

Avoid Being Hijacked on the Information Superhighway

If a Client's Online Identity is Being Misused, Counsel Must Act Fast to Mitigate Damage

July 13, 2009

Michigan Lawyers Weekly

VOL. 23, NO. 34

By Carol Lundberg

Technology

Don Tanner and Matt Friedman have no idea how many people saw the messages sent from the imposter Twitter account, the one that impersonated them and their firm, Tanner Friedman Strategic Communications.

They have no idea if it cost them any business.

They just know that by next week, they'll have to decide whether they're taking further legal action against the person- who works for a competitor- who used the social networking site to try to make them look like fools.

"What we're seeing is a sort of an online land grab coming on," said Christopher A. Mitchell, an intellectual property lawyer at Butzel Long's Ann Arbor office.

He's seen it before, when the Internet was the new big thing, and people would "cybersquat," or register as the owner of a domain name (or more typically, thousands of domain names) such as www.johnsmith.com or www.coke.com, which might be of interest to people or corporate entities.

Cybersquatting had trailed off after the passage of the federal Anticybersquatting Consumer Protection Act, but social networking is bringing misuse of domain names and usernames back to the forefront, Mitchell said.

"It's basically the wild west of the Internet," said John C. Blattner, Mitchell's colleague at Butzel Long. "Facebook and Twitter have opened new frontiers on the same battle."

In Tanner Friedman's case, the person who created the bogus Twitter account was sending messages that, for example, were about how to use social media, the type of information they would actually post online.

"But they twisted it to make us look bad," he said. "They would include links to different articles to make us look bad. Or they had included information about a past client, and linked us to that client to make it seem like we were connected to a very public issue this client was having."

A Matter of Defamation

The Farmington Hills-based firm discovered what had happened in March.

"When we started on Twitter, we set up individual accounts, but it exploded quickly to become a means of corporate communication," Friedman said. "By the time it had become that, our name had been hijacked."

They later learned that the impostor was sending out phony messages (tweets) for three months- an eternity in the life of social media.

First they tried to contact Twitter to see if the username could be shut down.

That was exactly the right thing to do, said Kathryn L. Ossian, of the Detroit office of Miller, Canfield, Paddock & Stone PLC.

She's seeing an increase in the number of businesses whose corporate identities are being hijacked or misrepresented online. She said it's because sites such as



Don Tanner, left, and Matt Friedman, right, called their lawyer Daniel P. Dalton, center, when they discovered someone had been impersonating the firm of Tanner Friedman Strategic Communications on Twitter.

Twitter are so easy to use and are anonymous.

"These sites are free, and anyone can sign up for accounts without having to give information like credit card information," Ossian said.

But the site's terms of service or terms of use do prohibit illegal or unauthorized use, and Twitter specifically states that users are not allowed to impersonate another person or business, she said.

So the fastest course of action when such a discovery is made is to report a terms of service violation, which will immediately shut down the phony user until the details can be sorted out, she said.

It may take persistence to get through to someone at Twitter.

"But you can't call anyone on the phone. They have 60 million users and 40 employees," Friedman said.

Once they got through to someone at Twitter; the username was shut down.

Then the partners called their lawyer.

The hijacking can be described as defamation, which covers libel and slander, unauthorized use, or trademark and copyright infringement, said Daniel P. Dalton, of Royal Oak-based Tomkiw Dalton Attorneys at Law, who is representing Tanner Friedman.

It was never Tanner Friedman's intent to sue Twitter, Dalton said. Even if that's what they wanted to do, they couldn't, because the Computer Fraud Act protects providers such as Twitter.

"Twitter is basically just a provider, and is not responsible for content," he said.

What Tanner and Friedman really wanted was to get the impostor user shut down, and to get control over the Twitter username "@TannerFriedman."

So Dalton determined that the best way to proceed was to file an action against John Doe, since he didn't know yet who had misused the Tanner Friedman name, and subpoena Twitter to get the information about where and when the Twitter username was generated.

"It's like when you file a Bivens Action, where the plaintiff was raided and arrested by six unknown DEA agents, and had to sue John Doe 1, John Doe 2, John Doe 3, and so forth, in order to find out what happened," Dalton said.

Fighting for Control

Dalton filed the suit and a motion for discovery in federal court May 27. The order was granted June 7, and the court issued the subpoena.

But Twitter didn't respond. So Dalton filed a motion to compel.

"Then Twitter faxed us the information we were looking for," Dalton said.

Twitter sent the Internet protocol address where the username was originated, and the e-mail account name used to generate the username. The account name was of no help,

because it was a nondescript name by a free Internet service.

"The IP address was the most important thing. We gave it to an IT expert, and he did a reverse lookup and it showed Marx Layne Public Relations," Dalton said.

Then Tanner Friedman asked the firm's internal IT expert to also look up the address, and he got the same result.

Michael Layne of Marx Layne Marketing & Public Relations in Farmington Hills said his firm is investigating the matter, and will take appropriate action, as it has in the past when company computers were used inappropriately.

Even though Dalton had the information his clients wanted, at that point Tanner Friedman didn't yet have control of the @TannerFriedman Twitter username and corresponding Web page.

Dalton sent Twitter a letter to compel them to allow Tanner Friedman to have the username and page, and 24 hours later, Tanner Friedman was given control of the page.

The firm quickly set up the Twitter profile page.

The partners say they had plenty of time to think about what they wanted and sent out their first tweet: "Yes, it's really us."

In hindsight, Tanner and Friedman admit they weren't thinking ahead, and should have acquired their Twitter username early, to keep a charlatan – or anyone else – from getting it.

Dalton said he advises his clients to regularly conduct informal audits of various networking sites, and the Internet, to be sure that no one is using a name similar to their corporate names.

"If the name is taken, you should find out who has it and determine if we can secure it," he said. "Even if we can't secure it, you should be aware of what's going on with that Web site."

If a client has been what Dalton called "Twitterjacked," he has urgent advice: "Take action now. The longer you wait, the less likely a judge will let you do anything about it."

Mill Canfield's Ossian agrees.

"Obviously, the best thing is to at least reserve your company's name as a placeholder. It's not always feasible to do that, or someone beat you to it," she said.

Blattner of Butzel Lond is still waiting to see what will be the result of the recent Facebook feature, launched in mid-June, which allowed users to create URLs that could include their names, such as www.facebook.com/johnsmith.

Facebook was allowing trademark holders to pre-block their marks so no one else would be able to use them.

"Facebook decided that it would let people pick whatever username they wanted, and it occurred to someone that trademark owners may have a problem with it," Blattner said. "So they sent out notice saying they would allow trademark owners to apply to pre-block such a use. But they didn't think this through very well, if at all."

"They were just inundated with pre-blocking requests. Their server crashed and they couldn't even begin to handle it."

Blattner filed dozens for his clients, and in some cases he got a response from Facebook. In other cases, he didn't.

"I've talked to other trademark attorneys, and that's been the universal experience," he said. "I guess we'll just have to wait to see if anything happens. It could be a total nightmare."

Online Paper Trail

Tanner and Friedman will have to decide if they care to pursue further legal action.

Ossian said the legal principles are the same for online infringement, misrepresentation, unfair competition, trademark, libel and slander, as they are offline.

Even though it may at first be difficult to determine who the defendant is, because the person has made efforts to be anonymous, once the person is found, building a case is in some ways easier when the offense occurred online.

“You have all this documentation of every message that was sent, and when it was sent,” she said.

As for who’s responsible – the competing firm or a rogue employee – it depends, Ossian added.

“Obviously, they’re saying that they didn’t authorize or condone this behavior. And that’s a potential risk a company takes when its employees are out there on the Internet,” she said.

“But one question that will be asked is, does the employer discourage it? There could be an argument for vicarious liability. At least if they have a policy on the books, they can point to that policy and say, ‘We prohibit it.’”

Layne said his firm does have a policy that prohibits inappropriate computer use. But it’s still a challenge, because he works with individuals.

“Of course we don’t condone this kind of activity,” Layne said. “I can also say that most agencies, like ours with over 40 computers with access to the Internet, are challenged by having an open system where the employees have unrestricted access to the Internet.” ■

If you would like to comment on this story, please contact Carol Lundberg at (248) 865-3105 or carol.lundberg@mi.lawyersweekly.com.