often first complain directly to the business. In enforcement actions, many regulators do look to see whether the business has resolved the consumer complaints that it has received directly from the consumer. As to external organizations, consumers often lodge complaints with local Better Business Bureaus, state and local consumer protection agencies, and the FTC. The organizations routinely share consumer complaints with one another. Direct marketing campaigns may also be subject to regulatory enforcement and private actions that often are brought on a class-wide basis. Businesses may face significant penalties for conducting a direct marketing campaign that does not comply with the law.

Consumer Complaints

Many procedures exist for filing consumer complaints against unsolicited communications. The FTC provides various complaint forms for consumers. It maintains on its website forms concerning general complaints, violations of CAN-SPAM, and the National DNC Registry. Similarly, the FCC provides complaint forms for unsolicited fax advertisements and violations of its telemarketing rules.

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.

The FTC also is part of econsumer.gov, a multi-jurisdictional effort to gather and share cross-border e-commerce complaints. The econsumer.gov project has a multilingual public website and a government, password-protected website. The public site provides:

- General information about consumer protection in all countries that belong to the International Consumer Protection Enforcement Network (ICPEN).
- Contact information for consumer protection authorities in those countries.
- An online complaint form.

The ICPEN is made up of law enforcement authorities that regulate trade practices from more than three dozen countries, most of which are members of the Organization for Economic Cooperation and Development. Using the

existing Consumer Sentinel network, incoming complaints can be shared with ICPEN.

Regulatory Enforcement and Private Rights of Action

The primary federal laws that regulate direct marketing impose significant penalties for violations and in some cases also permit private actions.

FTC Act and State UDAP Laws

The FTC is empowered to seek injunctive relief through administrative actions or through actions in federal district court against advertisers who make unfair or deceptive claims. Under certain circumstances the FTC may also seek equitable monetary relief (like disgorgement and restitution) and civil penalties. The maximum civil penalty amount per violation of Sections 5(l), 5(m)(1)(A), and 5(m)(1)(B) of the FTC Act is currently $50,120 (it gets adjusted for inflation every January). Each act that violates the FTC Act is a separate violation.

The FTC historically used Section 13 of the FTC Act (15 U.S.C. § 53(b)) to seek consumer redress, including disgorgement and restitution, in actions filed directly in federal district court. However, in 2021, the Supreme Court held that the FTC cannot obtain equitable monetary relief when it files an action in federal district court under Section 13(b) of the FTC Act (*AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (2021)).

Now the FTC must use other avenues to seek monetary relief (either consumer redress or civil penalties, or both), including:

- Its rulemaking authority under Section 18 of the FTC Act (15 U.S.C. § 57a) (Magnuson-Moss), which authorizes the FTC to issue rules for unfair or deceptive acts or practices affecting commerce. These trade regulation rules are promulgated after the FTC engages in a rulemaking proceeding regulated by statute. Violators of these rules may be liable for civil penalties (15 U.S.C. § 45(m)(1)(A)).
- Section 19 of the FTC Act, which allows the FTC to seek consumer redress, civil penalties, or both in federal court (15 U.S.C. § 57b) for:
  - knowingly dishonest or fraudulent conduct after completing administrative litigation which ended with a cease-and-desist order (after the issuance of a cease-and-desist order and judicial review is completed, consumer redress for the conduct underlying the order may be sought); or
  - an FTC rule violation (consumer redress and civil penalties may be sought).
- Section 5(a)(1) of the FTC Act, which allows the FTC to seek civil penalties for knowing violations of the standards articulated by the FTC (meaning that the FTC has completed an administrative adjudication and determined that a practice is unfair or deceptive and issued a final cease and desist order) (15 U.S.C. § 45(m)(1)(B)). Recently, the FTC sent businesses "Notice of Penalty Offenses" letters which alleged that certain practices may violate FTC administrative cases. These letters arguably give the recipients actual knowledge that the described practices violate FTC standards allowing the FTC to seek civil penalties for future violations.

Under the FTC Act, false advertising violations that constitute misdemeanors may be penalized by a maximum fine of $5,000 ($10,000 after a first conviction) or by imprisonment for up to six months, or both (15 U.S.C. § 54). However, criminal charges are rare and must be brought by the Department of Justice, not the FTC. For more detailed information on remedies the FTC can pursue under Section 5 of the FTC Act, see Practice Note, FTC Enforcement of Advertising Claims: Penalties.

Consumers do not have a private right of action under the FTC Act. However, state UDAP laws usually provide consumers with a private right of action. State attorneys general can also file lawsuits on behalf of consumers under these state laws to seek injunctive relief, restitution for harmed consumers, and disgorgement of unlawfully acquired profits, depending on the scope of the law. Further, state and sometimes local enforcement agencies may recover steep civil penalties which range from a few hundred dollars to tens of thousands of dollars per violation (which often means per act that violates the law) of the UDAP law.

CAN-SPAM

Each violation of CAN-SPAM is subject to civil penalties of up to $50,120 per violation. The DOJ may also seek criminal penalties, including imprisonment, for marketers who do or conspire to:

- Use another's computer without authorization and send commercial email from or through it.
- Use a computer to relay or retransmit multiple email messages to deceive or mislead recipients or an internet access service about the origin of the message.
- Falsify header information in multiple email messages and initiate the transmission of those messages.

- Register for multiple email accounts or domain names using false identity information.
- Falsely represent themselves as owners of multiple internet protocol addresses that are used to send commercial email messages.

There is no private right of action under CAN-SPAM other than for internet service providers. State attorneys general may enforce CAN-SPAM, but state laws that regulate the sending of emails are preempted by CAN-SPAM except in so far as they regulate falsity or deception. In addition, deceptive commercial email is also subject to sanctions under federal and state laws banning false or misleading advertising generally.

TSR and TCPA

The FTC may directly bring a federal court action for injunctive relief and civil penalties for a breach of the TSR. State attorneys general may also bring actions for violations of the TSR on behalf of their residents. Violators of the TSR are subject to civil penalties of up to $50,120 per breach. In addition, the TSR provides for private rights of action for a consumer. Under the TSR, a private citizen may bring an action if they have suffered $50,000 or more in actual damages.

The TCPA also creates a private right of action for monetary damages and injunctive relief, but does not have a damages threshold for private citizens. It allows a plaintiff to recover the greater of $500 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 (the TSR does not). In *Mims v. Arrow Financial Services, LLC*, the Supreme Court held that state and federal courts have concurrent jurisdiction over private actions brought under the TCPA (565 U.S. 368 (2012)).

The FCC enforces the TCPA by bringing administrative proceedings. The TCPA also provides for state attorneys general to bring actions on behalf of their residents against persons violating the law. For more information on penalties under the TCPA, see Practice Note, TCPA Litigation: Key Issues and Considerations: Enforcement.

DMPEA

Direct mail solicitations that are not in compliance with the DMPEA are deemed non-mailable matter and are subject to mail detention and prosecution by the US Postal Service. Civil penalties can be imposed up to $10,000 per violation of sending non-mailable matter and up to $2 million per violation for sharing for commercial use the names and addresses of people who have opted out of receiving future mailings (39 U.S.C. § 3017 (g-h)). The DMPEA authorizes the postal service to impose stop-mail orders and monetary penalties of:

- Up to $25,000 for each mailing up to 50,000 pieces.
- $50,000 for each mailing from 50,000 to 100,000 pieces.
- An additional $5,000 for each additional 10,000 pieces above 100,000, not to exceed $1 million.

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

COPPA

The FTC has civil penalty authority under COPPA and aggressively enforces the law, regularly seeking millions of dollars in penalties for even unintentional violations of the COPPA Rule. State attorneys general can also enforce COPPA, but there is no private right of action.

Direct Marketing Campaign Best Practices

Considering the patchwork of regulations, it can be a challenge to weigh the multitude of legal risks against the manner in which a business wants to run a direct marketing campaign. Some best practices can help balance these legal risks alongside the business decisions for creating and publishing direct marketing campaigns.

Assess Compliance and Gaps

- Conduct a readiness assessment and gap analysis based on existing compliance materials and current direct marketing practices (by medium) and then develop a detailed work plan listing all required and optional tasks to allocate roles and responsibilities.
- During this phase, it is critical to work alongside company marketers while agreements and marketing and e-commerce user experiences are being tested and designed so legal can identify compliance gaps before final design decisions are made. Marketers favor the user experience that generates the most growth, but that often does not align with an opt-in consent framework. For example, marketers lean toward pre-selected consent boxes to streamline the user experience. However, if legal works alongside marketers during the test and design phase, there is a higher likelihood

the legal risk associated with pre-selected boxes can be weighed to persuade the marketers to use more compliant design changes. It is extremely difficult to change designs once they have been implemented, especially if the current design drives revenue growth.

Create or Update Data Inventories or Maps and Develop and Deploy Data Management Capabilities

- Update or develop data maps to identify how categories of personal data are collected, used, transferred, or disclosed, and for what purpose.
- Update data maps to account for direct marketing uses, like consent management practices.
- Make sure to determine the reasonably necessary retention periods alongside internal record keeping policies so necessary records (like opt-out records and do-not-call lists) are not destroyed before the relevant record keeping deadline.

Update or Implement a Vendor and Data Recipient Management Program

- Review and, as necessary, amend or execute contracts to ensure compliance with consumer protection, marketing, and privacy laws to allocate risk, especially if a direct marketing program relies on third parties (like current customers and influencers) to deliver marketing messages (like calls and "send-to-friend" tools).
- Keep in mind that companies can be vicariously liable for third-party marketers' conduct, and it is often a hotly litigated and fact-intensive undertaking.

Shore-Up Data Security and Breach Preparedness

- Assess security posture and remediate vulnerabilities.
- Review and update a written information security program plan, including an incident response plan, an acceptable use policy, cookie and consent management, and a vendor security program.

Audit and Train

- Establish an internal audit program to continually test and evaluate direct marketing practices, like consent management and record retention.
- Train stakeholders on compliance basics and the importance of working with legal during the planning stage of campaigns.