Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Combating False Celebrity Endorsements Online

By **Marc Rachman, Brooke Singer and Claudia Cohen** (June 7, 2019, 12:04 PM EDT)

Marc Rachman

Brooke Singer

Claudia Cohen

Dr. Mehmet Oz, the celebrity surgeon and television host, recently co-authored an op-ed piece for The Wall Street Journal addressing the proliferation of false celebrity ads on Facebook and how these ads are deceiving consumers and harming the reputation of the celebrities involved.[1] Dr. Oz is not the only celebrity facing this issue. Others include Kelly Ripa, Denzel Washington, Bill Gates, Barbara Corcoran, and Will Ferrell, to name a few.[2]

What has celebrities so upset is not only that their fans are being duped, but also that the online social media platforms where many of these fake ads appear often do not police themselves to catch these deceptive ads before they are posted.

One of the reasons for the reluctance of social media platforms to take proactive measures to address these deceptive postings is that the platforms are often immune from liability under Section 230 of the Communications Decency Act of 1996.[3] This provision protects social media websites and other internet service providers from liability for content created by others that they simply host.

For example, in a recent decision by the U.S. Court of Appeals for the Second Circuit in Herrick v. Grindr LLC,[4] the plaintiff sued Grindr, a gay dating and social networking application, after his ex-boyfriend created fake Grindr profiles impersonating him that led to numerous Grinder users reaching out to him and trying to meet him in person. The plaintiff alleged that Grindr, among other things, had failed to take steps to stop his ex-boyfriend from abusing its platform.

In upholding the trial court's dismissal of the action, the Second Circuit found that Section 230 of the CDA shielded Grindr from liability because Grindr, like Facebook, is an interactive computer service that provides subscribers with access to a common server; the plaintiff's claims were based on information provided by a third-party user; and the plaintiff was improperly treating Grindr as the publisher or speaker of content.

Fake online celebrity ads are pervasive and run the gamut as to the products being sold, often with initial "free" trial offers that are really negative options that lead to recurring monthly charges that are difficult to cancel. Many of these scams are for health supplements and skincare

products that purport to cure cancer and other diseases, relieve pain, cause weight loss, or prevent aging.

Stopping the bad actors behind these false celebrity and brand endorsements and holding them accountable is challenging because of the extensive steps they take to avoid detection. This is done in a myriad of ways, including providing false contact information on their websites and to their domain name registrars, registering their domain names using privacy protection services, and cloaking the fake ads being delivered from third-party intermediaries who are used in connection with the publication of the ads. Coupled with these tactics is the deliberately deceptive format used in the ads themselves.

Many of these ads are made to look like real news reports, including the unauthorized use of various media brands in the domain name itself and in the heading of the ad (e.g., CNN, ABC News, Forbes, etc.), as well as the placement of the ads on social media platforms like Facebook and Twitter in ways designed to make them appear to be organic posts rather than paid advertisements.

Despite the challenges of pursuing social media websites for hosting these false celebrity and brand endorsements, there are still ways to find and hold responsible the marketers behind them. And while the Federal Trade Commission has successfully pursued these marketers under the FTC Act over the past few years,[5] private lawsuits for false advertising, trademark infringement and right of publicity violations are also a viable option.

As discussed below, there are various strategies that can be employed to unmask these bad actors and hold them accountable for their infringing conduct.

**The Challenges in Identifying the Responsible Bad Actors**

There are many barriers to identifying the bad actors responsible for fake advertisements. As an initial matter, although the false ads contain offers for specific products, there may be multiple companies or individuals involved in their creation and publication. The typical scenario is that the advertiser's website, which is usually the landing page where the product is sold, contains no infringing content. Rather, the false ad is actually published by a third party who is engaged through what is referred to as an affiliate network.

The affiliate network acts as the intermediary between the advertiser and the publisher of the ad. In some affiliate networks, the advertiser is not given access to the identity of the affiliate publishers that are creating the ads. Rather, the affiliate network maintains this information and only provides the advertiser with a number, typically referred to as an "affiliate ID," to distinguish the different affiliates in its network that are publishing ads for the advertiser. Adding additional opacity to this arrangement, the actual infringing content published by the affiliate could have been created by the affiliate, the affiliate network, the advertiser, or another third party.

Not all advertising placed through affiliate networks is unlawful, and not all affiliate networks and publishers are engaged in these unscrupulous acts. However, the setup for how ads are published through affiliate networks allows for those looking to engage in deceptive marketing to do so in ways designed to avoid detection.

One method to achieve anonymity is the use of third-party domain privacy services. The contact information for the holder of a domain name may be publicly available online by using the Internet Corporation for Assigned Names and Numbers' WHOIS search[6] or another similar search function.[7] A

holder that uses its domain for a website where fake advertisements are posted will often pay a privacy service to act as the "registrant" of the domain. The privacy service then registers the domain under its name, and the result is that only the privacy service's identity and contact information are publicly accessible. The privacy service must be contacted in order to identify the domain holder, but the privacy service may not respond to such a request or may require the issuance of a valid subpoena before doing so.

In addition, with the recent advent of the EU General Data Protection Regulation, there is frequently redaction of identifying information that previously would otherwise have been available through a WHOIS search. Nevertheless, privacy services are still being used to further conceal identifying information concerning the registrant.

Another strategy employed to evade detection is the use of false contact information. The domain holder may give false contact information to the domain privacy service it uses to register its domain. Also, the domain holder who operates a website where fake advertisements are posted may include false contact information on its own website. In addition, an affiliate publisher in an affiliate network who engages in infringing conduct may provide false or limited contact information (i.e., solely an email address) to the affiliate network.

Further, operators of websites (whether that is the advertiser, affiliate network or affiliate publisher) that publish false advertisements also have advanced tools at their disposal to obscure their infringing conduct. For example, they may use "redirect URLs" to hide the origin of infringing advertisements: When a user attempts to access the URL where a fake advertisement was previously posted, the user's browser automatically and instantly redirects them to a different URL that does not show the fake advertisement or the URL where the fake advertisement resides.

Another tactic employed is to cause the URL used to host infringing content to have a short life span, such that a user who once accessed infringing content at that URL cannot access that content again there a few days later. Then there is what is referred to as "cloaking": Through internet protocol address detection, two different versions of the URL are displayed — an infringing version and a noninfringing version — and only the noninfringing version appears when certain parties seek to view the ad (e.g., an affiliate can cloak the ad, so the affiliate network and the advertiser do not see it).[8]

**Strategies to Address Online False Celebrity and Brand Advertisements**

While these efforts to avoid detection are frustrating, there are still ways to successfully identify, stop and hold accountable advertisers, affiliate networks, and affiliate publishers involved in the creation, publication, and use of false online celebrity and brand endorsements.

As an initial matter, sending cease-and-desist letters can be a cost-effective strategy to quickly halt these online false advertisements. Recipients of cease-and-desist letters can include (to the extent known): (1) the registrars of domains for websites that host the false advertisements, and the privacy services used by the registrant; (2) the advertisers of the products featured in the false advertisements; and (3) the affiliate networks involved in the false advertisements.

Relatedly, submitting takedown notices to social media websites that host false advertisements that infringe registered trademarks and copyrights is often a fruitful way to have this content removed. Having registrations for trademarks and copyrights is an important step in this process as takedown procedures often require proof of ownership through such registrations.

In addition, digital advertising tracking services can provide invaluable data about online affiliate marketing campaigns. These services collect the campaign name, affiliate network, publisher and advertiser involved in the campaign, referring URLs used in the campaign, and even images of advertisements used in the campaign. Once armed with this information, more targeted cease-and-desist letters can be sent to capture all parties involved in the dissemination of the infringing content, including the affiliate network that has direct contact with the affiliate publisher.

A more involved, but often effective, strategy involves the institution of John Doe lawsuits, which provide subpoena power to identify the unknown defendants behind the false advertisements. Third-party subpoenas are often necessary to obtain information from domain privacy protection services, social media websites, affiliate networks, and tracking services. We recently found success with such tactics in an action brought by the celebrity talk show host Montel Williams in Montel Williams et al. v. Advanceable Technology LLC et al.[9] In that case, which was commenced in the United States District Court for the Southern District of Florida, Williams sought the identity of parties responsible for online advertisements that falsely claimed he endorsed their CBD oil products.[10]

Information that can be obtained through third-party subpoenas includes what are referred to as "click reports" and "conversion reports" for marketing campaigns run through affiliate networks. Such reports are generated by affiliate marketing tracking software, which is typically used by, and in the possession of, affiliate networks to track their campaigns.

Click report data includes the dates that consumers clicked on advertisements in the campaign; the affiliate ID and/or affiliate name for the affiliate publisher in the campaign; the advertiser's name; the campaign name; and the referrer or referral URLs, which are the URLs where the advertisements in the campaign were posted. Conversion reports list similar data and also show the dates that consumers purchased the advertised product, as well as the dollar amount of the purchases and the referral fees paid to the affiliates.

A referrer or referral URL used in a marketing campaign often actually includes a celebrity's name (e.g., xyz.com/montel-williams), which is a clear indication that a fake advertisement featuring the celebrity was posted on that URL. Because click and conversion reports show the affiliate ID that used that URL and the advertiser for whom the campaign was run, a targeted third-party subpoena to the appropriate affiliate network can be issued requesting the identity of and contact information for a specific affiliate by their affiliate ID based upon the data obtained through the conversion and click reports. Once uncovered, the party that published the infringing ad can be directly approached to seek appropriate remedial action.

**Conclusion**

It is often worth conducting an investigation to determine the source of online false advertisements that use a celebrity or brand. Before instituting litigation, cease-and-desist letters and takedown requests are important, cost-effective tools to stop these false advertisements. If such prelitigation efforts are unsuccessful, instituting a "John Doe" litigation may bring results through the use of strategically targeted third-party subpoenas.

---

*Marc J. Rachman and Brooke Erdos Singer are partners and Claudia G. Cohen is an associate at Davis & Gilbert LLP.*

***Disclosure: The authors of this article recently represented Montel Williams and Montel Williams Enterprises Inc. in the referenced lawsuit Montel Williams et al. v. Advanceable Technology LLC et al. Rachman and Singer have also represented Dr. Mehmet Oz in false endorsement matters.***

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] Mehmet Oz and Kai Falkenberg, Facebook's Scandal of Fake Celebrity Ads, The Wall Street Journal (Apr. 14, 2019 3:26 p.m. ET), https://www.wsj.com/articles/facebooks-scandal-of-fake-celebrity-ads-11555270000.

[2] Oz and Falkenberg, supra note 1; Lesley Fair, Fauxmats, false claims, phony celebrity endorsements, and unauthorized charges, FTC Business Blog (Nov. 16, 2017 10:03 a.m.), https://www.ftc.gov/news-events/blogs/business-blog/2017/11/fauxmats-false-claims-phony-celebrity-endorsements.

[3] 47 U.S.C. § 230.

[4] See Herrick v. Grindr LLC, 18-396, 2019 U.S. App. LEXIS 9318 (2d Cir. Mar. 27, 2019).

[5] See, e.g., FTC v. LeadClick Media, LLC, 838 F.3d 158, 170-72 (2d Cir. 2016) (holding affiliate network directly liable under Section 5 of the FTC Act for deceptive false news websites published by its affiliate publishers); see also FTC v. Tarr Inc., Case No. 3:17-cv-02024-LAB-KSC, Complaint (S.D. Cal. Oct. 3, 2017) (complaint under the FTC Act against defendants for, among other things, their use of affiliate networks in deceptive advertising that contained fabricated celebrity endorsements); FTC v. Tarr Inc., Case No. 3:17-cv-02024-LAB-KSC, Stipulated Order for Permanent Injunction and Monetary Judgment Against All Defendants (S.D. Cal. Nov. 14, 2017) (settlement ordering, among other things, that (i) defendants were permanently banned from certain sales practice, including deceptive advertising using false endorsements, and (ii) a judgment of $179 million be entered in favor of the FTC against defendants, which was suspended upon defendants' payment of about $6.4 million paid to the FTC upon defendants' relinquishment of title to assets held by payment processors).

[6] See ICANN WHOIS, https://whois.icann.org/en (last visited May 3, 2019).

[7] See, e.g., Domain Tools Whois Lookup, http://whois.domaintools.com/ (last visited June 4, 2019).

[8] See Wikipedia, https://en.wikipedia.org/wiki/Cloaking (last visited June 4, 2019).

[9] Montel Williams et al. v. Advanceable Technology, LLC et al., Case No. 1:17-cv-23942-KMW (S.D. Fla.).

[10] Adam Lidgett, Montel Williams Settles with CBD Cos. to End Likeness Row, Law360 (Apr. 3, 2019, 5:52 p.m. ET), https://www.law360.com/articles/1146120/montel-williams-settles-with-cbd-cos-to-end-likeness-row.