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

How Law Firms Can Fight Back Against Fake Websites

By **Aebra Coe**

Law360 (April 4, 2018, 12:12 PM EDT) -- Impostors who clone law firm websites or pretend to be lawyers in order to scam the public have come out of the woodwork in recent years, leaving many firms wondering what they can do to protect themselves from the same fate.

Last year, the Houston Bar Association filed a lawsuit claiming an entity calling itself Walsh & Padilla PLLC stole the identity and images of several actual attorneys and used them to create a "sham" website to defraud elderly individuals in the United States and Canada, an illegal ploy that highlights a not-uncommon problem surrounding alleged fraud against legal consumers across the globe.

In addition to the case in Texas, there have been reports of fake lawyer and fake law firm websites in, among other places, New York, California, Colorado and Maryland, and outside the U.S. in the U.K. and Canada.

"There's nothing to stop somebody from doing this and making themselves look as if they're a real law firm by taking pictures off the internet, downloading them and purporting to be someone else," said John Simek, vice president of Sensei Enterprises, a digital forensics, information technology and cybersecurity company.

Over the past several years, an IP boutique in New York filed a lawsuit claiming a website sprung up with a nearly identical domain name to its own that was used to intercept emails intended for the firm's lawyers and staff, a Canadian newspaper reported that plagiarized photos from a real law firm website were used to create the appearance of a legitimate Toronto law firm so that scammers could conduct a fraudulent real estate deal, and a high school graduate with no law degree set up a website pretending to be a lawyer and represented at least 50 bankruptcy clients in Maryland.

A law firm's reputation may be at stake if someone commits fraud using its identity, content or photos without its knowledge, Simek said, making it all the more important to monitor its online presence.

He suggests law firms at the very least set up Google alerts under the names of each of its lawyers, as well as for the name of the law firm, to track each time those names pop up on the internet.

"Like with anything you need to be vigilant and watch what's going on. Be aware of yourself and make sure you have those alerts or someone is monitoring your online presence," he said.

If a law firm detects someone is using its name, its logo, or the names or photos of its lawyers in order to perpetrate a fraudulent scheme, John Reed Stark, owner of a cybersecurity consulting firm and former longtime SEC enforcement attorney, suggests they should have a strong set of policies and procedures in place for what to do in each of those situations and not expect attorneys to handle the situation off the cuff.

"There should be centralized decision making for who's accountable when it happens," whether that's an internal employee or an outside expert, in order to take swift and uniform action, Stark said.

One action law firms can take is litigation. The lawsuit brought by the Houston Bar Association against the fake law firm Walsh & Padilla last year yielded a positive result.

According to Houston Bar Association president Alistair Dawson, a partner at Beck Redden LLP, the organization filed suit in federal court after it learned the alleged fraudsters' website had used a bar member's identity and images and had purported to be "endorsed" by the bar association.

The organization was able to quickly obtain a restraining order against the company that hosted the website, and within minutes of being handed the TRO, the South African host had removed the site from the internet.

"If you draft the order broadly enough to include the domain hosting companies you can send them a copy of the order and they'll take down the website," Dawson said. "Then you can decide if you want to pursue any further litigation after the immediate harm and immediate threat is eliminated."

According to Dawson, in another instance of a Houston lawyer whose identity had been used for a fake website, the victim simply had to threaten litigation to the web host and reference the Walsh Padilla case and was able to get the offending webpage removed.

"If you allow it to continue your reputation can be tarnished. I think you've got to be vigilant about it to shut it down from the very beginning," he said.

Another possibility for potentially preventing fake lawyer websites before they fool consumers is the adoption of a new top level domain, .law, which was launched in 2015.

Similarly to a .gov or .mil top level domain where authentication as a government or military entity is required, .law requires those registering a domain name to prove that they qualify to represent themselves as a law firm.

The private enterprise is run by a for-profit company, Dot Law Inc., that screens those applying for a .law domain name to ensure they are in fact a lawyer and are who they say they are, allowing consumers to know with certainty that the website belongs to an actual lawyer.

"The goal of creating .law was to create this environment on the internet where people had some sense of certainty they're dealing with actual attorneys," said CEO Lou Andreozzi.

According to Andreozzi, the idea is "starting to percolate" and the company has now sold approximately 15,000 website domain names, mostly in the U.S.

The success of the strategy in terms of a preventative measure for fake websites rests on its recognizability to the public and widespread adoption, something the company has not yet accomplished and is still working on.

"We don't see this as a quick home run, but we see it as a slow build over time, especially as new attorneys enter the field," he said of the domain's growth.

--Editing by Rebecca Flanagan and Emily Kokoll.

All Content © 2003-2018, Portfolio Media, Inc.