Real Estate Technology
Virginia Salesperson PLE Series

MODULE 1
Do Not Call Rules and Regulations

Learning Objectives:

- Understand the Do Not Call Rules and Regulations as they pertain to licensees
- Recognize exemptions to the Do Not Call Rules and Regulations

Introduction

On March 11, 2003, President Bush signed the Do-Not-Call Implementation Act (Do-Not-Call Act), authorizing the Federal Trade Commission (FTC) to collect fees for the implementation and enforcement of a national do-not-call registry. In addition, the Do-Not-Call Act required both the Federal Communications Commission (FCC) and the FTC to issue rules under the Telephone Consumer Protection Act (TCPA) that implement the Do Not Call Registry.

It is important for real estate professionals to understand that certain calls to prospective clients are covered by federal rules implementing the Do Not Call Registry. This Section of the Course explains the two primary Do Not Call rules and exceptions, concluding with a discussion of special topics applicable to real estate professionals.

FCC and FTC Jurisdiction

While both the FTC and FCC have rules implementing the Do Not Call Registry under the TCPA, the FCC has the broadest authority. As such, the FCC rules implementing the national do-not- call registry cover all entities that use the telephone to advertise, including those entities over which the FTC lacks jurisdiction. Also, whereas the FTC's jurisdiction extends only to interstate calls (from state to state), the FCC's jurisdiction extends to both intrastate and interstate calls (state to state and calls made within a state).

The FCC and FTC jointly implemented a nationwide do-not-call registry following the adoption of rules by each agency to protect consumers from unwanted telemarketing calls. The FTC received funding to set up and administer the do-not-call registry, while both the FCC and FTC are responsible for enforcement of the do-not-call rules, along with the states. Telemarketers must pay fees to access the database and to "scrub" their calling lists of the telephone numbers in the database at least every 31 days.

Legal Challenges

Several telemarketers filed separate actions challenging the FCC-FTC registry in the Western District of Oklahoma and in the District of Colorado. On September 23, 2003, the Western District of Oklahoma Court entered judgment for the plaintiffs, holding that the FTC lacked authority to promulgate rules that pertain to the registry. Congress acted quickly to overrule this decision by enacting a statute ratifying the FTC's authority to establish the registry.

However, on September 25, 2003, the District of Colorado Court also entered judgment for plaintiffs, holding that the registry violated the First Amendment and enjoining the FTC from enforcing the rule provisions creating and implementing the registry. Although the FTC was forced to temporarily shut down the registry due to the court's decision, the FCC's rules nevertheless went into effect on October 1, 2003. The FCC announced that it intended to do everything legally permissible to enforce the registry and provide consumers with the protections afforded by the national do-not-call list.

On October 7, 2003, the U.S. Tenth Circuit Court of Appeals stayed the decision by the District of Colorado and allowed the FTC to reopen the do-not-call registry on October 9 to allow consumers to continue adding numbers to the list. Telemarketers were given access to the registry on October 10, 2003. Finally, on February 17, 2004, the Tenth Circuit upheld the constitutionality of the national do-not-call registry.

Principal Do Not Call Rules

There are two principal Do Not Call Rules that real estate professionals must understand—Entity-Specific Do Not Call Rules, and the National Do Not Call Registry. While there are exceptions to these rules as explained below, real estate professionals and others who violate them could face fines of up to $50,120 per violation. Violations may be measured on a per-call basis.

The Entity-Specific Rules

Since 1995, Federal rules have prohibited calls to any consumer who has asked not to be called again. These rules also prohibit a seller from

calling a consumer again after being asked not to call. Sellers and telemarketers are responsible for maintaining these individual Do Not Call lists of consumers who have asked not to receive calls placed by, or on behalf of, a particular seller. Calling a consumer who has asked not to be called potentially exposes a seller and telemarketer to a civil penalty of $50,120 per violation.

The National Do Not Call Registry

Since June 27, 2003, consumers may also place their telephone numbers on a National Registry by making a toll-free telephone call or via the Internet. Federal rules prohibit sales, telemarketing, and solicitation calls to consumers who register on the National Registry. Registration is valid until the consumer asks to be taken off the National Registry or the number is disconnected. The registry includes both traditional "land" lines and cellular or wireless telephone numbers. All household members who share a number must not be called after the number is registered.

Sellers, telemarketers, and their service providers can access the Registry through a dedicated Web site. In order to avoid penalties, sellers must access the Registry before making a call to a consumer.

Additionally, sellers must update their call lists—that is, delete all numbers in the National Do Not Call Registry from their lists—at least every 31 days. Violators will be subject to civil penalties of up to $50,120 per violation, as well as injunctive remedies. However, this provision does not apply to business-to-business calls or calls to consumers from or on behalf of charities. Still, telefunders calling to solicit charitable contributions must honor a donor's request not to be called on behalf of a particular charitable organization, under the Entity Specific Rules.

How the National Do Not Call Registry Works

The Do Not Call rules broadly prohibit any "telephone solicitation" to any residential telephone subscriber who has registered his or her telephone number on the National Do-Not Call Registry. This includes calls by sellers and telemarketers who solicit consumers on behalf of third-party sellers. It also includes sellers who are paid to provide, offer to provide, or arrange to provide goods or services to consumers, including some calls by real estate professionals.

However, the Do Not Call rules do not cover calls from political organizations, charities, telephone surveyors, or companies with which a consumer has an existing business relationship. Thus, real estate professionals may contact existing clients without violating the Do Not Call Rules, unless they have made an Entity Specific request.

Accessing the Registry

Access to the National Registry is limited to sellers, telemarketers, and other service providers. Some sellers are exempt from the FTC's Rules, but are required to access the National Registry under the FCC's Rules. Other sellers (charities and political organizations) are exempt from accessing the National Registry under both agencies' rules. These exempt sellers still may access the National Registry voluntarily and do not have to pay a fee for access. They must, however, submit appropriate certification information to gain access to the National Registry.

Access Must be for a Legitimate Purpose

The National Registry may not be used for any purpose other than preventing prohibited calls to the telephone numbers on the Registry. Any entity that accesses the National Registry will be required to certify, under penalty of law, that it is accessing the Registry solely to comply with the rules or to prevent calls to numbers on the registry.

Access and Update Methods

The FTC and the FCC host a fully automated and secure Web site at www.telemarketing.donotcall.gov to provide industry with access to the National Registry's database of telephone numbers, sorted by area code. The first time you access the National Registry, you must provide identifying information about yourself and your firm. Telemarketers or service providers accessing the National Registry on behalf of seller-clients must identify seller-clients and provide their unique account numbers.

The only consumer information available from the National Registry is telephone numbers. After you (or the company telemarketing on your behalf) have accessed the National Registry the first time, you will have the option to only download any changes that have occurred since the last time you accessed the Registry.

Sellers and telemarketers must synchronize their lists with an updated version of the National Registry every 31 days. You will be able to access data as often as you like during the course of your annual period for those area codes for which you have paid. However, to protect system integrity, you may download data files from the National Registry only once in any 24-hour period.

Companies that have provided the required identification information and certification and paid the appropriate fee (if they want to access more than five area codes) will be allowed to check a small number of telephone numbers (10 or less) at a time via interactive Internet pages. This will permit small volume callers to comply with the Do Not Call Rules without having to download a potentially large list of all registered telephone numbers within a particular area.

Paying for Access

Data for up to five area codes is available for free. Beyond that, there is an annual fee of $75 per area code of data, with a maximum annual fee of $20,740 for the entire U.S. database. The fee must be paid annually. Payment of the fee provides access to the data for an "annual period," which is defined as the twelve months following the first day of the month in which the seller paid the fee.

For example, a seller who pays its annual fee on September 15, 2023, has an "annual period" that runs from September 1, 2023 through August 31, 2024.

Enforcing The Do Not Call Registry

The FTC, the FCC, the states, and private citizens may bring civil actions in federal district courts to enforce the Rule. State attorneys general or any other officer authorized by the state to bring actions on behalf of its residents may bring actions by the states.

Private Citizens may bring an action to enforce the Rule if they have suffered $50,000 or more in actual damages. If state officials or private citizens bring a legal action under the Rule, they must provide written notice of their action to the FTC before filing a complaint, if feasible,

or immediately upon filing the action. The notice must include a copy of the complaint and any other pleadings to be filed with the court.

Compliance

It's against the law to call (or cause a telemarketer to call) any number on the National Registry (unless the seller has an established business relationship with the consumer whose number is being called, or the consumer has given written permission to be called). It is also against the law for a seller to call (or cause a telemarketer to call) any person whose number is within a given area code unless the seller first has paid the annual fee for access to the portion of the National Registry that includes numbers within that area code.

Safe Harbor

The Do Not Call Rules include a "safe harbor" for inadvertent mistakes. If a seller or telemarketer can show that, as part of its routine business practice, it meets all the requirements of the safe harbor, it will not be subject to civil penalties or sanctions for mistakenly calling a consumer who has requested not to be called (Entity Specific Rules), or for calling a person on the National Registry.

If a seller or telemarketer can establish that as part of its routine business practice, it meets the requirements detailed below it will not be subject to civil penalties or sanctions for erroneously calling a consumer who has asked not to be called, or for calling a number on the National Registry.

- The seller or telemarketer has established and implemented written procedures to honor consumers' requests that they not be called.

- The seller or telemarketer has trained its personnel, and any entity assisting in its compliance, in these procedures.

- The seller, telemarketer, or someone else acting on behalf of the seller or charitable organization has maintained and recorded an entity-specific Do Not Call list.

- The seller or telemarketer uses, and maintains records documenting, a process to prevent calls to any telephone number on an entity-specific Do Not Call list or the National Do Not Call Registry. This, provided that the latter process involves using a version of the National Registry from the FTC no more than 31 days before the date any call is made.

However, if there is a high incidence of "errors," the safe harbor may not prevent a penalty. The determination of whether an excusable "error" occurs is based on the facts of each case. A safe rule of thumb to ensure that adequate Do Not Call procedures are implemented is to test periodically for quality control and effectiveness.

Exemptions to the National Registry Rules

The Established Business Relationship Exemption

Sellers and telemarketers may call a consumer with whom a seller has an established business relationship, provided the consumer has not asked to be on the seller's entity-specific Do Not Call list. The Rule states that there are two kinds of established business relationships.

One is based on the consumer's purchase, rental, or lease of the seller's goods or services, or a financial transaction between the

consumer and seller, within 18 months preceding a telemarketing call. The 18-month period runs from the date of the last payment, transaction, or shipment between the consumer and the seller.

The other is based on a consumer's inquiry or application regarding a seller's goods or services, and exists for three months starting from the date the consumer makes the inquiry or application. This enables sellers to return calls to interested prospects even if their telephone numbers are on the National Registry.

For example, a consumer calls a broker to ask for more information about the broker's services. If the broker returns the consumer's call within three months from the date of the inquiry, whether the consumer's telephone number is on the National Registry is immaterial. But after the three month period, the broker would need either the consumer's express agreement to receive a call or a transaction-based established business relationship (assuming the consumer is registered on the National Registry).

An established business relationship is between a seller and a customer; it is not necessarily between one of the seller's subsidiaries or affiliates and that customer. The test for whether a subsidiary or affiliate can claim an established business relationship with a sister company's customer is: would the customer expect to receive a call from such an entity, or would the customer feel such a call is inconsistent with having placed his or her number on the National Do Not Call Registry?

Factors to be considered in this analysis include the nature and type of goods or services offered and the identity of the affiliate. Are the affiliate's goods or services similar to the seller's? Is the affiliate's

name identical or similar to the seller's? The greater the similarity between the nature and type of goods sold by the seller and any subsidiary or affiliate and the greater the similarity in identity between the seller and any subsidiary and affiliate, the more likely it is that the call would fall within the established business relationship exemption.

The Written Permission to Call Exemption

The Rule allows sellers and telemarketers to call any consumer who gives his or her express agreement to receive calls, even if the consumer's number is in the National Do Not Call Registry. The consumer must give express agreement in writing to receive calls placed by—or on behalf of—the seller, including the number to which calls may be made, and the consumer's signature. The signature may be a valid electronic signature, if the agreement is reached online.

If a seller seeks a consumer's permission to call, the request must be clear and conspicuous, and the consumer's assent must be affirmative. If the request is made in writing, it cannot be hidden; printed in small, pale, or non-contrasting type; hidden on the back or bottom of the document; or buried in unrelated information where a person would not expect to find such a request. A consumer must provide consent affirmatively, such as by checking a box. For example, a consumer responding to an email request for permission to call would not be deemed to have provided such permission if the "Please call me" button was pre-checked as a default.

Other Do Not Call Rules

Selling or Using a Do Not Call List for Purposes Other than Compliance

It is a violation of the Rule for anyone to sell, rent, lease, purchase, or use an entity-specific Do Not Call list or the National Registry for any purpose other than complying with the Rule's Do Not Call provisions or preventing calls to numbers on such lists. This provision applies to list brokers, third-party services, and others, in addition to sellers and telemarketers. It is intended to ensure that consumers' phone numbers on Do Not Call lists and the National Registry are not misused. It is a violation of this provision for a seller to market its own entity specific Do Not Call list to another entity for use as a "do call" list.

Sellers and telemarketers (on behalf of sellers) must purchase access to the relevant Do Not Call data from the National Registry database. The Rule prohibits participating in any arrangement to share the cost of accessing the National Registry database. A telemarketer may not divide the costs to access the National Registry database among various client sellers; access for each client seller must be purchased separately. Similarly, a telemarketer may not access the National Registry to obtain Do Not Call data and transfer the data to or share it with another telemarketer.

Denying or Interfering with Someone's Do Not Call Rights

It is a Rule violation to deny or interfere with someone's right to be placed on the National Do Not Call Registry or on any entity-specific Do Not Call list. This provision prohibits a seller or telemarketer from refusing to accept a consumer's entity-specific Do Not Call request,

whether by hanging up the telephone when the consumer asserts the request, harassing the consumer for having made such a request, or simply failing to diligently capture information about a consumer's Do Not Call request and add it to the appropriate entity-specific Do Not Call list. In addition, it would violate this part of the Rule for any person to purport to accept telephone numbers or other information for entry into the National Do Not Call Registry. No data from third parties is accepted into the National Do Not Call Registry.

Calling Time Restrictions

Unless a seller or telemarketer has a person's prior consent to do otherwise, it is violation of the Rule to make outbound telemarketing or telephone solicitation calls to the person's home outside the hours of 8 a.m. and 9 p.m.

Call Abandonment (and Safe Harbor)

The Rule expressly prohibits telemarketers from abandoning any outbound telephone call. While not typically used by real estate professionals, this part of the Rule exists to deal with telemarketers' use of predictive dialers to call consumers.

Predictive dialers promote telemarketers' efficiency by simultaneously calling multiple consumers for every available sales representative. This maximizes the amount of time telemarketing sales representatives spend talking to consumers and minimizes representatives' "downtime." But it also means some calls are abandoned: consumers are either hung up on or kept waiting for long periods until a representative is available.

Under the Rule's definition, an outbound telephone call is "abandoned" if a person answers it and the telemarketer does not

connect the call to a sales representative within two seconds of the person's completed greeting. The use of prerecorded message telemarketing, where a sales pitch begins with or is made entirely by a prerecorded message, violates the Rules because the telemarketer is not connecting the call to a sales representative within two seconds of the person's completed greeting.

The abandoned call safe harbor provides that a tele-marketer will not face enforcement action for violating the call abandonment prohibition if the telemarketer:

- Uses technology that ensures abandonment of no more than three percent of all calls answered by a live person, measured per day per calling campaign.
- Allows the telephone to ring for 15 seconds or four rings before disconnecting an unanswered call.
- Plays a recorded message stating the name and telephone number of the seller on whose behalf the call was placed whenever a live sales representative is unavailable within two seconds of a live person answering the call.
- Maintains records documenting adherence to the three requirements above.

A telemarketer also must eliminate "early hang-ups" by allowing an unanswered call to ring either four times or for 15 seconds before disconnecting the call. This element of the safe harbor ensures that consumers have reasonable time to answer a call and are not subjected to "dead air" after one, two, or three rings.

In addition, in the small permissible percentage of calls in which a live representative may not be available within two seconds of the

consumer's completed greeting, the telemarketer must play a recorded message. The message must state the name and telephone number of the seller responsible for the call, enabling the consumer to know who was calling and, should the consumer wish, to return the call. The Rule expressly states that sellers and telemarketers still must comply with relevant state and federal laws, including, but not limited to, the Telephone Consumer Protection Act (47 U.S.C. § 227) and FCC regulations at 47 C.F.R. Part 64.1200.

The FCC regulations prohibit such recorded messages from containing a sales pitch, but, like the FTC Rules, require that the message state "only the name and telephone number of the business, entity, or individual on whose behalf the call was placed and that the call was for "telemarketing purposes." The number on the recorded message must be one to which a consumer can call to place an entity specific Do Not Call request.

Finally, a telemarketer wishing to avail itself of the safe harbor for abandoned calls must keep records that document its compliance with the first three safe harbor components in accordance with the recordkeeping provision of the Rule. The records must establish that the abandonment rate has not exceeded three percent and that the ring time and recorded message requirements have been fulfilled.

Transmitting Caller ID Information

It is a violation of the Rules to fail to transmit or cause to be transmitted the telephone number, and, when available by the telemarketer's telephone company, the name of the seller or telemarketer to any consumer's caller identification service. To comply with this requirement, a telemarketer may transmit its own

number and, where available, its own name, to consumers' caller identification services.

The Rule also allows a substitution of the name of the seller (or charitable organization) on whose behalf the telemarketer is calling, and the seller's (or charitable organization's) customer (or donor) service telephone number, which is answered during regular business hours.

There may be situations when a consumer who subscribes to a Caller ID service does not receive a telemarketer's transmission of Caller ID information despite the fact that the telemarketer has arranged with its carrier to transmit this information in every call. This can happen if the Caller ID information is dropped somewhere between the telemarketer's call center and the consumer's telephone.

Telemarketers who can show that they took all available steps to ensure transmission of Caller ID information in every call will not be liable for isolated inadvertent instances when the Caller ID information fails to make it to the consumer's receiver. Nevertheless, a telemarketer's use of calling equipment that is not capable of transmitting Caller ID information is no excuse for failure to transmit the required information.

Threats, Intimidation, and Profane or Obscene Language

Sellers and telemarketers are prohibited from using threats, intimidation, and profane or obscene language in a call. This prohibition covers all types of threats, including threats of bodily injury, financial ruin, and threats to ruin credit. It also prohibits intimidation, including acts that put undue pressure on a consumer, or that call into question a person's intelligence, honesty, reliability, or

concern for family. Repeated calls to an individual who has declined to accept an offer also may be viewed as an act of intimidation.

PROGRESS CHECK 1

1. Solicitors must "scrub" their calling lists for telephone numbers in the do not call registry database at least _____.
   A. Quarterly
   B. Annually
   C. Every 180 days
   D. Every 31 days

2. Who may access the National Registry?
   A. Sellers
   B. Telemarketers
   C. Other Service Providers
   D. All of the Above

3. Who enforces the National Do Not Call Registry?
   A. FCC
   B. FTC
   C. EPA
   D. Both A and B

4. Real estate agents who violate the Do Not Call Registry could face a penalty of:
   A. Fines of up to $41,484 per violation.
   B. Fines of up to $48,242 per violation.
   C. Fines of up to $50,120 per violation.
   D. Fines of up to $42,856 per violation.

MODULE 2
Special Concerns & Do Not Email Legislation

Learning Objectives:

- Be familiar with the Do Not Call Registry Special Concerns & Do Not Email Legislation
- Explain the parameters of the CAN-SPAM act, specifically the unsubscribe rules

Special Concerns for Professionals

Even though the law is intended primarily to combat professional telemarketing, Real estate professionals must comply with the Do Not Call Rules and related provisions. Real estate professionals do, however, face unique challenges under the rules.

For Sale By Owner

Real estate professionals may need to contact owners attempting to sell their own property. This may arise, for example, where an agent either desires to list a property that is for sale by owner, or needs to arrange a walk through for a client/ buyer. The issue then arises whether the agent must be mindful of the Do Not Call Rules. In the case of arranging a walk through, the agent's call would not be implicated by the rules because the agent is not calling to solicit or sell a product or service. However, in the case of the agent calling to

obtain a listing, he or she must first check the National Registry. Such transactions do not appear to satisfy the requirements for the business to business call exemption.

Consumers Calling to Discuss Listings

If a consumer calls to inquire about a particular listing, it is permissible to call that consumer for a three month period, regardless of whether they are registered on the National Do Not Call Registry. However, if the consumer directly requests that they not be called again by the agent, that request must be honored under the "Entity-Specific" Do Not Call Rules. Provided there is no such request, an agent may call this prospect to discuss not only the listing they inquired about, but also any other listing.

Referrals

If an agent receives a referral, even from a previous or current client, that agent must follow the Do Not Call Rules. In other words, the agent must check the registry before placing a call to the prospect. This is so even if the purported referral regards a person who wants to receive a telephone call. Because the request is indirect, it does not constitute a customer inquiry.

Open House Events

Open house visitors commonly fill out sign-in sheets that request contact information for further information. While this may be a customer inquiry under the Rules, the matter is not entirely clear. The best course of action is for the agent to include a disclaimer on the sign-in sheet sufficient to gain the consumer's consent to receive a call from the agent about his or her services.

Do Not Email Legislation

Email is a marketing tool used by many companies, including real estate professionals. In order to avoid penalties, Virginia licensees must understand Virginia State and Federal laws that regulate bulk emailing.

What is Spam?

Spam is unsolicited "junk" email sent to large numbers of people to promote products or services. It is the email equivalent of junk mail delivered by the Post Office. Spam is a common marketing tactic used by real estate professionals and other business interests. However, like junk postal mail, consumers are not always happy to receive spam.

Is Spam Bad?

Your feelings about spam probably have a lot to do with whether you are a consumer of Spam or a source of spam. Both parties can benefit from spam—consumers may learn of new products or services that they want, and companies can increase sales by directly reaching potential customers cheaply and quickly. However, when abused, spam can be problematic.

In some ways, the spam receiver pays a higher price to receive it than the sender pays to send it. For example, AOL at one time claimed to receive 1.8 million spams from one spamming company per day until they stopped it with a court injunction. Even if it took the average user only 10 seconds to identify and remove a spam email, this could total 5,000 hours per day of connection time per day to discard spam from just one spam company on just one service provider. Also, some experts claim that the volume of spam slows Internet traffic and in some cases can disable or slow company servers.

Federal Laws Governing Unsolicited Email

The Federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) was signed by President Bush on December 16, 2003, and took effect on January 1, 2004. The CAN-SPAM Act regulates unsolicited commercial email messages, stating that it must be labeled, include opt-out instructions, and include the sender's physical address.

The Act also prohibits deceptive subject lines and false headers. Finally, the Act authorized the Federal Trade Commission (FTC) to establish a do not email registry, similar to the do not call registry. However, the FTC has not yet developed such a registry.

Do Not Email Legislation

The Federal Trade Commission (FTC) is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address. Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include your valid physical postal address.

Note that it is common for businesses to mix commercial and transactional or relationship content in a single message. When an email contains both types of content, the primary purpose is the deciding factor for whether it must follow the regulations of the CAN-SPAM Act. If the message contains only commercial content and was primarily sent for that purpose, the email must comply with the regulations of the CAN-SPAM Act.

Prohibited Conduct

The following is a summary of CAN-SPAM's main provisions:

- **It bans false or misleading header information.** Your email's "From," "To," and routing information – including the originating domain name and email address – must be accurate and identify the person who initiated the email.

- **It prohibits deceptive subject lines.** The subject line cannot mislead the recipient about the contents or subject matter of the message.

- **It requires that your email give recipients an opt-out method**, similar to the Entity Specific Rules for telephone solicitations. You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future email messages to that email address, and you must honor the requests. You may create a "menu" of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender.

Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial email. When you receive an opt-out request, the law gives you 10 business days to stop sending email to the requestor's email address. You cannot help another entity send email to that address, or have another entity send email on your behalf to that address.

Finally, it's illegal for you to sell or transfer the email addresses of people who choose not to receive your email, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.

It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address. Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include your valid physical postal address.

Civil Penalties

CAN-SPAM act violators are subject to penalties of $250 per violating e-mail, with a maximum of $2 million, plus attorneys' fees. Additional fines are provided for commercial emailers who not only violate the rules described above, but also:

1. "harvest" email addresses from Web sites or Web services that have published a notice prohibiting the transfer of email addresses for the purpose of sending email;

2. generate email addresses using a "dictionary attack" – combining names, letters, or numbers into multiple permutations;

3. use scripts or other automated ways to register for multiple email or user accounts to send commercial email

4. use another computer without authorization and send commercial email from or through it;

5. use a computer to relay or retransmit multiple commercial email messages to deceive or mislead recipients or an Internet access service about the origin of the message;

6. falsify header information in multiple email messages and initiate the transmission of such messages;

7. register for multiple email accounts or domain names using information that falsifies the identity of the actual registrant;

8. falsely represent themselves as owners of multiple Internet Protocol addresses that are used to send commercial email messages.

Future Rules

The Act also instructs the FTC to explore a National Do Not Email Registry, and issue reports on the labeling of all commercial email, the creation of a "bounty system" to promote enforcement of the law, and the effectiveness and enforcement of the CAN-SPAM Act.

However, be advised, that the FTC recently reported to Congress that a national do not email registry would not be effective at this time for a number of reasons, including the high risk that it would result in more in-box clutter because illegal spammers would use the registry as a "do spam" list.

The FTC advises consumers not to submit their email addresses to any organization that claims to be creating a do not spam list. If you have already submitted your email address to a "national do not email registry" that promises to reduce the amount of spam you receive, you may be the victim of a scam.

The FTC is concerned that some sites could be part of a high-tech scam to trick consumers into disclosing their email address or other sensitive personal information. The site may be a ruse to collect valid email addresses to sell to spammers. The result could be even more spam for consumers who sign up for the "registry." Or, it may be even worse - some scammers have collected information through bogus Web sites that mimic those of legitimate organizations, and then use the information to commit identity theft.

Unsubscribe Requirements

In addition to the requirements of the CAN-SPAM Act, claims made in any advertisement for products or services, including those sent by email, must be truthful under the Federal Trade Commission Act. This means that any promises made to remove consumers from email mailing lists must be honored.

If email solicitations claim that consumers can opt-out of receiving future messages by following removal instructions, such as "click here to unsubscribe" or "reply for removal," then the removal options must

function as claimed. That means any hyperlinks in the email message must be active and the unsubscribe process must work.

Keep in mind:

1. You should review the removal claims made in your email solicitations to ensure that you are complying with any representations that you make.
2. If you provide consumers a hyperlink for removal, then that hyperlink should be accessible by consumers.
3. If you provide an email address for removal, then that address should be functioning and capable of receiving removal requests. It may be deceptive to claim that consumers can "unsubscribe" by responding to a "dead" email address.
4. Any system in place to handle unsubscribe requests should process those requests in an effective manner.
5. The Federal Trade Commission Act prohibits unfair or deceptive advertising in any medium, including in email. That is, advertising must tell the truth and not mislead consumers. A claim can be misleading if it implies something that's not true or if it omits information necessary to keep the claims from being misleading.

Other points to consider if you market through commercial email:

Disclaimers and disclosures must be clear and conspicuous. That is, consumers must be able to notice, read or hear, and understand the information. Still, a disclaimer or disclosure alone usually is not enough to remedy a false or deceptive claim.

If you promised refunds to dissatisfied customers, you must make them.

Virginia Laws Governing Unsolicited Email

Virginia has enacted computer and Internet related laws, including laws that make it illegal to: send unsolicited commercial email (spam) containing falsified transmission or routing information; to possess and/or distribute software designed to falsify spam transmission or routing information; or to hire someone to perform such acts.

Violations may be penalized criminally with a misdemeanor or felony charge, depending on the number of intended recipients and the revenue received from such falsified spam emails. If the sender thereby violates a service provider's policies, he may be penalized civilly: up to $10 per email or $25,000 per day by the injured person; or $1 per recipient or $25,000 per day by the email service provider.

This law was a first among states and is an effort to address crimes committed via computers or computer networks. In November 2004, the Attorney General's Computer Crime Unit obtained the first felony spam conviction using this new law. In 2008, the constitutionality was questioned by the Virginia Supreme court, as the original wording might be applied towards all commercial emails. However, the Act has since been re-written to correct the issue. As of 2010, the Act differentiates between lawful commercial emails and unsolicited spam.

PROGRESS CHECK 2

1. What obligations do Federal laws currently impose on SPAM?
   A. It must be labeled
   B. It must include opt-out instructions
   C. It must include the sender's physical address
   D. All of the Above

2. Which authority enforces the CAN-SPAM act?
   A. Department of Justice
   B. Federal Trade Commission
   C. Internet Service Providers
   D. Any of the above

3. If a sender of spam receives an opt-out request, within how many days must the sender stop sending emails to the requester's address?
   A. 14 days
   B. 10 days
   C. 30 days
   D. 48 hours (2 days)

4. Senders who violate service providers policies regarding email solicitations can be fined up to _____ per day.
   A. $10,000
   B. $25,000
   C. $50,000
   D. $80,000

MODULE 3
The Wired Real Estate Consumer

Learning Objective:

- Understand How Real Estate Consumers Use the Internet to maximize marketing

---

Background

The Internet has changed almost every American business, including the real estate profession. Many consumers turn to the Internet in order to research products and seek competitive pricing. A recent study found that 79% of Internet Buyers found their real estate agent online. Of those, 88% did so on a site that listed a home they were interested in. The median price of homes purchased by Internet Buyers was 46% higher than homes bought by Traditional Buyers. Finally, 96% of Internet Buyers were "Very Likely" to use the Web again the next time they buy a home.

As the Internet continues to affect consumer and business relationships, it will eventually be the leading method of selecting a real estate agent. For example, buyers from distant markets can now access more information about agents than ever before, and they are now more likely than ever to consider the quality and helpfulness of information provided on an agent's Website. This section discusses how to keep up with the wired customer while maintaining professionalism, avoiding ethical and legal violations, and securing information.

Listing Property on the Internet

Once highly coveted by brokers, Multiple Listing Services (MLS) are now available to anyone with an Internet connection, free of charge. Why make MLS listing freely and widely available? Some believe that the ability to view all listings together spurs competition. Competition benefits the consumer by increasing the scope of one's property search. Increased availability and wider exposure can increase demand.

In addition to MLS and other property listings, many sites provide local community profiles and links to lending data. Community profiles include information on local demographics, schools, crime, community governance, and community events. Lending data includes basic requirements for qualifying for various loan amounts, payment calculators, and interest rates. Such a broad range of information enables consumers to focus their requirements before contacting an agent. The agent may then experience greater efficiency and increased transactions.

The Agent's Value to the Wired Consumer

While today's wired consumer can obtain a wealth of information about real estate products and services without using an agent, the fact remains that most real estate transactions involve at least one real estate agent. Like any other professional service, real estate agents offer expertise and experience that most consumers do not have or choose not to acquire. Free Internet data enhances a consumer's experience with an agent, but in most cases it does not replace the

agent. As such, an agent's skill in consummating a complex transaction will always be in demand.

Maximizing Internet Tools

Agents must maximize their Internet skills in order to effectively serve the increasingly sophisticated consumer and remain competitive with other agents. It is better to think of the Internet as a tool to increase efficiency and productivity, rather than a threat. However, to realize the power of this tool, real estate professionals must continually sharpen their skills and continue to learn.

Today, Internet-savvy real estate professionals obtain plat maps, property records, and link consumers to lenders. Some online mortgage companies can connect licensees and their clients with loan representatives via Internet video. Once connected, they can see and hear one another and process interactive mortgage applications or pre-qualifications in real time.

The Internet lending experience can include the transmittal of electronic signatures for credit report authorizations, and in some cases, loan approval on the spot or within 48-hours. If a model for Internet-based notary services is developed, parties will be able to complete entire transactions online, including escrow and title functions.

Internet Tools for Real Estate Licensees

Internet marketing is likely the most changed aspect of the real estate profession. In addition to the broader availability of listings, virtual property tours allow greater marketing efficiencies.

Virtual tours enable the consumer to tour a listing from their computer. Virtual tours often include the ability to freely "move" throughout the home and view bedrooms, the grounds, breathtaking views, secluded gardens, and other selling points. In some cases, the virtual tour includes audio, like the sound of waves crashing on the waterfront. Such exposure was once limited to live appointments or open house tours. Increasing the visibility of a property's key features may increase the number of interested purchasers.

There are many opportunities to use the Internet to highlight an agent's role as a provider of experience and knowledge, rather than a mere purveyor of information. Clearly, the Internet is changing forever the way the real estate business is conducted. Yet, despite these changes in the presentation and availability of information, the need to connect with people remains as critical as ever. Next, we will discuss the basic building block of all Internet services, the webpage.

Website Development

An Agent's Internet presence begins with a web page. Increasingly, real estate salespersons create personal web pages to supplement their broker's site. These sites range from simple web pages that agents create from off the shelf software, to sophisticated sites that employ the use of professional web designers. Some web designers even specialize in real estate-related products for agents such as virtual tours, guest books to capture prospecting data, and automatic email replies.

Regardless of how you choose to create your webpage, it should include a theme that targets a specific market. In planning a successful theme, one must work on their own or with a developer to determine:

1. their target audience;
2. any niche products such as luxury homes, first-time buyers, lake properties, or golf course homes;
3. and how competitive Internet sites are or are not successful.

In addition to design, web designers and developers may also post and maintain a web page. Perhaps the most important task after web design is choosing a domain name, or the address of your web page. Some agents designate their domain name as their first and last name, like jacksmith.com. Other agents use the name of their principal market like “fairfaxrealestate.com,”or “fairfaxhomesforsale.com.” Still other agent’s use the names of niche markets, like “downtown-homesforsale.com.” Although many of the more popular names are taken, a little creative thinking may yield similar results.

After you choose a domain name, you must select a hosting service. A hosting service offers to post your web design on a computer with a high-speed connection to the Internet so that others may view your content. Most website design and development firms also provide hosting services for a monthly fee. Hosting fees are usually based on the amount of content (memory) that your site contains—more content means more space, which increases costs. Fancier features like virtual tours and video clips may add to the cost as well.

PROGRESS CHECK 3

1. What is the most changed aspect of the real estate profession?
   A. Do Not Call Registry Rules
   B. Internet marketing
   C. Fair Housing Law updates (including gender identity and sexual orientation as protected classes)
   D. Licensing qualifications

2. If an agent wants to have an internet presence they must:
   A. Secure a service provider
   B. Clearly understand social media
   C. Get approval from VREB to advertise online
   D. Establish a webpage

3. What are website hosting fees based on?
   A. Region
   B. Amount of content
   C. Prorated share of profits garnered from the site
   D. Website views

4. Who is allowed to access the MLS?
   A. Brokers
   B. All real estate licensees
   C. Anyone who buys a subscription
   D. Anyone with internet service

MODULE 4
Internet Security

Learning Objective:

- Explain the risk associated with the Internet
- Explore measures to improve internet security

This section presents practical tips for reducing the amount of legal and illegal Spam received, and tips for detecting and deleting spyware.

SPAM

As discussed previously, Spam is now regulated under both state and federal laws. To reduce the amount of Spam you receive, consider the following:

- Check privacy policies before providing your email address on Web registration forms, surveys, etc. If you must provide your email address, look for a box that asks if it is okay to send you offers or information. You may want to say "no" if the Web site won't protect your address.

- Request net directories such as WhoWhere. com, 411.com and Switchboard.com to remove your name, e-mail address and other personal information from their databases. Simply go to the Web site, click on the "contact us" link and then request that your information be removed.

- If you subscribe to a list, ask the list administrator to shield you from outside email commands that allow third parties to view the list.

- Where services provide for member profiles, consider leaving your email address out of your profile.

- Avoid posting your email address in chatrooms, newsgroups, or on auction and sales sites.

- Do not list your email address directly on a Web page, even your own. Use an alias or a secondary account that you can delete later if necessary.

- If you attempt to use a "remove me" link that does not work, make sure you report it to the Federal Trade Commission (FTC) or to the Office of the Attorney General in Virginia. The new Anti-SPAM law in Virginia makes it a crime to use fraudulent means such as falsifying header information or other routing information to send SPAM.

- Block unwanted emails from a specific spammer by using filters within your email program. This feature is available in most standard e-mail programs. Simply type "filters" into the help section for instructions.

- When choosing an ISP consider whether the ISP offers spam-filtering options.

- Once you've been "spammed," ask your ISP to block all future email from the sender.

- Consider using a disposable e-mail account that you can easily change or shut down if it begins to receive too much spam.

Spyware

Just when you thought you were Web savvy, one more privacy, security, and functionality issue crops up — spyware. Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to identity theft.

Many experienced Web users have learned how to recognize spyware, avoid it, and delete it. The Federal Trade Commission (FTC) advises that all computer users should get wise to the signs that spyware has been installed on their machines, and then take the appropriate steps to delete it.

Clues You Might Be Infected

The clues that spyware is on a computer include:

1. a barrage of pop-up ads;
2. a hijacked browser — that is, a browser that takes you to sites other than those you type into the address box;
3. a sudden or repeated change in your computer's Internet home page;
4. new and unexpected toolbars;
5. new and unexpected icons on the system tray at the bottom of your computer screen;

6. keys that don't work (for example, the "Tab" key that might not work when you try to move to the next field in a Web form);
7. random error messages;
8. sluggish or downright slow performance when opening programs or saving files

Prevention

The good news is that consumers can prevent spyware installation. Indeed, experts at the FTC and across the technology industry suggest that you:

1. Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that spyware could exploit.

2. Download free software only from sites you know and trust. It can be appealing to download free software like games, peer-to-peer file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware, however, that some of these free software applications bundle other software, including spyware.

3. Don't install any software without knowing exactly what it is. Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find — or difficult to understand — think twice about installing the software.

4. Minimize "drive-by" downloads. Make sure your browser security setting is high enough to detect unauthorized

downloads, for example, at least the "Medium" setting for Internet Explorer. Keep your browser updated.

5. Don't click on any links within pop-up windows. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the "X" icon in the title bar.

6. Don't click on links in spam that claim to offer anti-spyware software. Some software offered in spam actually installs spyware.

7. Install a personal firewall to stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and will alert you if spyware already on your computer is sending information out.

If You're Infected

If you think your computer might have spyware on it, experts advise that you take three steps:

1. Get an anti-spyware program from a vendor you know and trust.
2. Set it to scan on a regular basis — at least once a week — and every time you start your computer, if possible.
3. Delete any software programs the anti-spyware program detects that you don't want on your computer.

PROGRESS CHECK 4

1. If a "remove me" link doesn't work to properly remove you from an email distribution list, notify:
   A. DPOR
   B. The internet service provider
   C. The sender of the email
   D. The Office of the Attorney General

2. Which of the following is NOT typically a result of spyware?
   A. Monitor internet searches
   B. Sends pop up ads
   C. Send spam emails
   D. Record keystrokes

3. An unexpected toolbar or hijacked browser could be a sign of:
   A. Spyware
   B. Spam
   C. Firewall test
   D. Any of the above

4. Which of the following can be effective in preventing spyware installation?
   A. Keep operating system updated
   B. Don't install unfamiliar software
   C. Don't click on links within pop-up ads
   D. All of the above