F&I and Showroom

ARTICLE

August 2010 - Feature

A Dealer's Guide to Digital Compliance

By Joe Bartolone

As many dealers are learning today, the Internet presents a host of opportunities to communicate and sell to consumers. It combines aspects of print, television and radio advertising in an interactive environment. However, digital marketing also raises a host of interesting — and, occasionally, complex — questions about the applicability of the laws that were developed long before "dot-com" became a household term.

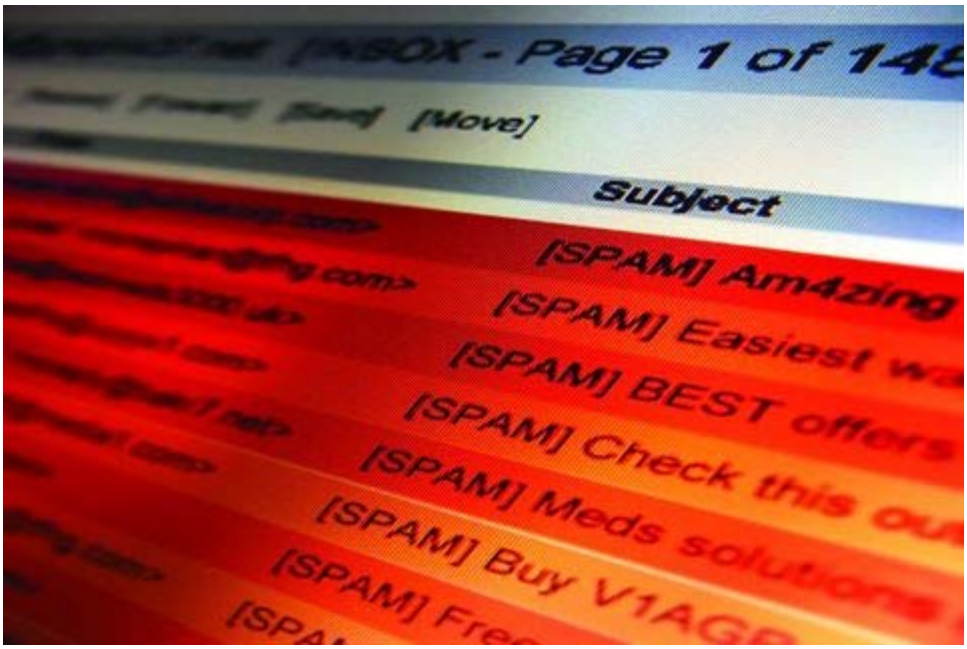
For most dealers, Internet sales departments can range from a single Internet manager to a full-blown business development center (BDC). Regardless of how you staff this department, every individual tasked with managing the dealership's online presence is subject to the same rules and regulations. Let's run through the digital sales cycle and identify several laws and regulations that you should consider when developing a compliance manual for the digital realm.

Internet Advertising

Many of the general principles of advertising law apply to Internet ads, but new issues arise almost as fast as technology develops. Your primary guide should be the Federal Trade Commission Act's prohibition on "unfair and deceptive acts or practices," which broadly covers advertising claims, marketing and promotional activities, and sales practices in general.

The FTC also has published several booklets to help you develop your rules of the road for advertising on the Web. "Dot Com Disclosures: Information About Online Advertising" is particularly useful. The 83-page booklet provides insight into the FTC's expectations for online marketers. The main topics covered are:

- How FTC regulations apply to Internet ads.
- Clear and conspicuous disclosure in online ads.
- How to apply certain rules to Internet activities.



The CAN-SPAM Act established rules for commercial e-mail usage, mandates for commercial messages, and put in place e-mail opt-out requirements. It also spelled out tough penalties for violators, with each violating e-mail sent to a consumer subject to a $16,000 penalty.

E-Mail Campaigns

If you use e-mail in your business, you should be aware of the CAN-SPAM Act of 2003. It was created to establish rules for commercial e-mail usage, mandates for commercial messages, e-mail opt-out requirements, and to spell out tough penalties for violations. In fact, each violating e-mail you send to your customers is subject to a penalty of $16,000. Let's take a look at some of the key requirements:

- Don't use false or misleading header information.
- Don't use deceptive subject lines.
- Identify the message as an ad.
- Tell recipients where you're located.
- Tell recipients how to opt out of future e-mails from you.
- Honor opt-out requests promptly.
- Monitor what others are doing on your behalf.

In the event of a violation of the Telephone Consumer Protection Act, consumers can collect from solicitors damages of $500 to $1,500 for each violation, or recover actual monetary loss, whichever is higher.

Telemarketing

Whether you are cold calling a prospect, chasing an Internet lead, making a courtesy follow-up call to a recent sales or service customer, or soliciting your customers to schedule a service appointment, you should be aware of the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), and the National Do Not Call Registry. Let's take a look at each one:

1. Telephone Consumer Protection Act: In the event of a violation of the TCPA, individuals are entitled to collect damages directly from the solicitor of $500 to $1,500 for each violation, or recover actual monetary loss, whichever is higher. Let's run through some of the TCPA's key provisions:

- Solicitors may not call residences before 8 a.m. or after 9 p.m.
- The solicitor must maintain a Do Not Call Registry, which must be honored for five years.
- Solicitors must provide their name, the name of the person or entity on whose behalf the call is being made and a telephone number or address at which that person or entity may be contacted.
- Solicitation calls cannot be made to residences with artificial voices or recordings.
- Calls cannot be made with artificial voices or recordings to cell phones or to any service in which the recipient is charged for the call.
- Prerecorded or autodialed calls cannot engage two or more lines of any business or any emergency number.
- Unsolicited advertising faxes also are prohibited.

2. The Telemarketing Sales Rule: The FTC issued the amended TSR in January 2003 and, like the original 1995 version it amended, the rule gives effect to the Telemarketing and Consumer Fraud Abuse Prevention Act. This legislation gives the FTC and state attorneys general law enforcement tools to

combat telemarketing fraud, adds privacy protections and defenses against unscrupulous telemarketers for consumers and helps them tell the difference between fraudulent and legitimate telemarketing.

One significant amendment to the TSR prohibits calling consumers who have put their phone numbers on the National Do Not Call Registry. Another change covers the solicitation of charitable contributions by for -profit telemarketers. Other key provisions include:

- Requires disclosures of specific information.
- Prohibits misrepresentations.
- Limits on when telemarketers may call customers.
- Requires transmission of caller ID information.
- Prohibits abandoned outbound calls that are subject to safe harbor.
- Prohibits unauthorized billing.
- Sets payment restrictions for the sale of certain goods and services.
- Requires that specific business records be kept for two years.

The Do Not Call Registry

Pursuant to its authority under the TCPA, the Federal Communications Commission, together with the FTC, established the National Do Not Call Registry. The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls.

According to the TCPA, commercial telemarketers are not allowed to call consumers if their numbers are on the registry. As a result, consumers can, if they choose, reduce the number of unwanted phone calls to their homes. But like everything, there are certain exceptions to this rule. Let's take a look:

- Consumers may be called for up to 18 months after their purchase, rental or lease of the seller's goods or services, or any other financial transaction between them and the seller.
- Consumers may be called for up to three months after they contact the seller with an inquiry.
- Consumers may be called if they have given their written consent to receive telemarketing calls.

Fax Solicitation

The main rule governing fax solicitations is the Junk Fax Prevention Act (JFPA), which was signed into law in July 2005. Among other things, it significantly altered the TCPA and the CAN-SPAM Act with regards to fax solicitations.

The statute is one of strict liability. Even if one sends an unsolicited fax advertisement by accident, his or her minimum liability is $500 per page. Damages also may be tripled at the court's discretion if the violation is found to be willful or knowing.

The only real defense for the sender is if the transmission meets the established business relationship (EBR) exception the JFPA created. To qualify, the sender must have the following:

- An EBR with the recipient.
- The recipient's fax number voluntarily from the recipient in the context of the EBR.
- A clear and conspicuous notice included on the first page of the advertisement that instructs the recipient on how to opt out of future advertisements.
- A domestic telephone or fax number to opt out included in the solicitation.
- At least one cost-free mechanism for transmitting an opt-out request, which must be available 24 hours a day, 7 days a week.
- An opt-out notice that's distinguishable from the advertising material through, for example, use of bolding, italics, a different font, or the like.
- An opt-out option that is not in the form of a "negative option." A facsimile advertisement containing a telephone number and instructions to call if the recipient no longer wishes to receive such faxes would constitute a "negative option," as the sender presumes consent unless advised otherwise.
- Honor all opt-out requests within a reasonable period of time (not to exceed 30 days).

Online Credit Applications

For several years now, I have informally surveyed Internet managers and other e-marketing professionals about the number of credit applications they're receiving online. The answers are always somewhere between 5 and 10 percent of all Internet leads. This could mean a couple of applications a month for some dealers and hundreds of applications per month for others.

Applications are most likely to come from the dealership's Website, but occasionally they might come from a manufacturer's Website or a third-party lead source. Regardless of the number of applications received or where they were originated, the same rules that apply to in-house credit applications apply to online applications.

Internet Privacy

Compliance with the Gramm-Leach-Bliley Act is mandatory, whether a financial institution (including dealers) discloses nonpublic information or not. That means there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

Major components governing how a customer's nonpublic personal information (or personally identifiable information) is collected, disclosed and protected include:

1. Privacy Notice: Financial institutions must provide their clients with a privacy notice that explains what information the company gathers about the client, where this information is shared, and how the company safeguards that information.

2. Safeguards Rule: Requires financial institutions (including dealers) to develop a written information security plan that describes how the company will protect its clients' nonpublic personal information. This plan must include:

- Denoting at least one employee to manage the safeguards.

- Constructing thorough risk management of each department handling a customer's nonpublic information.

- Develop, monitor and test a program to secure the information

- Update policies or procedures as needed and document whatever changes are made.

3. Pretexting Protection: Sometimes referred to as "social engineering," pretexting occurs when someone tries to gain access to personal nonpublic information without proper authority. This may entail requesting private information while impersonating the account holder by phone, mail, e-mail, or even phishing for data over the phone, online or via e-mail.

Dealerships that experience high volumes of online credit applications must also be aware of the provisions of both the Equal Credit Opportunity Act and the Fair Credit Reporting Act. Obtaining consent to check credit is a requirement of the ECOA. Typically, having a "submit" button on your Website will fulfill the electronic consent requirement.

Taking online credit apps also brings into play the Adverse Action Notice requirement. This is especially true as dealers attempt to maintain positive look-to-book ratios with their lenders. So, if your dealership is screening applications before submitting them to the lender, you are required to send an Adverse Action Notice. But there is more to the requirement than just sending the notice. The methods with which you send the notice, the information you provide in the notice and having a process to address customer inquiries are also part of the requirement.

Internet Sales

Two sites that come to mind when it comes to Internet sales are Craigslist and eBay Motors. They allow people and businesses to buy and sell a variety of goods and services worldwide. Dealers are very active in marketing vehicles on both sites. But when I think of these two platforms, I can't help but to think of the would-be terrorist who tried to set off a car bomb in Times Square. The vehicle used in the plot was purchased through eBay.

Now, the vehicle was classified as a private party sale. If it had been purchased from a dealership, two very important rules would have come into play — the USA PATRIOT Act and the Red Flags Rule. Let's review each rule.

1. The Patriot Act's Three Main Provisions:

- Verify the identity of any person seeking to open an account. A non-expired government issued identification, such as a driver's license, military ID or passport are acceptable forms of ID.

- Maintain records of the information used to verify a person's identity, including the name, address and other identifying information. Create and retain a photocopy of the ID.

- Consult government lists of known or suspected terrorists or terrorist organizations (i.e., conduct an OFAC check).

2. The Red Flags Rule: Financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs — or "red flags" — of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents.

The program also must describe appropriate responses that would prevent and mitigate the crime and create a framework for updates. The program must be managed by a board of directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of all service providers.

When it comes to the Internet, it is important that your digital compliance manual provides your employees with a clear understanding of how they must conduct themselves when working online. Most importantly, it should cover behaviors and detail the risks involved.

Joe Bartolone is an associate with gvo3 & Associates, a nationally recognized sales and F&I compliance consulting company. He can be reached at joe.bartolone@bobit.com.

Sidebar: Social Media Risks

A review on digital compliance would not be complete without a brief discussion about social networking. Last year, Facebook surpassed 300 million users, while Twitter claimed to have six million unique monthly visitors and 55 million monthly visitors. So, it seems reasonable that dealerships would want to participate in that kind of exposure.

The positive side of social networking is that users can upload and exchange pictures, text, music, and other types of information with little effort. The negative side of social networking is that users can upload and exchange pictures, text, music and other types of information with little effort. Social networking sites are meant to get as many users as possible in one place. One security analyst described these sites as a perfect storm of social engineering and bad programming. For attackers, there's a lot of return on investment for going after these sites.

In the workplace, sites like MySpace, Facebook, LinkedIn and Twitter have been the bane of information technology administrators. They dislike it and cyber crooks depend on it, so make sure you address the risks of social networking in your policy and procedures manual and be ready for changes as new scams pop up.