

Reproduced with permission from Electronic Commerce & Law Report, 21 ECLR, 1/6/16. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Cybersquatting

In Rem Federal Cybersquatting Suit Successful Against Unknown Foreign Hacker

BY ALEXIS KRAMER

A domain name registrant was entitled to relief under the in rem provisions of the federal Anticybersquatting Consumer Protection Act even though the registrant possessed only common law rights in the name, the U.S. District Court for the Eastern District of Virginia held Dec. 21 (*Watson v. Doe*, E.D. Va., No. 115cv00831, 12/21/15).

U.S. Magistrate Judge Michael S. Nachmanoff said the plaintiff's allegations that he had used the domain name in commerce since 1997 to provide information and services sufficiently created common law rights in the domain 256.com. Nachmanoff recommended an order directing the registrar to restore the plaintiff as the listed registrant of the domain name.

This ruling follows the court's earlier decision in *Acme Billing Co. v. Doe*, No. 1:14-cv-01379-LO-MSN (E.D. Va. 2015), which marked the first time a stolen domain name was recovered via the ACPA (20 ECLR 959, 7/15/15). In *Acme Billing*, the court ordered the return of an e-commerce company's stolen domain names based on allegations that Acme Billing had common law rights in the domain names due to use in commerce in connection with the sale of products and services.

On Dec. 8, the same court applied the reasoning of *Acme Billing* to another case, ordering the return of 12 stolen domain names, also based on alleged violations of common law rights (20 ECLR 1736, 12/16/15).

The ACPA permits actions to recover domain names that are identical or confusing similar to trademarks and used with bad faith intent to profit.

Applying Acme Billing. David Weslow, the plaintiff's counsel and a partner at Wiley Rein LLP in Washington, told Bloomberg BNA Dec. 22 that *Acme Billing* is a good roadmap for courts to follow when addressing domain name theft claims.

"Unfortunately, domain name theft continues to be a growing problem, and UDRP proceedings involving domain name thefts continue to yield mixed results," he said. "These cases demonstrate that there are legal claims that can be successfully used to recover stolen domain names."

Here, the plaintiff alleged that an unknown hacker gained unauthorized access to his domain name management account with eNom Inc. and transferred his 256.com domain name to another account.

The plaintiff brought an in rem action against the domain name itself, a novel cause of action created by the ACPA, 15 U.S.C. § 1125(d). The ACPA permits a trademark holder to file an in rem action against a domain name if it can't locate or obtain personal jurisdiction over the registrant of a name that violates its marks.

The plaintiff also filed a claim against the unknown individual under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, for the unauthorized access of Watson's domain name account to obtain registration information. The court rejected the CFAA claim due to a lack of factual allegations to support the claim or establish personal jurisdiction over the John Doe defendant.

Wiley Rein LLP represented Gray Watson.

To contact the reporter on this story: Alexis Kramer in Washington at akramer@bna.com

To contact the editor responsible for this story: Thomas O'Toole at totoole@bna.com

Full text at http://www.bloomberglaw.com/public/desktop/document/Watson_v_Doe_et_al_Docket_No_115cv00831_ED_Va_Jun_29_2015_Court_D/2?1450807182.