FDIC Insurance Notification
Federal Deposit Insurance Corporation (FDIC) regulations require that, when a bank advertises deposit accounts or products (which are insured by the FDIC) or the bank itself, the public must be made aware of FDIC insurance protection by including an official advertising statement. The advertising statement consists of the words “Member of the Federal Deposit Insurance Corporation,” “Member of FDIC,” or “Member FDIC.” FDIC regulations provide some exceptions to this requirement, such as when radio or television advertisements do not exceed 30 seconds in length.

Unfair, Deceptive, or Abusive Acts or Practices
Virtually all states have laws regulating deceptive trade practices, but the principal federal statute governing business marketing practices in the United States is the Federal Trade Commission (FTC) Act. Enacted in 1914 to regulate industrial policy and commercial trade practices, the law created the Federal Trade Commission, whose first enforcement efforts were directed to price-fixing, monopolies, and unfair practices in commercial competition. The FTC has since taken on consumer protection as well.

Although the FTC has authority strictly over nonbank businesses, the federal banking regulators and the CFPB have the authority to enforce the FTC Act, Section 5, which details the unfair, deceptive, and abusive practices that are forbidden in the financial industry.

Marketing departments should develop productive working relationships with the bank’s compliance department. A strong, respectful relationship between these two departments can assist marketing with proper disclosures and help ensure that messages are delivered in customer-friendly language.

Deceptive acts or practices are those that are likely to mislead the reasonable consumer and constitute a material practice, defined as follows:

- Likely to mislead. A representation, omission, act, or practice can mislead. Examples are false oral or written representations, misleading claims about costs, bait-and-switch tactics, and failure to provide the service or product.
- Reasonable customer. The act or practice would be deceptive to a person of average intelligence exercising an average amount of judgment. Omitting material information from an otherwise truthful advertisement could mislead a reasonable customer and thus be deceptive.
- Material practice. The misrepresentation, omission, act, or practice affects the customer’s choice or conduct, as when misleading information about costs leads the customer to decide to buy the product.

The FTC Act, Section 5, defines the elements of unfair acts or practices as those causing substantial injury or injuries that are not outweighed by the benefits and could not be reasonably avoided, defined as follows:

- Substantial injury. This occurs when a customer suffers, for example, monetary harm, such as paying an unnecessary fee or interest charge due to an unfair practice. The injury may be small but affect many people or be significant for a single customer. An example would be claiming there are no fees in the promotion and mentioning the fees only in the small print.
- Benefit less than the injury. For this element, the net effect of the practice is analyzed to see if the overall benefits are not greater than the harm caused by incomplete or misleading communications.
- Not a reasonably avoidable injury. The consumer could not avoid the injury. This can occur when information is withheld or distorted to impede the customer’s reasonable choice.
- The Dodd-Frank Wall Street Reform and Consumer Protection Act added “abusive” acts or practices to the scope of the FTC Act. An abusive act or practice is one that would meet one of these tests.
Bank Marketing Laws and Regulations

- Materially interferes with a consumer’s ability to understand the terms or conditions of a financial product or service
- Takes unreasonable advantage of the consumer’s lack of understanding of the material risks or costs of the product or service
- Takes unreasonable advantage of the consumer’s inability to protect his or her own interests when selecting or using a financial product or service

Do Not Call, Do Not Fax

Telemarketing involves using telephone lines (phone or fax) to promote products and services. Because customers are contacted in their own homes or offices, telemarketing raises questions about privacy, full disclosure, and whether there are places that marketers should be off-limits.


The FCC regulations give consumers options to avoid unwanted telephone solicitations. For example:

- No seller, or entity telemarketing on behalf of a seller, may initiate a telephone solicitation to residential telephone subscribers who have registered their number on the National Do Not Call Registry.
- Calls (other than pre-recorded calls) are permitted, however, to those with whom the seller has an established business relationship.
- Banks must maintain bank-specific do-not-call lists with the names of people with whom they have a business relationship who have asked to be excluded from telemarketing.
- Telemarketing calls may be made between 8:00 a.m. and 9:00 p.m. only.
- Telemarketers must comply with limits on abandoned calls.
- Consumer-friendly practices must be used when calls are made with automated telephone-dialing equipment.
- Prerecorded messages must identify the name and telephone number of the entity responsible for the call.
- Telemarketers must transmit caller ID information, when available, and refrain from blocking such transmissions to the consumer.
- The advertiser must first obtain the written permission and signature of the intended recipient before sending unsolicited advertising fax transmissions unless there is an established business relationship and the recipient has provided a fax number for such communications.

Prescreening

To make the best use of marketing expenditures, banks sometimes prescreen prospective customers. When undertaking a mass marketing effort, such as a direct mail campaign to offer credit cards, a bank may match its credit criteria against credit reporting agency data to create a list of prospective new accounts. Individuals whose credit scores meet or exceed the bank’s credit criteria are included in the mailing campaign.

When banks prescreen customers for marketing purposes, the Fair Credit Reporting Act (FCRA) contains several rules with which banks must comply. Banks that prescreen consumers must offer to extend credit to anyone who applies for it. If a consumer responds to a prescreened offer, the bank normally does a more in-depth credit analysis. Recipients of the advertising must be informed that they received the solicitation based on information in their credit reports and that they satisfied the bank’s criteria. Consumers must also be told that they may prohibit the use of information in their credit file in connection with future prescreened offers.
The FCRA also defines when banks can share third-party information (such as credit reports or transaction or experience information) with affiliates for marketing purposes. The requirements of the FCRA with regard to information sharing were subsequently amended and then changed again by the Fair and Accurate Credit Transactions (FACT) Act. As it now stands, before a bank can use certain information about a consumer received from an affiliate to solicit the consumer for marketing purposes, the customer must be given an opportunity to opt out.

Fair lending laws prohibit creditors from prescreening credit applicants on a prohibited basis—that is, based on the applicant’s race, sex, national origin, or other prohibited personal characteristic.

Privacy of Customer Information
Banking laws, such as the Gramm-Leach-Bliley Act (GLBA), require financial institutions to protect the privacy of personal customer information. The GLBA requires banks to tell customers whether they share customer information with third parties and to refrain from doing so if the customer objects. Banks have always made protecting customer account information a priority, but the GLBA privacy provisions offer additional assurance that the banking industry is committed to protecting private financial information.

E-Commerce and Social Media Guidance
Marketing laws and regulations have had to keep pace with the ever-changing ways that bank products are sold. In particular, the rise of e-commerce has created a vast new area of marketing mandates.

The FTC addressed the issue of online marketing as far back as 2000 when it published the .com Disclosures guide. The guidance said that the FTC’s consumer protection rules and regulations regarding unfair and deceptive advertising in traditional media (such as print media, radio, and television) apply to online advertising as well. For example, material information presented to consumers on websites cannot mislead, as discussed earlier in this section.

In 2013, the FTC updated its .com Disclosures guide to reflect the new digital technologies and practices that have been adopted since 2000. The FTC said that all advertisers must ensure that their ads comply with the agency’s broad principles, whether those ads appear on websites, social networks, mobile devices, tablets, or whatever devices might be invented in the future. Reflecting the unique nature of online advertising, the FTC’s guidance contains recommendations pertaining to hyperlinks, scrolling, click-through pages, and other attributes that do not apply to traditional media. Complying with the FTC’s marketing disclosure requirements is made especially difficult considering that the devices on which the disclosures must be made can be small, as is the case with smart phone screens.

Bank regulators, under the auspices of the FFIEC, also issued guidance that pertains to e-commerce and social media use by banks. The FFIEC’s guidance addresses the risks of social media use by banks to conduct their business, the purpose often being to market and sell to consumers. Social media refers to any online communication in which the bank interacts with the public, such as Facebook or Twitter. It also includes online forums, blogs, customer review websites, bulletin boards like Yelp, photos and video sites such as YouTube, and professional networking sites such as LinkedIn. The FFIEC notes that the consumer protection laws apply to all forms of consumer and customer communications, regardless of the medium.

CAN-SPAM Act
In addition to this recent guidance from the FTC and FFIEC, specific laws and regulations have been imposed to curtail opportunities for abusive marketing and sales practices through electronic channels. One of the most notable is the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, better known as the CAN-SPAM Act. The CAN-SPAM Act sets rules for commercial use of electronic mail.
Email solicitations are inexpensive, immediate, direct (reaching the recipient’s computer inbox in a matter of seconds), and actionable (inviting a reply with just a click of the mouse). Those benefits also invite abuse, which prompted passage of the CAN-SPAM Act. The law protects recipients who do not wish to be subject of multiple emails or children who should not be the target of marketing efforts in the first place.

The CAN-SPAM Act covers email that has as its primary purpose the advertising or promotion of a commercial product or service. It does not cover emails facilitating a transaction or providing information to a customer with whom there is an established business relationship. Both the FTC and the Department of Justice enforce the CAN-SPAM Act. The act prohibits, for example, false or misleading header information and deceptive subject lines, and requires senders to give recipients an opt-out method, respond to opt-out requests, and identify commercial email as advertising. The CAN-SPAM Act focuses on:

- False or misleading header information. The email address must be accurate and identify the person who initiated the email.
- Deceptive subject lines. The subject line may not mislead the recipient about the message’s contents.
- Opt-out methods. The message must contain a return email address or other Internet-based response mechanism allowing recipients to opt out of future email messages.
- Response to opt-out requests. Senders must process opt-out requests for at least 30 days after the original commercial email. Upon receipt of an opt-out request, the sender has 10 business days to stop sending the emails.

Identifying commercial email as advertising. The email must clearly state that the message is an advertisement or solicitation and that the recipient can opt out of future emails. A valid postal address is required.

One of the purposes of the CAN-SPAM Act is to deter phishing, which is the illegal transmission of email masquerading as coming from a legitimate sender. Phishing and other targeted scams are discussed in detail in Reading 3, Safeguarding the Customer and the Bank. Because the purpose of phishing is to obtain sensitive personal and financial information such as bank account numbers and Social Security numbers, the fraudulent email is often in the guise of a marketing solicitation that appears to be from a bank.