An Ounce of Outreach is Worth a Pound of Enforcement

By B. Chad Bungard

Advances in communications and technology have granted people real-time access to information through social networking, mobile applications and traditional Web browsers. These days, we would much rather click a mouse or swipe a touchscreen than grab a book from the shelf. This trend has had a seismic impact on American society; as a sign of the times, the Encyclopedia Britannica—an iconic publication—recently discontinued printing hard copies after more than two centuries.¹

There were 215 million Americans actively² using the Internet in August 2011,³ according to recent Nielsen Internet usage data. During that same month, Google and Yahoo! experienced 176 million and 149 million unique visitors, respectively.⁴ A 2010 Pew Internet and American Life Project Report revealed, “Americans are turning in large numbers to government websites to access information and services” and “typically rely on search engines to guide them to their destination when seeking government information online.”⁵ According to the report, 41 percent of Americans have downloaded government forms.⁶

Scam artists are well aware of these staggering numbers. It was only a matter of time before unscrupulous individuals targeted the Social Security Administration—an agency that touches the lives of virtually every American. SSA issues a Social Security number to all U.S. citizens, permanent residents⁷ and temporary working residents, and SSA benefit payments serve as the financial lifeline to many Americans.⁸

“...Americans are turning in large numbers to government websites to access information and services...”

THE NET FORMS SCHEME
In 2009 and 2010, a Google or Yahoo! search for a “new or replacement Social Security card” would likely have led consumers to the website, ssnhome.com (pictured). The site appeared at or near the top of the search results in the sponsored section of both the Google and Yahoo! search engines.

The sleek site greeted visitors with the prominent words, “Social Security Home,” an eagle logo, and a subtle image of the U.S. flag at the top of the webpage. An official-sounding slogan, “Securing America’s Promise,” sat above two large images of a Form SS-5, SSA’s Application for a Social Security Card. The site displayed many Social Security-related words and phrases, and featured “statement of earnings” and “eligibility quiz” tabs. The site offered the consumer the ability to download the SS-5 form and avoid long lines by applying from home. It also contained images of three official federal government logos: the White House, USA.gov and SSA. A click on the first two logos took the consumer directly to the official sites; the SSA logo,

³) Nielsen estimates that Americans on average spent more than 30 hours on the Internet during August 2011 and visited 99 different websites. Nielsen also estimates that 275 million Americans had access to the Internet during that same period. Nielsen Wire, supra note 3.
⁴) Id.
⁶) Id.
⁸) As of Dec. 21, 2011, 55.4 million individuals were receiving Social Security benefits. See http://www.ssa.gov/OACT/STATS/OASIDBenef.html. See also U.S. Seniors Assoc., Inc. v. SSA, 423 F.3d 397, 497 (4th Cir. 2005) (“The government has a substantial interest in protecting Social Security, as the financial lifeline of most senior Americans, and it has a strong interest in protecting Social Security recipients from deceptive mailings”). It is also important to note that SSA offers a robust Internet presence, offering comprehensive program information and publications, Social Security forms, and the ability to file for Social Security benefits online at www.socialsecurity.gov.
however, was not an operational link—leaving individuals with the impression that they were already on SSA’s official site.

The problem: the website was a fake and fooled thousands of people. Net Forms, LLC, a Houston-based company, operated ssnhome.com as part of a deceptive, profit-seeking scheme by luring unsuspecting consumers into purchasing the Form SS-5. SSA provides the SS-5 at no cost on its website, accessible at www.socialsecurity.gov or www.ssa.gov, as well as at all SSA field offices and other SSA-approved locations across the country. Net Forms purchased more than a million dollars of online advertising services from Google and Yahoo! to ensure that online searches for terms related to obtaining a new or replacement Social Security card would direct potential customers to ssnhome.com. Net Forms accumulated significant revenues from its sale of the SS-5; fees reached as high as $29.99 and often unbeknownst to the consumer, the site also charged a $9.99 automatically renewable annual membership fee.

THE LAW
In 1988, to combat a rise in deceptive mailings targeting seniors, Congress enacted Section 1140 of the Social Security Act—a provision prohibiting the misuse of words, letters, symbols and emblems of SSA.9 This provided SSA with a consumer protection tool against misleading advertising. As the Fourth Circuit Court of Appeals recognized in United Seniors Ass’n, Inc. v. SSA, “[i]n passing Section 1140, Congress sought to protect Social Security recipients from potential identity theft, from spending their Social Security benefits on organizations camouflaging as governmental entities and from endless solicitations.”10

In particular, Section 1140 protects SSA’s brand by prohibiting the use of SSA words and symbols in advertisements, solicitations or other communications in a manner that conveys the false impression that such item is approved, endorsed or authorized by SSA, or that such person has some connection with or authorization from SSA.11 It also prohibits the fee-based reproduction, reprinting or distribution of SSA forms, applications or other publications without authorization from SSA.12 For these prohibitions, Congress made clear that the use of a disclaimer is not a defense.13 This was because, as noted in the legislative history, “[m]any consumers do not read, or cannot read, disclaimers.”14 In 2004, Congress amended Section 1140 to also prohibit providing services for a fee that are available directly from SSA free of charge, without the use of a prominent disclaimer that the product is available free of charge by SSA.15

The Social Security Administration’s Office of the Inspector General aggressively enforces Section 1140. The statute provides for as much as $5,000 in civil monetary penalties for each separate violation of the Social Security Act.16 Entities are subject to a separate penalty for each time an individual visited (or viewed) a website in violation of Section 1140 or purchased an SSA form that was sold without proper authorization. The Social Security Act also provides that a penalty of as much as $25,000 may be imposed for each time a violating broadcast or telecast is viewed.17 Penalties collected for violations of Section 1140 are deposited into SSA’s Old-Age and Survivors Trust Fund.18

Congress initially enacted Section 1140 to combat misleading insurance marketing tactics—often referred to as “lead card” mailings.19 This scam typically involved a lead company sending misleading solicitations to senior citizens to lure them into completing a reply card and forwarding highly sensitive personal information to the company. This lead company would market this sensitive data to insurance companies, which in turn, would solicit

---

9) 42 U.S.C. § 1320b-10, as implemented by 20 C.F.R. part 498.
10) 423 F.3d. 397, 399 (4th Cir. 2005).
11) 42 U.S.C. § 1320b-10, as implemented by 20 C.F.R. part 498.
16) 42 U.S.C. § 1320b-10(b)(1).
17) 42 U.S.C. § 1320b-10(b)(2).
18) 42 U.S.C. § 1320b-10(c)(2).
seniors to purchase burial and other private insurance policies. Through our aggressive enforcement efforts over the years, including countless hours of investigations and litigation, these deceptive SSA-related mailings are now rare. However, as the Net Forms case illustrates, we are now confronting a new breed of misleading SSA-related advertising via the Internet.

NET FORMS: CASE RESOLUTION
Net Forms went to great lengths to shield its identity and relationship with its SS-5 website operation. Because of the covert nature in which Net Forms operated, we had concerns the company would shelter its assets from the government’s reach when it became aware of the investigation. Therefore, in partnership with the U.S. Attorney’s Office, Southern District of Texas, we requested and the court granted, ex parte injunctive relief prohibiting Net Forms from operating its SS-5 websites and freezing significant Net Forms assets. We reached a settlement agreement in which Net Forms agreed to permanently shut down its SS-5 website operation and pay a $325,000 penalty into the trust fund, representing a disgorgement of its net profits.

OUTREACH EFFORTS
As the Net Forms case wore on, tying up significant resources, we realized that we could not rely solely on litigation to stem the ever-increasing tide of Social Security-related Internet fraud. During the nine months investigating and litigating the Net Forms case, the number of allegations of similarly fraudulent website operations grew exponentially.

At the beginning of fiscal year 2012, the SSA OIG Office of the Counsel to the Inspector General initiated an outreach program to combat the alarming increase of Internet-based violations of Section 1140. To combat this fraud, we met with senior officials from Google, Yahoo!, Microsoft (Bing), GoDaddy, web.com, Demand Media, Discover, JPMorgan Chase, eBay/PayPal, Visa, MasterCard and American Express. Our goal was to educate these companies about Section 1140, discuss how website operators are using the Internet (and their services) to commit fraud in violation of Section 1140 and discuss ways that we could work together. This outreach effort is helping us successfully fight this fraud using a multipronged approach, which has five key elements.

ELEMENT 1: LEARN THE GAME
The outreach meetings provided us with valuable insight and knowledge of some of the key technical aspects of how individuals use legitimate business methods to lure unsuspecting customers. For example, we learned that it is a common practice to use more than one URL (or domain name) to direct traffic to a particular website. These additional URLs, referred to as display URLs, allow website operators to increase their presence in Internet searches and direct more traffic and ultimately more business to their destination URL.

ELEMENT 2: DEVELOP RELATIONSHIPS WITH KEY CONTACTS
We developed key contacts to help us gather information quickly and expedite action. Several companies have worked with us to establish mechanisms to identify the website operators quickly, halt these schemes and even prevent such activities from starting. It used to take us up to several months to discover who was operating a particular website; it can now take only hours. We have also shut down a website within just a few days of learning of its operation; this was not possible before the outreach began.

ELEMENT 3: FIND COMMON GROUND
We conveyed to each company why it was smart business to be proactive in fighting Social Security-related fraud. Working with us would not only protect the Social Security brand and protect millions of consumers, but the company’s own brand was also at stake if it conducted business with fraudulent entities. Soon, after we met with one credit card company, and it created a filtering system, with our assistance, to identify websites immediately that may violate Section 1140 and that accept (or purport to accept) its credit cards as a form of payment. The company refers all websites
that it identifies through this filtering system to SSA OIG for review. This proactive method has allowed us to take immediate action to shut down upstart websites operating in violation of Section 1140. For example, we took action against two North Carolina-based sites, socialsecuritycardservice.com and social-security-card-now.com, in just a few short weeks from notification; the website operator immediately agreed to cease its violative operations.

ELEMENT 4: CHANGE THE PLAYING FIELD
Based on our outreach efforts, Google and Microsoft (which powers both its Bing and Yahoo! search engines) modified their AdWords Terms and Conditions and Ad Content and Style Guidelines polices, respectively, to protect its users from advertisements, websites and businesses that create the false impression of a connection with a governmental agency. These new policies could be extremely effective in preventing individuals and entities from deceiving SSA consumers using Google’s and Microsoft’s advertisement services.

Google also took quick action to discontinue its ongoing advertising relationships with two Internet companies—Bennett & Gray, LLC and SimpleFilings—until it was satisfied the sites were no longer acting in violation of Section 1140. Bennett & Gray of Lindon, Utah, agreed to pay a $50,000 civil monetary penalty to settle our claim that the company violated Section 1140. The company operated the websites, www.sscards.us and www.sscardapplication.com, which offered for a fee, assistance in applying for a new or replacement Social Security card. We determined that the websites’ design, along with related domain names, created the false impression of a connection with SSA. Bennett & Gray voluntarily redesigned its website operation to bring it into compliance with Section 1140, and agreed to discontinue the use of the domain names www.sscards.us and www.sscardapplication.com.

Similarly, SimpleFilings agreed to discontinue the use of the domain names, gov-tax.net/sss-card and simplefilings.gov-tax.net/sss-card, which we deemed to be in violation of Section 1140, voluntarily made changes to its website to further clarify its services and agreed to pay an $82,000 civil monetary penalty to settle our claim that the company violated Section 1140. We received a significant number of complaints of consumer confusion caused by the use of these domain names.

“The results...”

ELEMENT 5: CUT OFF THE MONEY SUPPLY
Previously, we spent months investigating violative websites only to learn that they operated overseas—likely out of our reach to shut the websites down and impose Section 1140 penalties. However, by working closely with financial institutions, we have been able to effectively combat even overseas-based schemes without jurisdictional impediment. Financial institutions have moved responsibly and quickly to stop accepting funds from sites that we have deemed are operating in violation of Section 1140. Cutting off the money supply provides a quick end to the fraudulent activity; some sites have shut down within hours after financial institutions refused to process their payments.

THE RESULTS
In the first few months of fiscal year 2012, through aggressive enforcement and outreach efforts, our office halted 18 Internet-based fraud schemes that we determined were operating in violation of Section 1140. One of the sites, SocialSecurityCardService.com (pictured on page 18), followed a typical blueprint of deception for SS-5 scams. These sites...
typically included official-looking logos and images of the U.S. flag, Social Security cards and SS-5 applications; they also often used deceptive domain names that implied a false SSA connection.

CONCLUSION
Protecting the SSA brand ultimately protects SSA consumers. Collaborating with the entities that can stop fraud in its tracks is not only cost-effective, but it can also prevent fraud from ever occurring. This public/private sector endeavor is proving to be a powerful one-two punch against Internet scams. To date, our outreach efforts have stopped 18 violative Internet operations in less time than it took to shut down the Net Forms website scheme. This kind of enforcement action quickly gets noticed; unscrupulous individuals will think twice before expending resources to set up a fraudulent operation, and legitimate businesses will ensure due diligence in complying with Section 1140. The tremendous success of our outreach program in just a short time demonstrates how an ounce of outreach is worth a pound of enforcement.

ACKNOWLEDGMENTS
The author would like to thank David Rodriguez, attorney, Office of the Counsel to the Inspector General, SSA OIG; Tracy Lynge, deputy assistant inspector general for external relations, SSA OIG; and Andrew Cannarsa, public affairs specialist, SSA OIG, for their significant efforts in the development and drafting of this article. The author would also like to thank David Rodriguez, Sandi Archibald, attorney, and Erin Justice, acting associate counsel for CMP Litigation for their creativity and innovation in uncharted territory, through their significant roles in the development and implementation of the outreach program. Mr. Rodriguez, Ms. Archibald and Ms. Justice have made a significant contribution towards protecting the public from fraud.

B. Chad Bungard
B. Chad Bungard serves as the counsel to the inspector general for the Social Security Administration, where he provides executive leadership as the chief legal advisor to the inspector general and senior staff. He is also responsible for administering the Civil Monetary Penalty Program, including the imposition of penalties and assessments, and the settlement and litigation of CMP cases. Prior to serving in this position, Bungard has held several positions. Most recently, Bungard served as the general counsel of the Merit Systems Protection Board, where he served as the chief legal advisor and chief legal representative.

Bungard received his Bachelor of Science degree cum laude from Liberty University, Juris Doctor degree from Regent University School of Law and Master of Laws degree in Law and Economics from George Mason University School of Law. He has been published in numerous legal publications, including the UCLA Entertainment Law Review, the Seton Hall Legislative Journal and the University of North Carolina First Amendment Law Review. He was also recognized as a practitioner contributor in the 9th Edition of Black's Law Dictionary.