



May 27, 2015

National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230
Via email to securityRFC2015@ntia.doc.gov

Re: Comments in Response to the Request for Public Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

Docket No. 150312253–5253–01

The Recording Industry Association of America (RIAA) hereby submits these comments in connection with the above referenced matter. The RIAA is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members comprise the most vibrant record industry in the world. RIAA members create, manufacture and/or distribute approximately 85% of all legitimate recorded music produced and sold in the United States. In support of this mission, the RIAA works to protect the intellectual property and First Amendment rights of artists and music labels; conduct consumer, industry and technical research; and monitor and review state and federal laws, regulations and policies. As such, we and our members are key stakeholders in the digital ecosystem.

Our members, and their consumers, have both benefitted greatly from an online distribution ecosystem for our members' products and services, but have also been harmed via that ecosystem. As others have noted, “[w]hile the diversity within the technology industry enables innovation and low prices, it also increases the chances of tainted, counterfeit, and malicious goods entering the market.”¹ Similarly, as online demand for our products and services has grown, so have criminal enterprises that want to illegally profit from that demand.

¹ See D. Inserra et al, “*Cyber Supply Chain Security: A Crucial Step toward U.S. Security, Prosperity, and Freedom in Cyberspace*”, March 6, 2014, available at <http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.

Often that criminal activity takes the form of offering infringing or counterfeit goods and services. This, in and of itself, is a type of cybercrime that should be deterred, and everyone in the Internet ecosystem has a role in addressing and deterring such activity. While several voluntary initiatives have been implemented to address this, more can and should be done.²

In addition, this criminal activity also often takes the form of scams, malvertising, malware or other malicious activity intended to either trick users into downloading unwanted and damaging software to their computers or to engage in identity theft. Consider, for example, the following:

- A study by Incopro from March of this year found that in reviewing the advertisements on 250 popular piracy sites, “just under one-third of the total number of ‘adverts’ viewed in this study were in the trick button/malware category, where a click on the ‘advert’ could potentially infect the user’s computer with malware and bots, potentially perpetrating fraud and possibly compromising user data.”³
- In 2014, a working paper from the Association of Internet Security Professionals reported that “[f]rom botnets to DDoS attacks, video streaming has become the number one method to propagate highly dangerous malware on the Internet.”⁴
- A 2014 report from the Heritage Foundation found that counterfeit software frequently threatens cybersecurity because such software is often accompanied by malware and often directs the user to dangerous websites. The report noted that “[w]hile too few studies exist to fully analyze the international scope of this problem, clearly software counterfeiting is a serious and costly cybersecurity threat.”⁵
- This month, Digital Citizens Alliance released a report that found that of the 589 sites engaged in infringement that it reviewed, one third of them included links with the potential to infect users’ computers with viruses or other malware.⁶ The report noted that “[i]n most cases, the links are hidden behind download or play buttons, but in many cases, it is not even necessary to click on a link to spawn the unwanted download.”⁷

² See, e.g., Statement of Cary H. Sherman Chairman and CEO Recording Industry Association of America, before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet, September 18, 2013, available at http://judiciary.house.gov/files/hearings/113th/09182013_02/091813%20Testimony%20of%20Cary%20Sherman.pdf, and Statement for the Record of Cary Sherman, Chairman and CEO, Recording Industry Association of America on “Section 512 of Title 17” before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet, March 13, 2014, available at <http://judiciary.house.gov/cache/files/22c3acda-551c-41ba-b330-8dd251dd15fd/113-86-87151.pdf>.

³ See <http://www.incopro.co.uk/wp-content/uploads/2015/05/Revenue-Sources-for-Copyright-Infringing-Sites-in-EU-March-2015.pdf>.

⁴ See AISP Working Paper, “Illegal Streaming and Cyber Security Risks: A Dangerous Status Quo?”, Autumn 2014, available at <http://cryptome.org/2014/09/illegal-streaming-malware-epoch-times-full-14-0923.pdf>.

⁵ See D. Inerra et al, “Cyber Supply Chain Security: A Crucial Step toward U.S. Security, Prosperity, and Freedom in Cyberspace”, March 6, 2014, available at <http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.

⁶ See Digital Citizens Alliance, “*Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business, A Follow-Up to the 2014 Report on the Profitability of Ad-Supported Content Theft*”, May 2015, available at <https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/298a8ec6-ceb0-4543-bb0a-edc80b63f511.pdf>.

⁷ Id., p2.

- Several other recent articles continue to note the tie between cybersecurity vulnerabilities for users and businesses and sites that offer pirated or counterfeit goods and services.⁸

To illustrate this point, note what has happened with a rogue site associated with the trademark GrooveShark. The original site, GrooveShark.com, was an infringing music site that was found to willfully infringe our members' copyrights by a court of law. As soon as GrooveShark.com was disabled, a rogue operator started a copycat site called GrooveShark.io. That domain (and related domains) was also suspended, and the site currently operates at GrooveShark.li. When one searches for content on GrooveShark.li, the user is directed to download unrelated, unrequested and unwanted software. The site operators of the copycat GrooveShark site are simply trading on the name GrooveShark to attract users, and engaging in domain hopping when one of the domains is suspended. This creates significant harm in terms of continued cybercrime and increased cyber-vulnerabilities for users.

In short, as noted above, rogue operators use the offer of infringing versions of our members' sound recordings and music videos as the "candy" to attract users that are necessary for them to create and exploit cyber vulnerabilities. In light of this, any discussion addressing malvertising or trusted downloads should also address some of the roots of these problems. These include the sites and applications that engage in pervasive copyright infringement, and the way criminals that operate these sites and applications exploit the public's desire for content to further the criminals' illegal activities.

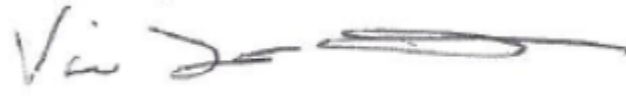
We are sure that there are several proposals that might be worthy of discussion to address malware and trusted downloads, particularly as it relates to sites and applications offering music or music videos. In any event, consideration of copyright, and the practical and ongoing threats posed by those engaged in copyright infringement are central to this discussion. Our collective goal should be to achieve the proper balance between promoting competition online and ensuring the Internet remains a safe and vibrant ecosystem for legitimate commerce without undue risk from cyber-threats and cybercrime.

⁸ See, e.g., SpamFighter News, "Incopro says that Top Piracy Sites in UK Contain Malware and Scams", May 5, 2014, available at <http://www.spamfighter.com/News-18969-Incopro-says-that-Top-Piracy-Sites-in-UK-Contain-Malware-and-Scams.htm>; Computer Weekly, "Malware in counterfeit software to cost business \$114bn in 2013", March 25, 2013, available at <http://www.computerweekly.com/news/2240180104/Malware-in-counterfeit-software-to-cost-business-144bn-in-2013>; Computer Weekly, "Pirated software malware to cost business \$491bn in 2014, study shows", March 19, 2014, available at <http://www.computerweekly.com/news/2240216380/Pirated-software-malware-to-cost-business-491-in-2014-study-shows>; and LastLine Labs, "Rogue Online Pharmacies Use Fake Security Seals and Content Obfuscation to Deceive Humans and Programs", September 17, 2014, available at <http://labs.lastline.com/rogue-online-pharmacies-use-fake-security-seals-and-content-obfuscation>.

We thank NTIA for looking into this matter, and for convening a process to address these concerns.

Respectfully submitted,

RECORDING INDUSTRY ASSOCIATION OF AMERICA

A handwritten signature in black ink, appearing to read "Vic Sheckler", with a long horizontal flourish extending to the right.

Victoria Sheckler
Senior Vice President, Deputy General Counsel
1025 F St., NW, 10th Floor
Washington, DC 20004