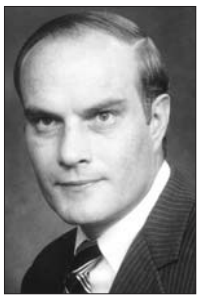

Technology Corner

By Joseph G. Hodges, Jr.

Spam and Junk Mail—When Will It Ever End?

You may ask, why would receiving too much spam and junk e-mail be of any consequence to the average estate planning professional?

Well, as you shall see by the time you finish reading this article, it is of significant consequence, especially given the current significant volume of this sort of stuff. It is particularly significant because of the way it adversely impacts our time online and the efficiency with which we normally like to deal with e-mail and Web sites in our work. This wasted time in turn translates into less time being available to us to perform our normal client billable work, not to mention to attend to all those things that are important to the success of our professional practices.

Now, it is important for you to understand at the outset that when I refer in this article to "spam" I do not mean SPAM, as spam in capital letters stands for the canned meat product that Hormel makes. Spam in small letters refers to what the Federal Trade Commission calls unsolicited commercial e-mail (UCE). This distinction is important because Hormel does not like the way some commercial companies are using its product brand name to describe their anti-spam software products. Currently, Hormel is suing SpamArrest. Will iHate Spam or others be next? The official word from Hormel is that they do not "object to use of this slang term to describe UCE, although we do object to the use of our product image in association with that term. Also, if the term is to be used, it should be used in all lowercase letters to distinguish it from our trademark SPAM, which should be used with all uppercase letters." You can't get more official than that, can you?

The Survey

Just how serious is this situation today? Well, in order to try and find out in a somewhat scientific way, a few months ago I asked the subscribers to various e-mail discussion lists, such as the ABA-PTL list, to compile a list of spam counts on their office PCs or networks for a one-week period of time and to send those counts to me so I could compile the results and analyze them for purposes of writing this article. Much to my surprise, I heard back from 38 list subscribers. While this is not a large sampling, I think this sample is large enough to be representative of what all of us are experiencing these days when it comes to spam. The results, while not scientific, are nonetheless both very revealing and rather scary.

The Survey Results

Counts were not recorded every day by all 38 respondents during the measuring period (which ran from Monday, July 14, through Tuesday, July 22), so the averages for some of the days—and particularly for Monday, July 14, Monday, July 21 and Tuesday, July 22, when the number of subscribers reporting were in the 10 to 18 range—may not be a fair reflection of the average counts on the other six days during the measuring week.

The daily counts from each subscriber varied significantly, all the way from as low as zero to three per day for some subscribers to as high as 550 on average for at least one subscriber. Judging from the individual comments of the subscribers about their particular e-mail systems and the various spam "filters" they and their IT Departments and/or ISPs were using, this diverse of a range in counts is explainable, with those using effective filters and blockers scoring the lowest counts. One missing statistic for those with low counts was how many of these spam messages were actually either being blocked from ever getting to them or were being placed into a trash or holding bin that they were not bothering to look at. (It could be a mistake not to check this holding bin in the event a message they

Joseph G. Hodges, Jr. is an attorney in Denver, Colorado and serves as Co-Chair of the ABA's Real Property, Probate and Trust Law Section Technology Committee.

might need ends up being blocked, as no filtering tool is 100 percent perfect.) Given this, it is probably fair to say that the systems of those with very low counts were actually receiving a much higher daily volume of this sort of message traffic if the counts of the other list subscribers are a fair indication of what is really going on out there and the problems this junk mail are causing. It does not matter whether this junk mail ends up on the individual user's PC, on the hard drives of the firm's server or on the servers or mainframes of the firm's ISP. It is still junk the user is receiving and the user is still being compelled to pay good money for this junk to be stored and/or dealt with by someone.

As for the actual survey, the average daily count for these ranged from a low of 38 per user per day to a high of 96 per user per day. The average for the survey week was 81 per user per day. The heaviest day was Monday, July 21, which is probably explained in part by the fact that the spammers tend to send most of this junk mail out either over the weekends or late at night when the blast mail servers they are using to do this are less likely to be busy with normal e-mail traffic and the overall e-mail traffic on the Internet is lower.

Perhaps what is most frightening—although not all that surprising given your author's typical daily volume of this sort of junk mail, not only during the survey week but prior to and since then—is that it was not a surprise to see that the average number of these messages that were received per day by this group of list subscribers was as high as 81. Even allowing for a survey sample error factor as high as 10 percent, this still leaves the average daily count per subscriber in the range of 70 messages per day. In my opinion, that level of volume for junk mail on a daily basis is way too high for any one of us to have to deal with on a regular basis.

How to Spot Junk Mail Easily

Perhaps the only saving grace in all of this for us is that most of these junk mail messages can be easily and quickly identified in most e-mail clients and summarily deleted for good from those systems just by glancing at who or where they are coming from and/or their rather strange subject lines.

For instance, here are some typical individual sender names you might see (note how these names are often slight misspellings of popular names): Juana, Jen, Krissie, Felix, Micah, Pandorella, and the well known Jenny Jones, among many others. These individual names even include such luminaries and lesser knowns as Reuben Kent, Jasmine Dickerson, Guadalupe Munson, etc. Even more obvious are sender names such as Ann's Free Gifts, Equlamail, Super Mail Contest, Super Email Bargain, Top Offers By Mail, Tax Relief Headquaters, No Prescription Necessary and many many others too numerous to mention here. Perhaps the most obvious are the "forged" domain names that are usually found in the headers and return e-mail addresses of these messages, many of which falsely appear as if they are coming from legitimate and popular e-mail domains such as AOL, Yahoo and MSN. A few typical examples are: *s188y4ax@uae.ac, s480mvf@aol.com, aywvf412e@ifluentialdelight.com, gq0ny2e6w@yahoo.com.hk, juana@hun-dinger.com, dkkcpps@msn.com, 3g00tis98@mailcity.com* (I think you get the general idea).

How Spammers Find Us

So, just how do these spammers find us in the first place? According to a recent Consumer Reports magazine investigation, spammers find us by capturing our e-mail address in four common ways.[1] One is by mining our e-mail address from public Web sites if we have it posted there. Those could be either Web sites we maintain ourselves or sites being hosted by professional and other organizations we belong to (unless these sites are configured to block any attempts to mine such information). A second common source is from e-mail chat rooms and e-mail discussion lists if we participate in those (unless those services have tools in place to block such address mining—most good ones do). A third is by what is commonly referred to as a "dictionary" attack whereby the spammer sends an e-mail message to a series of e-mail addresses using a combination of similar names and numbers in the hopes that yours is one of those and you will reply or even simply open the message to read it and thereby confirm that your address is a real one. A fourth is by the use of online registrations, especially with shopping sites that have either no privacy policy or one that clearly states (as many of them do) that they have your permission to send you more spam and even to sell your address to other "partner" spammers.

So How Do We Combat This Stuff?

That is not an easy question to answer, as the current solutions are not ideal, and there currently are over 200 software products on the market that claim to be able to help you filter out and/or eliminate this junk mail. However, we can gain some useful clues from a feature article entitled *E-Mail Spam—How to*

Stop It From Stalking You that was published in the August 2003 issue of CONSUMER REPORTS (hereinafter referred to as "CR").[2]

This well-written and easy to read article explains how spam finds you, suggests eight ways to block it and six common mistakes to avoid, and rates 11 popular spam-blocking software programs. This article also identifies some horrifying facts about spam. These include such things as the fact that the volume of spam throughout the Internet has grown to such an extent now that it is about to overtake that of legitimate e-mail (according to AOL, the volume of spam, which was below 500 million in the first quarter of 2002, had reached close to 2,500 million by the second quarter of 2003). Another is that a spammer can broadcast a million messages for as little as $500, and only needs a few people to respond and buy the offered goods in order for the campaign to pay for itself. Another is that, according to the Federal Trade Commission, nearly two-thirds of all spam messages contain false information, and only about one-third of consumer requests to be taken off the sender's mailing list are ever honored. Worse yet, CR found that spam-blocking software only works to varying degrees, with the highest recognition rate of the 11 products they tested being 90 percent.

As for legislative solutions, CR reports that, as of press time for their August 2003 article, while 33 states had laws regulating spam, many of those laws were not very effective or simply require the spammer to label the message as an ad. The state of Virginia seems to be an exception to this, as their law provides for up to five years in jail for spammers who send out more than 10,000 deceptive messages in a single day. Also, the Attorney General of California recently won a $2 million judgment against a Los Angeles marketer that specialized in selling how-to-spam books over the Internet under a recently enacted law that bars companies from barraging computer users with unwanted e-mail sales messages. On the federal front, things look equally dismal, as there currently is no federal anti-spam law in place in spite of the fact that several bills have been proposed, although one with some promise (if it is not blocked by the U.S. House) was approved by the U.S. Senate on October 22, 2003, by a vote of 97 to 0. This bill (1) prohibits spammers from disguising their identity through the use of false return e-mail addresses or misleading subject lines, (2) prohibits spammers from harvesting e-mail addresses from Web sites, and (3) creates a do-not-spam list that is similar in concept to the current (and possibly unconstitutional) federal do-not-call list. Given the world-wide nature of the Internet and the fact that much of the spam mail we receive today comes to us from servers that are outside the jurisdiction of the law enforcement agencies and courts in the United States, it remains to be seen if any of these laws, if ever enacted, will truly be effective as a tool in fighting spam e-mails.

In the meantime, and while we wait for these laws to be passed and/or enforced, what is one to do to effectively combat spam? Well, maybe the solution suggested in the CR article is the best one, as they acknowledge the obvious—spammers need our orders and money in order to stay in business. CR's advice is clean and simple (perhaps too simple to be totally effective): "[D]on't buy anything sold through spam. Don't respond to spam. Don't even open it."

Spam Blocking—The Alternative Solution

Given that it is so difficult to stop spam from being sent to us in the first place, our best lines of defense may well be what we do with it once it arrives at our doorstep. This is where effective spam blocking alternatives come into play.

The first and best line of defense is to use an ISP that filters incoming e-mails for spam, such as AOL, MSN or Earthlink, although the degree to which these services effectively filter out this stuff has been open to debate, at least in the past. These days, they all claim to have effective tools for doing this, although they often charge an extra fee for such services. Also, they all allow you to set up your own user-defined e-mail filters, which can be somewhat effective in certain cases but certainly are not an ultimate solution.

Your next best line of defense is to use spam-blocking software (which is discussed further below), as some of these products were shown by CR's recent tests to be up to 90 percent effective in identifying and filtering out spam messages.

The next best line of defense is either to avoid posting your e-mail address on public Web sites or using it in chat rooms and on discussion lists, or to obtain a secondary public or alias e-mail address that you use just for those purposes. You can obtain free e-mail addresses from providers such as Yahoo and Hotmail, or you can use a disposable address such as those that are now being offered by Yahoo or a forwarding service such as *www.SpamMotel.com.*

The next best line of defense is to simply delete all the spam messages you receive without even reading or opening them. The efficiency of this method can

be improved significantly by using the e-mail "rules" or "filters" that come with most of the popular e-mail client software programs so that at least the bulk of this junk mail will end up in its own separate bin for easy scanning for good messages that accidentally were sent there too. Also, it is vital that you not respond to those "unsubscribe" instructions that typically are a part of these messages, as that simply allows the spammer to confirm that your e-mail address is in fact working and is a good address for purposes of future spamming.

The last best line of defense is to make good use of your state and any federal laws against such spam, as well as the services of the Federal Trade Commission, especially if any frauds that have been committed against you as a result of your receipt of such junk mail. In fact, the FTC invites you to forward your spam messages to them at *uce@ftc.gov* ("uce" stands for unsolicited commercial e-mail) so they can more effectively monitor and attack this stuff.

Spam-Blocking Software

There are a variety of software solutions, some of which are good, some of which are bad, and a lot of which are offered by the spammers themselves who are in the business of selling such stuff. Moreover, the cost can range from free or a nominal fee to several thousand dollars, depending on the level of security and screening you want and whether that screening is going to take place on your individual PC or on your firm's or an ISP network server.

One caution here is *do not* purchase or use any of the spam-blocking software that is offered to you through one of those spam messages. Not only are you likely to loose your money and never receive the advertised product but, even if you do receive it, the seller will have thereby captured your e-mail address and other vital information and likely will soon be reselling it to other spammers.

Consumer Reports tested and rated 11 spam-blocking software products for their August 2003 report. Nine of those were add-on products that are designed to be used with an e-mail program, while the other two were e-mail programs themselves that are equipped to recognize and filter out spam without the need for additional software. The products in the latter category were Microsoft Outlook and Apple's Mac OS X-Mail. Sadly, if you use AOL, MSN or a Web-based service like Yahoo or Hotmail, none of the add-ons that CR tested can filter your e-mail unaided, although there is a special version of Spam Inspector available for AOL users. However, you can make some of these add-ons compatible with those services by using Web2Pop (available from *www.jmasoftware.com*) with a considerable amount of extra effort.

There is not enough space in this column to allow for an in-depth examination of each of these software programs, so reference should be made to the CR article itself for the details. The add-on software products that were tested were:

- SAProxy by Stata Labs—*www.bloomba.com*
- SpamCatcher Universal by Mailshell—*www.mailshell.com*
- Spam Sleuth by Blue Squirrel—*www.bluesquirrel.com*
- Spam Alert by Symantec—*www.symantec.com*
- Matador by MailFrontier—*www.mailfrontier.com*
- iHateSpam by Sunbelt Software—*www.sunbeltsoftware.com*
- MailWasher Pro by FireTrust—*www.firetrust.com*
- SpamKiller by McAfee—*www.mcafee.com*
- Spam Subtract by InterMute—*www.spamsubtract.com*

The CR editors came up with two recommendations, depending on how computer savvy you are. If you feel you are a knowledgeable computer user and you are willing to put up with the detailed installation instructions, they recommend SAProxy, which, while it is free and maintained by volunteers, has an online database of known spammers that is constantly being updated. If ease of use and installation are more your cup of tea, they recommend one of three products, all of which cost under $100: SpamCatcher, Spam Sleuth and Symantec's Spam Alert, the latter of which is only sold as part of the Norton Internet Security 2003 software package. They particularly liked SpamCatcher and Spam Sleuth because these products automatically consult online databases as they work, plus Spam Sleuth learns from experience as the spammers change their spamming tactics.

Interestingly, the July 31 issue of PC World's Deal Watcher e-newsletter reported under the 10 top downloads for that week that SpamCatcher was in fourth place, with products like Ad-aware, Spybot Search and Destroy and Pop-Up Stopper, all of which are specifically designed to attack pop-ups versus spam e-mails, occupying the first three places.[3] Also, PC Magazine awarded iHateSpam for Outlook as a Best Buy in their May 2003 issue.[4]

A few additional spam-blocker software products that I learned about while working on this article are Postini by Postini, Inc., which is available from *www.estreet.com*, the Google Toolbar at *www.toolbar.google.com* (which offers some interesting possibilities for both spam blocking and pop-up management), Spam Remedy by DarkSoft Group (which relies on message content versus just key words in order to do its spam filtering), SpamCop, Spam Arrest (which stores the spam messages on its own Web site for a period of seven days), Spam Slayer and SpamNet Outlook. NEWSWEEK magazine listed over 200 such products in its November 11, 2002, issue, so there are plenty of options available.[5] However, I recommend you use one that is well known and has proven itself to be effective.

This Issue's Featured Web Sites

- **IRS Announcement 2003-56**—Fiscal year 2002–2003 estates should see this announcement for special rules for filing Schedule D (Form 1041), Capital Gains and Losses, and Form 1041, U.S. Income Tax Return for Estates and Trusts. *www.irs.ustreas.gov/formspubs/article/0,,id=112807,00.html*
- **IRS Tax Scams/Consumer Alerts**—*www.irs.gov/newsroom/article/0,,id=98269,00.html*
- ***2002–2003 Guide To Internet Research* by Glenn S. Bacal Esq.**—*www.ali-aba.org/aliaba/glenbacal_2002.htm*
- **May (Insert Name Here) Rest in Peace**—Purchase your own professionally pre-written eulogies for only $25 U.S. *www.speech-writers.com/funerals.htm*

ENDNOTES

1 *E-mail Spam—How to Stop It from Stalking You,* CONSUMER REPORTS, Aug. 2003, at 12.
2 *Id.*
3 *See www.pcworld.com/downloads/index.asp.*
4 Daniel Tynan, *Natural Born Spam Killers,* PC WORLD, May 2003.
5 Brad Stone, *Technology: The New Spam Blockers,* NEWSWEEK, Nov. 11, 2002.