Crowell

CLIENT ALERT

Four Health Care Company v. John Doe Cases: Scare Tactics, Accidental Disclosures, Hacking, and Impersonation Lead to Loss of Anonymity

August 3, 2017

The health care industry has seen more than its share of defamation and intellectual property infringement cases. Many of these cases involve unknown persons hiding behind the anonymity of the internet and invoking the First Amendment to remain anonymous. All is not lost, however, for the victims of injurious speech and conduct by anonymous persons. As demonstrated by the following four health care cases, the First Amendment anonymity defense is surmountable.

- **Anonymous Drug Company Defamers**. Anonymous posters on a health website made alleged defamatory statements about a pharmaceutical company and its products, including accusations of criminal and unethical behavior. According to the company, the statements impacted participation in drug trials, FDA approvals, and business prospects by scaring others about the company's drugs. The company sued the John Doe posters for defamation and intentional interference with prospective business. It also filed an *ex parte* motion to discover the identities of the Does. The court granted the motion and allowed the company to serve a subpoena on the health website for discovery of the Does' names, addresses, phone numbers, e-mail addresses, and internet protocol addresses. In granting the motion, the court held that the company had met the two-part *Highfields* First Amendment test for the disclosure of anonymous speakers by establishing a *prima facie* case of defamation – indeed, the statements were defamatory *per se* – and identifying greater harm to the company than the Does would suffer by having their identities revealed. According to the court, "[d]enying this discovery would leave this wrong without any remedy." *OBI Pharma, Inc. v. Does*, No. 16-2218 (S.D. Cal. Apr. 27, 2017).

- **Anonymous Nursing Defamation 101**. Anonymous posters on a nursing community website made alleged defamatory statements about a nursing test prep company. The company sued the website, its founder, and the John Doe posters for defamation, consumer fraud, and trademark infringement. In discovery, the company unsuccessfully moved to compel the website to produce identifying information (*e.g.*, names, addresses, phone numbers, and internet protocol addresses and logs) for the Does. The court held that the company had failed to satisfy a *Dendrite*-type First Amendment test for the disclosure of anonymous speakers. But outside discovery, the company successfully identified some of the Does, in part due to their accidental disclosure of their real names on the public court docket. As a result, when the company later sought to amend its complaint to substitute real names for the Does, the court held that the company did not need to satisfy any First Amendment disclosure test. The First Amendment didn't apply. "The standard provided in the Court's prior order applies when a party is seeking discovery of … information that might unmask [an] anonymous speaker…. By the plain terms of the order, the standard does not apply to a motion seeking leave to add previously anonymous defendants to a complaint after the plaintiff discovers their identities." *East Coast Test Prep LLC v. Allnurses.com*, No. 15-3705 (D. Minn. May 22, 2017).

- **Hospital Hackers**. Anonymous hackers broke into a hospital's e-mail server and sent defamatory e-mails hospital-wide, comparing certain employees to Adolf Hitler and accusing other employees of sexual misconduct. The hospital and

targeted employees filed a defamation suit against the John Doe hackers and served subpoenas on internet service providers (ISPs) to reveal the identities of the Does. The Does moved to quash one of the outstanding subpoenas, claiming anonymity rights under the First Amendment. The trial court granted the motion, but the appellate court reversed and remanded for enforcement of the subpoena. It held that the four-part *Dendrite* First Amendment test for the disclosure of anonymous speakers should not be rigorously applied considering the unlawful mode of the Does' speech – this was not a case of anonymous persons posting statements on internet message boards – and the clearly defamatory statements. The appellate court also held that it didn't matter that enforcement of the subpoena may lead to the discovery of additional anonymous speakers and other statements (defamatory or not). *Warren Hosp. v. Does*, 63 A.3d 246 (N.J. Super. 2013).

- **Fake Drug Company News**. "Neil Herson" wrote comments on a news website falsely trashing the financials of a major pharmaceutical company. Company executive Neil Herson, however, didn't write the comments – imposters did. So the company initiated pre-complaint discovery against the John Doe imposters and served subpoenas for their identities on the news website and a related ISP. The ISP demanded a court order to comply with the subpoena. The trial court issued that order following briefing and argument by the company and the Does. It rejected arguments that the Does' identities were protected by the First Amendment: First Amendment protections would be available only to anonymous or pseudonymous speakers, not impersonating speakers. The appellate court agreed, holding that "[n]or were the comments anonymous or pseudonymous, which are the only categories of commentary clearly protected by the case law…." Accordingly, the court dismissed the Does' appeal for lack of jurisdiction given that they could not maintain that the disclosure order affected constitutional rights – in other words, the Does had no constitutional rights in their misappropriation conduct to argue the disclosure order was immediately appealable as a collateral order. *AmerisourceBergen Corp. v. Doe*, 81 A.3d 921 (Pa. Super. 2013).

These internet defamation cases present interesting First Amendment issues in the anonymity context. While some other anonymous defendant cases go the other way, health care entities can mount strong arguments that the First Amendment doesn't apply, or that if it does the plaintiff has satisfied the First Amendment tests for disclosure of the defendant's identity.

And it certainly helps the plaintiff's case when the anonymous defendant abuses his constitutional rights by making false criminal or unethical accusations, engages in wrongful conduct by hacking computer systems or impersonating others, or waives his anonymity by disclosing his real identity.

Crowell & Moring's cyber reputation attorneys have a broad array of capabilities to investigate, defend against, and fight back high-profile online reputational attacks.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Troy A. Barsky
Partner & CHS Managing Director – Washington, D.C.
Phone: +1.202.624.2890
Email: tbarsky@crowell.com

Christopher Flynn
Partner – Washington, D.C.

Phone: +1.202.624.2864
Email: cflynn@crowell.com

Clifford J. Zatz
Partner – Washington, D.C.
Phone: +1.202.624.2810
Email: czatz@crowell.com