



The  
**\$16,000**  
EMAIL MARKETING MISTAKE



LEAF Commercial Capital, Inc. is a subsidiary of People's United Bank, N.A.

Email marketing can be a game changer for virtually any business—but only if it's done the right way. Today, investing in and launching an email marketing campaign is a strategy that makes sense for just about any company. In terms of the relative cost of marketing tactics, the investment required to launch and maintain an extensive email marketing program is modest. Beyond the cost and effectiveness of email marketing however, and regardless of whether you're just considering or are already using it, there is one more very important caveat. It is important to be familiar with the federal regulations governing email marketing and how they impact you, a subject that is often overlooked when embarking on an email marketing program.

Compliance is the first step in maximizing the effectiveness of—and results from—your email marketing efforts. This white paper covers the major aspects of anti-spam regulations and provides some advice on compliance with them. Future white papers will cover the other important aspects of email marketing best practices as well.

### Ask Permission - Don't Beg For Forgiveness

---

Email marketing best practices have evolved over the years to the point where most legitimate email marketers confine their efforts to an “opt-in” list of recipients. These targeted prospects and existing customers have given consent and are willing to accept marketing messages. Opt-in lists are typically created in one of two ways. The first is to enable potential prospects to sign up for ongoing emails from your dealership. One effective way of framing this is to offer an ongoing electronic newsletter—often called an e-zine—that provides valuable information that subscribers can use. Additionally, as an incentive to sign up, many email marketers offer an incentive such as a white paper or special report in return for signing up.

Another means of obtaining an opt-in list is to simply buy it from a professional list broker. These brokers typically use a network of websites that continuously attract visitors and invite them to sign up for information about particular areas of interest such as in this case office automation or business equipment. These brokers then compile the lists and sell them to businesses. It should be noted that even if you purchase a professionally compiled list, it is still your responsibility to make sure that everyone on the list has, in fact, opted in.

This is more than simply good business etiquette—permission marketing is a very powerful marketing approach since every recipient has expressed at least some degree of interest in your company. Although they might not be considering buying from you right now but by expressing at least some level of interest they become warm leads. Choosing to opt-in to your list is the first step in customer engagement during which the seed of a potentially long-term and lucrative customer relationship is planted.

This permission-based approach is radically different from old-school direct mail marketing which is essentially cold-calling. In this case, direct mail is simply sent out to a “cold” list in hopes that at least some percentage—the industry typically hopes for about 2%—respond to the mailing.

Marketers who use direct mail don't use opt-in lists for several reasons. Direct mail is primarily regulated by postal regulations and mailing fees. This fact naturally serves to provide at least some degree of control over how much direct

mail is sent at any given time since few companies can afford to continuously flood the marketplace with unwanted mailings. Postage fees and printing costs take the place of laws to regulate the flow of direct mail.

However, email marketing has no such limitations. Spammers can—and often do—blast out millions upon millions of email messages at a very low cost, simply playing the odds that at least some of the recipients will act and buy. Because the investment is virtually zero, any sale is considered to be a positive return. As determined spammers became more aggressive and inboxes became flooded with unwanted emails, the public outcry over the rising tide of unwanted email messages began to resonate with legislators.

It was quickly becoming clear that email marketing was here to stay and that spammers were not going to alter or abate their business practices of their own accord. A concurrent problem was the flood of pornographic websites that began directly soliciting customers with x-rated—and unwanted—emails. The government decided to take action, and congress began working on legislation that would reduce the amount of unwanted spam by regulating email marketing practices while also addressing the pornography problem. The result was the CAN-SPAM Act.

### The CAN-SPAM Act Of 2003

---

In 2003, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. The cumbersome, formal title was turned into the rather interesting acronym that now identifies the act: CAN-SPAM.

Somewhat surprisingly, the CAN-SPAM act does not require companies to use an opt-in list. Instead, it gives broad and sweeping rights to the Internet Service Providers (ISPs) to filter and block emails virtually any way they see fit in order to comply with their internally established policies. This provision is absolute and does not require due process—if an ISP classifies your emails as spam, they—along with all of your other email correspondence—can be legally blocked, no questions asked. The government essentially transferred responsibility for policing the distribution of spam from itself to the ISPs. Email marketers can—and should—protect themselves from this provision by emailing only to properly acquired opt-in lists.

Probably the most important thing to know about CAN-SPAM is that it reaches far beyond pornography and even email marketing. CAN-SPAM applies to all commercial messages, defined as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,” including email that promotes content on commercial websites. In other words, the law applies to a very large percentage of your business email.

CAN-SPAM also has some teeth. Each separate email found in violation of the act is subject to penalties of up to \$16,000, which can quickly add up to a hefty cost for non-compliance. Potential fines scale in proportion to the size of your list.

Although the limiting provisions of the CAN-SPAM Act only apply to commercial messages, as we've seen, the definition of what constitutes a commercial message is very broad. It is also important to understand that a message need not be strictly a commercial message in order to be regulated by the Act.

The other types of email a business sends are defined as transactional and relationship messages. A transactional message refers to the details of a purchase that has either been agreed to or has already happened. Examples would be an invoice, a purchase confirmation, a response to a balance inquiry, a statement of account, a purchase order, or any other message that refers to a sale. A relationship message would refer to a warranty or claim, an existing contract of some form, a reference to a membership or subscription, as well as any other communication that refers to business dealings that are already in effect and that have been agreed to. Transactional and relationship messages are predicated on the assumption that business has already been conducted or that an agreement exists to conduct business; they are not solicitations to conduct new business.

You have to be careful though. Many companies often combine these kinds of messages with other commercial messages that are intended to promote or sell something else. When this happens, for the purposes of the CAN-SPAM Act, the entire message is deemed to be commercial in nature. In this case, all of the provisions of CAN-SPAM would then apply to the entire message. Simply adding a commercial message to an otherwise exempt email immediately makes it subject to CAN-SPAM.

## CAN-SPAM And What You Need To Know

---

Here are some important provisions of the law that you should be aware of, regardless of whether you are considering launching an email marketing campaign or simply want to ensure that your business-to-business emails stay within the law. This information is provided by the Federal Trade Commission (FTC), Bureau of Consumer Protection.

- ✔ Don't use false or misleading header information. Everything in the address header must accurately identify the person and the business sending the message
- ✔ Don't use deceptive subject lines. Like the header information, the subject line must accurately identify the contents of the message
- ✔ Identify the message as an ad. The Act provides a lot of flexibility with this provision in that the specifics are not spelled out in detail, but at some point you must clearly and conspicuously identify your message is a commercial solicitation
- ✔ Tell recipients where you are physically located. Your message must include a valid physical postal address where mail can actually be delivered. This can be a street address, a post office box, or a mailbox provided by a commercial service

- ✔ Tell recipients how to opt-out of receiving future emails from you. This is arguably one of the most critical provisions of the law. If a recipient can't easily figure out how to opt-out and files a complaint, your server can quickly be blacklisted. These instructions should be clear, concise, easy to read, easy to find, and easy to follow. It is also important to ensure that your spam filter doesn't block these opt-out requests when they are submitted to you
- ✔ Honor opt-out requests promptly. Opt-out requests must be accepted for at least 30 days following delivery of your message, and must be processed within 10 days of receipt of the request. You are not permitted to charge a fee or to request more information in order to process an opt-out request. Furthermore, once an opt-out request has been processed, you may no longer transfer or sell that address, even in the form of a mailing list to another company
- ✔ Monitor what others are doing on your behalf. Even if you outsource your email marketing function to another company, you are still responsible for compliance. Regardless of who sends a commercial message on your behalf, you cannot discharge your legal liability as established by CAN-SPAM

### The Black Hole Of Black Lists

---

The federal government is not the only entity that regulates spam. Despite the intent and relatively broad scope of the CAN-SPAM Act, the FTC has been, by most accounts, somewhat lax in its enforcement of the law. The potential fines—not to mention the adverse brand association that spammers typically generate—are sufficient to motivate most companies to comply voluntarily.

All of the major search engines including Google, Yahoo, and Microsoft's Bing maintain comprehensive databases of spammers and their originating email addresses. Emails originating from these "blacklisted" domains are automatically blocked, regardless of the nature of the content. This effectively puts non-compliant spammers out of business, at least temporarily, or until they come up with other, unknown email addresses to mail from.

These blacklists can pose a risk to you as well, however. Despite your best intentions, if you fail to comply with spam regulations—even if your non-compliance is accidental—it is highly likely that you will be blacklisted for an indeterminate period of time. This will in turn create some major operational headaches for your business since a blacklist does not differentiate between commercial, transactional, and relationship emails. Once your server is listed, no emails that anyone in your company sends will get through, regardless of the purpose or intent. Simply imagining what it would be like to run your business for even one day without the use of email gives you a glimpse of the severity of this potential problem.

Email marketing is a powerful tactic that is simply too powerful to ignore. As you develop your email marketing program, it is important to be fully aware of the CAN-SPAM Act but not to be intimidated by it. The legislation protects us all—nobody wants to see an inbox overflowing with annoying spam messages—and complying with its provisions is not difficult for a legitimate company selling legitimate products and services.

There are several things that a business can do to not only manage risk and ensure compliance, but to improve the overall effectiveness of the email marketing program.

- ✔ Start with high quality content—Make sure that every promotional email provides some type of useful information to the reader
- ✔ Conduct rigorous internal review—Successful email marketers rely on an internal team to review and edit each and every email marketing message that goes out. The team looks at content quality, grammar and spelling, message effectiveness, and anything else that can ensure compliance and just as importantly, increase open rates and response rates
- ✔ Use a spam checker—The final step should be running the message through any one of a number of available anti-spam programs specifically designed to ensure spam compliance. If your dealership uses an email marketing application to facilitate email marketing, the program almost invariably has an integrated spam checker. If you don't use an email marketing platform, there are a number of low-cost or even free spam checking applications available online
- ✔ Test, monitor, adjust, and repeat—One of the major advantages of email marketing over direct mail is the virtually instantaneous feedback you receive. Make it a point to test different versions of every message, monitor the results, make adjustments as necessary, and continue the process

The most important thing to remember though is that email marketing works, but compliance is essential. Be sure to include email marketing in your overall marketing mix, and then ensure that you manage the process closely.

**For more information about LEAF, visit us at [www.LEAFnow.com](http://www.LEAFnow.com)**