THOMSON REUTERS
PRACTICAL LAW™

Direct Marketing

by Practical Law Commercial Transactions, with Alan L. Friel, Baker & Hostetler LLP

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

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

This Note considers the statutes, regulations, and voluntary codes of practice that apply to direct marketing activities, including marketing by telephone, fax, mail, email, and text message.

Direct marketing consists of communications (often, but not always, unsolicited) by which the sender tries to sell or market certain goods or services directly to consumers, without the use of traditional forms of advertising (such as radio, newspapers, and television). For a discussion of issues that apply to advertising generally, see Practice Note, Advertising: Overview.

Direct marketing communications are sent by mail, telephone, text message, fax, and email. Direct marketing is a powerful business tool, but if used in an irresponsible way, it can cause substantial nuisance, cost, and inconvenience to recipients and internet service providers (ISPs), whose networks can be slowed down considerably by unsolicited email. Direct marketing activities involve complicated legal issues arising from several statutes, regulations, and voluntary codes of conduct, the various provisions of which are not always consistent.

This Note focuses on the legal issues relevant to direct marketing activities and considers, in particular:

- The regulation of unsolicited commercial communications by telephone, fax, mail, email, and text message.
- Sanctions that exist for breaches of legislation on unsolicited marketing communications.
- Additional federal rules that may apply to direct marketing campaigns.
- Policies on cross-border communications.
- The application of self-regulation and codes of practice.
- Filing consumer complaints.

Regulation of Unsolicited Commercial Communications

Nearly all 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, mail, email, and text message.

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 (see Do-Not-Call 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.

(15 U.S.C. § 6101.)

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. 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. The TSR:

- Prohibits deceptive and abusive telemarketing acts or practices.
- Establishes a national do-not-call registry maintained by the FTC (see Do-Not-Call Registry).
- Establishes an allowable calling time from 8:00 a.m. to 9:00 p.m.
- Restricts unauthorized billing.
- Requires telemarketers to transmit caller identification information and imposes disclosure and consent requirements related to telemarketing transactions.

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.

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

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. 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 do-not-call registry requirements (see Do-Not-Call Registry), but the companies must keep their own do-not-call lists and honor requests not to be called.

Telephone Consumer Protection Act

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. The TSR only applies to telemarketing 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.
- 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).

In 2020, the Supreme Court ruled that the debt-collection exception to the TCPA's robocall restrictions, introduced in a 2015 amendment, 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 Federal Communications Commission (FCC) has authority to prescribe rules under the TCPA (FCC Rules), as well as to collect complaints and institute enforcement actions. Over the years, FCC Rules have provided guidance on the FCC's interpretation of the TCPA. For example, for detailed information on the 2013 rule amending prior FCC Rules, see Legal Update, New FCC Telemarketing Rule To Become Effective.

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. In June 2003, the FCC implemented the National Do-Not-Call Registry in coordination with the FTC (see Do-Not-Call Registry). The FCC also imposed limits on the number of abandoned calls that are permissible and specific restrictions on telephone solicitation, including restrictions on the use of unsolicited recorded messages to consumers without prior consent.

There have been several FCC rulings and much litigation over what type of equipment comprises an ATDS. In *ACA Int'l 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)). The Circuit Courts are now split over the definition in the absence of the FCC guidance. The FCC has indicated its intent to issue revised guidance on the definition, but until then, the definition remains unclear.

The FCC has since 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 new rulemaking. For more information on the uncertainty surrounding the ATDS definition, see Practice Note, Telephone Consumer Protection Act (TCPA): Overview: Defining an ATDS and Legal Update, FCC Issues Declaratory TCPA Ruling: Certain P2P Text Messaging Platforms Are Not Autodialers.

The TCPA creates a private right of action for monetary ($500 for each violation or actual damages, whichever is greater) and injunctive relief where the Act is infringed and provides for treble damages to the private action plaintiff if the violation was willing or knowing. In *Mims v. Arrow Financial Services, LLC*, 132 S. Ct. 740, 181 L. Ed. 2d 881 (2012), the Supreme Court held that state and federal courts have concurrent jurisdiction over private actions brought under the TCPA.

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

Do-Not-Call Registry

The National Do-Not-Call Registry empowers consumers to stop calls from almost all companies within the FTC'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. The do-not-call registry does not cover calls:

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

Many states have enacted opt-out legislation for telephone marketing, instead requiring the creation of statewide do-not-call registries. The national registry does not pre-empt state do-not-call laws. In 2013, Congress tasked the FTC to work with those states that have enacted do-not-call registry laws, as well as with the FCC, 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 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.

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 (see 47 C.F.R. § 64.1200). Prior written consent is required except for where there is an existing business relationship. In this case, the Junk Fax Prevention Act of 2005 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 TCPA. The opt-out must be easy to find and free.

Under the FCC regulations, 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 held in *Bais Yaakov of Spring Valley v. FCC* that while the TCPA gives the FCC the authority to regulate unsolicited fax advertisement, the law does not:

- Require a similar opt-out notice on solicited fax advertisements (fax advertisements sent with the recipient's prior express invitation or permission).
- Grant the FCC authority to require opt-out notices on solicited fax advertisements.

(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.

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). 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. In addition, 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.

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)).

Direct mail solicitations involving sweepstakes or contests are also regulated by state laws. The application of these laws generally is considered in Practice Notes, Sales Promotions, Contests, and Sweepstakes and Running a Sweepstakes or Contest in the US.

Direct mail advertising, like all advertising, must be in compliance with the Federal Trade Commission Act, 15 U.S.C. § 41 (FTC Act). 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.
- 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 mail solicitations. An advertisement, whether through mail or otherwise, 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.

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.

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. 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.

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 and there is no business-to-business exception.

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 existing business relationship (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.

The law's main provisions include a:

- Ban on false or misleading header information (an email's routing information, including the originating domain name and email address).
- Prohibition on deceptive subject lines.
- Requirement that those who send commercial email must give recipients a free, easy-to-use opt-out method.
- Requirement that commercial email be identified as an advertisement and include the sender's valid physical postal address.
- Requirement that warning labels be added to commercial email that contains sexually oriented material.

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

CAN-SPAM authorizes the FTC to adopt and enforce rules regarding commercial email sent to computers, while the FCC is authorized to adopt and enforce rules regarding commercial email sent to wireless phones and mobile devices. The FCC's Rules and Regulations Implementing the Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003 and Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 (69 F.R. 55765) (Implementation Rules), clarify the applicability of CAN-SPAM to email and text messages sent to mobile domains.

According to the Implementation Rules, CAN-SPAM covers email sent to mobile handheld wireless devices (that is, to a mobile domain or email to text). To facilitate implementation of the Act's provisions for handheld devices, the FCC's rules establish a wireless domain registry and require that wireless service providers supply the FCC with wireless mail domain names. Any commercial message sent to an email address that is on the registry is prohibited unless the recipient provides express prior authorization. Even if authorization is provided, the sender must allow the recipient to opt out of receiving additional messages. Note that the FCC determined that forwarded email messages in general are not covered by CAN-SPAM, unless the sender of the

forwarded email message receives compensation or inducement.

In addition to the FTC's enforcement authority, the Department of Justice (DOJ) is authorized to enforce CAN-SPAM through its criminal sanctions (see Sanctions). The FTC also can exercise its authority under section 5(a) of the FTC Act to pursue issues related to deceptive commercial email. Section 5(a) prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC can initiate federal district court proceedings to enjoin violations of the Act and secure other equitable relief as appropriate (including disgorgement and redress).

CAN-SPAM pre-empts all state and local laws that directly regulate spam. However, it does not pre-empt state laws that deal with related issues, such as laws related to fraud, deception, or computer crime.

The FTC generally makes no distinction between unsolicited commercial email communications directed to individuals and unsolicited commercial email directed to companies.

For more information on the regulation of online advertising and marketing in the US, see Practice Note, Online Advertising and Marketing.

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 apply to texts. The FCC regulations implementing the TCPA prohibit the use of an ATDS to provide a message to any mobile telephone without the prior written consent of the subscriber.

Text messages may also be covered by CAN-SPAM which requires the FCC to issue rules related to mobile service commercial messages. The FCC's Implementation Rules address CAN-SPAM's applicability to text messaging and provide that the technology employed to send the message will determine whether it is covered by CAN-SPAM. If the text message is from internet-to-phone, which involves addresses that reference internet domains, then it is covered by CAN-SPAM. In contrast, if the text message does not involve addresses that reference the internet, as in phone-to-phone text messages, then CAN-SPAM does not apply.

Sanctions

Each violation of CAN-SPAM is subject to civil penalties of up to $43,280 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.

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 would have to be brought by the Department of Justice, not the FTC. More typically, the FTC may seek injunctive relief and civil penalties. For more information on additional remedies the FTC can pursue under Section 5 of the FTC Act, see Practice Note, FTC Enforcement of Advertising Claims: Penalties.

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 $43,280 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 $50,000 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 $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, but the TSR does not. 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.

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)).

Additional Federal and State Laws

Besides the specific statutes and regulations enacted to deal with direct marketing campaigns, there is some targeted legislation related to data protection that could impact direct marketers. This legislation includes:

- 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 and Accurate Credit Transaction Act (see Fair and Accurate Credit Transactions Act).
- The California Consumer Privacy Act of 2018 (see California Consumer Privacy Act).

Drivers Privacy Protection Act

The Drivers Privacy Protection Act 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 Act 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 or other acceptable 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.

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.

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). The GLBA requires financial institutions to disclose their privacy policies to their customers 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, other federal banking and financial services regulatory authorities, and state insurance authorities enforce the GLBA and, in most cases, their own regulations promulgated under it. The FTC may bring enforcement actions for violations of the GLBA for the types of financial institutions where jurisdiction was not

provided to an alternative agency, 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 and Accurate Credit Transactions Act

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

- Expand access to credit and other financial services.
- Enhance the accuracy of consumers' financial information.
- Help fight identity theft.

For example, the Act requires that account numbers on credit card receipts be shortened or truncated so that merchants, employees, and others who may have access to the receipts do not have access to consumers' names and full credit card numbers. The FTC also enacted the Disposal Rule, which requires proper disposal of sensitive consumer report information.

The FTC and the Consumer Financial Protection Bureau (CFPB) are the two federal agencies charged with overseeing and enforcing the provisions of the act. Many states also have their own laws relating to credit reporting.

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). In order to give businesses time to adjust their practices to comply with the law, the law went into effect on January 1, 2020 and California did not begin to enforce it until July 1, 2020.

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(o)(1).) This definition of consumer personal information is far more expansive than has been typical under US laws 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.
- **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.

For more information on the CCPA, see Practice Note, Understanding the California Consumer Privacy Act (CCPA).

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 EU law, initially under the EU Data Protection Directive and now 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. Although the decision did not invalidate other EU cross-border data transfer mechanisms, like model contractual clauses, the court's reasoning arguably applies there too. It remains to be seen how the US and EU governments solve for this problem. 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).

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

Voluntary regulations and codes of practice provide guidance for direct marketers, although they do not have legal force to direct marketing activities. Direct marketing is self-regulated through a number of organizations, including:

- The Advertising Self-Regulatory Council (ASRC) (see ASRC).
- The Data & Marketing Association (see Data & Marketing Association).
- The Mobile Marketing Association (see Mobile Marketing Association).
- The Network Advertising Initiative (see Network Advertising Initiative).
- Digital Advertising Alliance (see Digital Advertising Alliance).
- The Credit Bureaus (see Credit Bureaus).

- The Messaging Malware Mobile Anti-Abuse Working Group (see Messaging Malware Mobile Anti-Abuse Working Group).

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

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 in the programs it administers, including:

- The National Advertising Division.
- The Children's Advertising Review Unit.
- The National Advertising Review Board.
- The Online Interest-Based Advertising Accountability Program (Accountability Program).

The self-regulatory system is administered by the BBB National Programs, Inc. (BBBNP) (the national self-regulatory unit of the former Council of Better Business Bureaus) and governs national advertisers. Each ASRC program has guidelines that advertisers must comply with, and it monitors and enforces them. Each program adjudicates claims between advertisers and those initiated by consumers or as a result of its own monitoring. 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.

Data & Marketing Association

The Data & Marketing Association (DMA), now a division of Association of National Advertisers (ANA), is comprised of businesses and nonprofit organizations that use data-driven marketing. It represents brands, marketing executives, and practitioners in the US and abroad, across a variety of industries. Under the auspices of the ANA, the DMA advocates industry standards for responsible marketing and maintains Guidelines for Ethical Business Practice applicable to all direct marketers. The DMA also maintains various consumer education programs and services, including the DMAchoice mail preference service, Telephone Preference Service, and Email Preference Service, which are free services for consumers who do not want to receive unsolicited communications.

Guidelines for Ethical Business Practice

The DMA's comprehensive guidebook (now under the ANA name), Guidelines for Ethical Business Practice, is intended to provide individuals and organizations involved in direct marketing with generally accepted principles of conduct. ANA Member Principles (formerly the DMA principles) (ANA Principles) provide the underlying framework for the Guidelines for Ethical Business Practice. The ANA Principles apply to members' relationships with all types of current and prospective customers, donors, and fellow members. They declare to the public what can be expected when dealing with an ANA member and provide that an ANA member:

- Is committed to customer satisfaction good corporate citizenship, and responsible environmental, community, and financial stewardship.
- Clearly, honestly, and accurately represents its products, services, terms and conditions, and delivers its products and services as represented.
- Responds to inquiries and complaints in a constructive, timely manner and communicates in a respectful and courteous manner.
- Maintains appropriate security policies and practices to safeguard data.
- Provides information on its policies about the transfer of personal information for marketing purposes.
- Honors requests not to have personally identifiable information transferred for marketing purposes.
- Honors requests not to receive future solicitations from its organization.
- Follows the spirit and letter of the law, as well as ANA's Guidelines for Ethical Business Practice.

DMAchoice

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.

In addition, DMAchoice offers other similar services to consumers, including:

- **Telephone Preference Service.** The DMA designed its Telephone Preference Service (TPS) to help consumers decrease the number of commercial calls they receive at home. However, since November 2006, the DMA discontinued most registrations for TPS, directing consumers to the FTC's National Do-Not-Call Registry instead (see Do-Not-Call 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 DMA's TPS file to remain in compliance with state mandated do-not-call requirements.
- **Email Preference Service.** The DMA's Email Preference Service (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.

Mobile Marketing Association

The Mobile Marketing Association (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 MMA's 2008 Global Code of Conduct was "designed to provide guidelines that all Mobile Marketers should consider and build their mobile programs around." The Code sets out general guidelines as to Notice, Choice and Consent, Customization and Constraint, Security, and Enforcement and Accountability. However, the MMA has not kept its code of conduct up to date and 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.

Network Advertising Initiative

The Network Advertising Initiative (NAI) is an organization for third-party online advertising technology companies, including networks, exchanges, DMPs, SSPs, RTB platforms, analytics companies, and service providers that deliver interest-based and cross-application advertising and retargeting (Personalized Advertising). Members must pledge full compliance with the NAI Code of Conduct (the NAI Code). The NAI is a member of the Digital Advertising Alliance (DAA) (see Digital Advertising Alliance).

In addition to adhering to the DAA's self-regulatory principles, the NAI Code includes additional requirements for its members, such as:

- Notice requirements for the prospective merger of personal information with device-identifiable information to be used for Personalize Advertising.
- Data retention limits and disclosure obligations.
- Opt-in consent requirements for the use of sensitive health information for Personalized Advertising.

To support its consumer privacy principles, the NAI:

- Conducts annual compliance examinations of its members.
- Offers a consumer complaint process.
- Imposes sanctions such as suspension and revocation of NAI membership and refers non-compliance matters to the FTC's consumer protection division.
- Provides annual reports of the nature and number of consumer complaints received.

The NAI issued an updated NAI Code effective January 1, 2020. The new code makes several changes, including:

- Prohibiting behavioral targeting of children under 16 (raised from under 13) without verifiable parental consent.
- Requiring NAI members to obtain consumers' opt-in consent before collecting and targeting sensitive data, such as geolocation data and health information, for:
  - ad targeting;
  - ad delivery; and
  - ad reporting.

- Requiring NAI members to disclose the political audience targeting segments they use for digital advertising.

For more information on the 2020 NAI Code, see Legal Update, Network Advertising Initiative (NAI) Prohibits Behavioral Targeting of Users Under 16.

Digital Advertising Alliance

The DAA, a group led by leading advertising and marketing trade associations, establishes and enforces self-regulatory principles to protect consumer privacy in relation to online behavioral advertising (OBA) and multi-site data collection. It has released two sets of principles (Self-Regulatory Principles):

- Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles).
- Self-Regulatory Principles for Multi-Site Data. These principles cover the prospective collection of data across multiple sites for purposes other than OBA.

BBBNP and the DMA work cooperatively as the Accountability Program to promote, monitor, and enforce the OBA Principles. The OBA Principles are comprised of seven individual principles, specifically:

- **The Education Principle.** Organizations must educate consumers about OBA.
- **The Transparency Principle.** Consumers must have clear and easily accessible disclosures about data collection and use practices.
- **The Consumer Control Principle.** Consumers have the ability to choose whether their personal data is collected and used.
- **The Data Security Principle.** Organizations must provide reasonable security for, and limited retention of, data collected and used for OBA purposes.
- **The Material Changes Principle.** Organizations must obtain consumer consent for any material change to their data collection policies and practices.
- **The Sensitive Data Principle.** There must be heightened protections to data collected from children and to certain health and financial data.
- **The Accountability Principle.** Programs must be enacted to monitor and report non-compliance to appropriate government agencies.

The OBA Principles recommend the use of an AdChoices icon that advertisers can place on their behavioral ads or on web pages that collect data for their ads. The icon alerts consumers about what is being collected and eventually allows consumers to opt-out.

In October 2013 the Accountability Program issued a compliance warning to clarify the enhanced notice requirement set out in the OBA Principles, and to inform advertisers that it would begin enforcement of the requirement in January 2014. The OBA Principles require websites to provide a clear, meaningful, and prominent link on each web page where data is collected for OBA (the enhanced notice link). The enhanced notice link must:

- Link directly to the website's disclosure of its OBA practices, which must:
  - direct consumers to an industry-developed page, like the DAA's Consumer Choice page; or
  - provide an accurate, up-to-date, and comprehensive list of links to the choice mechanisms of all third parties engaged in OBA on the site.
- Be distinct from the website's privacy policy link.
- Provide a link to an easy-to-use mechanism allowing consumers to control their participation in OBA, either:
  - through an in-ad notice, like the AdChoices Icon; or
  - if there is not an ad on every web page, but a page still collects data, then the enhanced notice link should appear elsewhere on the page (for example in the website footer).

First-parties (for example, website operators) are responsible for providing enhanced notice:

- When a third party (for example, an ad network) does not provide enhanced notice or make arrangements with the first party to do so.
- If the first party sells or otherwise transfers data to unaffiliated third parties for the third-parties' use in OBA.

For more information on the compliance warning, see Legal Update, BBB Accountability Program Issues First Industry-Wide Compliance Warning.

The DAA has also published additional guidance that can be used along with its Self-Regulatory Principles, including:

- **Application of Self-Regulatory Principles to the Mobile Environment**. These guidelines explain how the existing Self-Regulatory Principles apply to certain types of mobile data and the mobile application environment.
- **Application of the DAA Principles of Transparency and Control to Data Used Across Devices**. These

guidelines explain how the existing Self-Regulatory Principles and their application to mobile devices apply to cross-app data collected from a particular browser or device for use on a different computer or device.

- **Application of the DAA Principles of Transparency & Accountability to Political Advertising**. These guidelines explain how the OBA Principles apply to paid-for express advocacy political advertising for federal and certain state-wide elections in both the desktop and mobile environment.

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. The four major consumer reporting agencies are:

- Equifax.
- Experian.
- TransUnion.
- Innovis Consumer Assistance.

Messaging Malware Mobile Anti-Abuse Working Group

The Messaging Malware Mobile Anti-Abuse Working Group (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, and 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 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 Do-Not-Call 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.