call thousands of residential phone numbers? When the consumer complaints begin to mount, why not just change your name and continue business as usual?

Messaging abuse threatens the vitality of online commerce and infringes on consumers' privacy. I applaud MAAWG's efforts to combat messaging abuse through industry collaboration and the advocacy of technological solutions.

At the FTC, we share [illegible]

[2] *See* Press Release, "FTC Asks Court to Shut Down Text Messaging Spammer" (Feb. 23, 2011), *available at* http://ftc.gov/opa/2011/02/loan.shtm.

determining the scope of Flora's text messaging scheme, but a 40 day snapshot into his actions reveals the breadth of his activities, and how much havoc just one person can wreck. Using 32 pre-paid cell phones, Flora blasted over 5 million text messages — almost a million a week --- typically advertising loan modification or debt relief services. To transmit this many messages, Flora needed to send, on average, 85 messages per minute around the clock.

Flora sent email spam to consumers, advertising his text message blasting services. In these emails, Flora offered to send 100,000 text messages for only $300.

Many consumers who received Flora's text messages had to pay a per-message fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans. While the financial injury suffered by any consumer may be small, the aggregate injury is likely quite large. And, even for tho

In June 2009, however, members of the anti-spam community gave the Commission evidence about a rogue Internet Service Provider based in California, but controlled by overseas criminals. The ISP, 3FN, recruited and willingly hosted a massive amount of malicious electronic content, including child pornography, malware, phishing sites, and the servers that control botnets. In just two weeks, the FTC filed an enforcement action and obtained a TRO requiring the data centers where 3FN's servers were located to disconnect the servers from the Internet. According to statistics published by Google, the shutdown of 3FN resulted in a temporary 30% drop in worldwide spam levels. Ultimately, the Court issued a Default Judgment against the Defendant and ordered disgorgement in excess of $1 million.[3] This was the first time in FTC history that the Commission used its authority under Section 5 to shut down an ISP.

3. Misuse of pop-ups and banner ads

Scammers have found numerous other ways to trick consumers into paying money. For instance, in December 2008, the FTC sued Innovative Marketing, Inc., the corporate centerpiece of a massive, deceptive advertising scheme that flooded the Internet with more than one billion deceptive ads, ensnared millions of domestic and foreign consumer victims, and caused more than $163 million in consumer injury.[4] For more than five years, the Defendants marketed a wide range of computer security products to consumers. To frighten and intimidate consumers into purchasing these products, the Defendants relied on deceptive advertising that featured convincing, but utterly bogus, system scans that purported to scan consumers' computers for

---

[3] *See* Press Release, "FTC Permanently Shuts Down Notorious Rogue Internet Service Provider" (May 19, 2010), *available at* http://www.ftc.gov/opa/2010/05/perm.shtm.

[4] *See* Press Release, "Court Halts Bogus Computer Scans" (Dec. 10, 2008), *available at* http://www.ftc.gov/opa/2008/12/winsoftware.shtm.

obtained the call recipient's prior signed, written agreement to receive such calls from that seller.[5] An "established business relationship" does not provide a basis for placing a robocall.

The new r

[5] *See* 73 Fed. Reg. 51,163 (2008).

[6] *See* 71 Fed. Reg. 58,715, 58,718 (2006) and 69 Fed. Reg. 67,287, 67,288-89 (2004).

requiring a technological solution. The protocol for email allows for the spoofing of the "from" line, making it exceedingly difficult for receiving ISPs to determine whether a message is truly from the purported sender.

The FTC first advised Congress that domain level authentication showed promise as an anti-spam technology in 2004. Seven years have now passed since the Commission first called for the wide scale deployment of domain level authentication. I know that MAAWG has been helping lead this charge. It's time to make this happen. All outbound email needs to be authenticated. And receiving ISPs need to start rejecting unauthenticated messages or filtering them more aggressively. Only when there is a truly functioning authentication system in place can other anti-spam technologies (such as reputation services) function effectively.

2. Mobile Lab

The FTC's advocacy, enforcement, and rule making depend on the agency investing in new technologies and providing its investigators with necessary tools. For several years, the FTC has investigated online frauds using its Internet Lab, a facility jammed with computers with IP addresses that are not assigned to the government and with evidence capturing software.

We are now broadening our ability to investigate mobile devices. The statistics tell the story. Cell phone ownership has risen dramatically in the U.S. over the past decade and now 82% of American adults own a cell phone, Blackberry, iPhone or other device that is also a cellphone. More and more mobile subscribers are using smartphones (rather than feature phones) that allow users to access the web and email on the go and run a host of applications and smartphones will soon overtake feature phones in the U.S. market.

Corporations are using the mobile medium to reach consumers, whether it is to provide services or content, or to market their products. Just this month, one company predicted that

U.S. mobile advertising spending will reach 5 billion dollars by 2015.[7] Consumers can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase. Consumers can search mobile web sites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. Consumers can download mobile applications that perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, or calculating tips or debts. They can also play interactive games containing targeted advertising. This market is exploding with new options for consumers and businesses.

New technology can bring tremendous benefits to consumers, but it also can bring new concerns and provide a platform for old frauds to resurface. The mobile marketplace is no different. The FTC Act applies whether a company is marketing via the traditional telephone, the television, the desktop computer, or a mobile device. The important principle to remember, however, is that the same rules of the road apply. Marketing must not be deceptive or unfair. Marketers should not mislead consumers about what they are downloading on their mobile devices or treat them unfairly. Consumers should have clear information so they can make informed choices.

The FTC is ensuring that it has the tools necessary to respond to the growth of mobile commerce and conduct mobile-related investigations. Last year the FTC's Bureau of

---

[7] Leena Rao, "Smaato: U.S. Will Spend $5 Billion On Mobile Advertising In 2015," TechCrunch (Nov. 2, 2010), *available at* http://techcrunch.com/2010/11/02/smaato-u-s-will-spend-5-billion-on-mobile-advertising-in-2015/.

Consumer Protection created a Mobile Lab – a gadget-lover's dream-house stocked with mobile devices on various platforms and carriers and evidence-capturing equipment and software. With these additions, FTC staff has improved its ability to conduct research and investigations into a wide range of issues in the mobile space. I have also assembled a team to stay abreast of the new developments in m

[8] *See* Press Release, "Public Relations Firm to Settle FTC Charges That It Advertised Clients' Gaming Apps through Misleading Online Endorsements" (August 26 2010), *available at* http://www.ftc.gov/opa/2010/08/reverb.shtm.

OnGuardOnline.gov, which we manage, is a partnership of fourteen federal agencies, including all the heavy hitters in the realm of cybersecurity. The site – which gets more than two million unique visits each year – has materials you can use for your company's education programs, including advice on avoiding phishing attacks, scams and malware. Feel free to copy and distribute any of the OnGuard Online articles, videos and games for your clients and staff.

In 2008, Congress asked us to expand the OnGuardOnline.gov project to cover online safety for kids. In response, we developed a guide for parents, *Net Cetera: Chatting with Kids About Being Online*. Since October 2009, the FTC has distributed over seven million copies of the guide. Seven million!

Last year, we released the *Net Cetera Community Outreach Toolkit*. Each toolkit includes:

1. our guide for parents – *Chatting with Kids About Being Online*
2. a booklet for kids called *Heads Up*, with advice on dealing with cyberbullies, texting, file sharing, and using mobile phones
3. and videos, presentation slides and discussion guides to help you share this important information with your friends, family, coworkers and clients.

The other site I encourage you to bookmark is business.ftc.gov, the BCP Business Center. There you'll find practical compliance guidance on online advertising, privacy, data security, and other need-to-know topics for business people.

Many of the most popular pages on the Business Center deal with topics of interest to MAAWG members. Our CAN-SPAM Act compliance guide is the most viewed page on the site. And if you're responsible for data security, you'll want to check out our short video about Peer to Peer File Sharing. The resources on the BCP Business Center are yours to share.

doesn't cut it. That's especially true when personal information about children is being collected and shared.

The order requires EchoMetrix not to use or share the information it obtained through its Sentry parental monitoring program — or any similar program — for any purpose other than use by a registered user. The order also requires the company to destroy the information it had transferred from Sentry to its marketing database.

The FTC has also aggressively enforced data security laws. We've now brought 32 data security cases, ranging f Sentry

[10] The resellers are SettlementOne Credit Corporation and its parent company, Sackett National Holdings Inc.; ACRAnet Inc.; Fajilan and Associates Inc., doing business as Statewide Credit Services; and Robert Fajilan. *See* Press Release, "Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal

B. Non-Enforcement Initiatives

In addition to our enforcement efforts, the agency is also engaged in broader privacy initiatives. First, we're reviewing our Children's Online Privacy Protection Act rule to see if it has withstood the test of time. We are examining a number of questions: Does it provides adequate protection in light of significant changes in the marketplace affecting kids, such as the explosive growth in the use of social networking and smartphones and the development of technologies such as interactive TVs? Does COPPA's coverage of websites located on the Internet and online services reach the kinds of electronic media children use today? How should we address the collection of mobile geolocation data or information collected in connection with online behavioral advertising under the Rule? What about online gaming sites? Should they be covered? Are the methods for verifying parental consent, such as usin0 0 1 0 0 0 0 TD(nta)Tj 0.h

Information" (Feb. 3, 2011), *available at* http://www.ftc.gov/opa/2011/02/settlement.shtm.

We're also looking at ways to address concerns raised at the roundtables about the roles of data brokers, most of which have no direct interaction with consumers but collect and compile storehouses of data about consumers from myriad sources. Some panelists at the roundtables suggested that consumers should get access to their data as a means of improving transparency, while others discussed the costs of providing access and recommended that any access should vary with the sensitivity of the data and its intended use. Access is an important ingredient in accountability. The Report addresses this issue as well.

The Report also addresses the viability of some kind of universal mechanism, a one-stop-shop where consumers can register a preference not to be tracked, or not be targeted for online ads, and where marketers would have to respect such preferences. There have already been efforts to allow — by browsers and companies — to give consumers tools to indicate that they don't want to be tracked, or to adjust or tweak how they're tracked. These efforts are laudable. It is hard to say, though, how consumers will respond if many different associations, companies, and groups offer different options in different formats. A Do Not Track option against can simplify consumer choice.