Bloomberg BNA

Electronic Commerce & Law Report™

Domain Names

Cybersquatting, Computer Fraud Laws Offer Hope for Domain Name Theft Victims

By Alexis Kramer

A typical domain name theft scenario goes something like this: the victim's registrar account is hacked, domain names are transferred to a different registrar outside the reach of U.S. courts, and all of the content on the victim's website vanishes from the Internet.

It is a crime for which there is no clear remedy, though one recently decided case from the Eastern District of Virginia, *Acme Billing Co. v. Doe*, provides a glimmer of hope for dispossessed owners of .com domains. In *Acme Billing*, the court asserted jurisdiction over the domain name itself and ordered a transfer from a Chinese registrar back to its rightful owner, based on a claimed violation of the Anticybersquatting Consumer Protection Act.

The ruling, the first and only published federal decision in which a stolen domain name was recovered via the ACPA, marks a promising path for similarly aggrieved domain name theft victims to follow.

Other potential remedies include claims under the Computer Fraud and Abuse Act, the ICANN-administered Uniform Domain Name Dispute Resolution Policy, and ICANN's Transfer Dispute Resolution Policy.

Illegal Domain Transfer Violates ACPA. In *Acme Billing Co. v. Doe*, E.D. Va., No. 1:14-cv-01379-LO-MSN, 5/18/15), e-commerce company Acme Billing Co. alleged that an unknown hacker gained unauthorized access to its domain name management account with GoDaddy and transferred 35 of its domain names to Chinese registrar eName Technology Co. Ltd. GoDaddy was only able to recover 21 of the 35 domain names.

Acme raised an in rem cybersquatting claim under the ACPA against the 14 remaining misappropriated domain names, and in the alternative, a claim under the CFAA, against the John Doe hacker (19 ECLR 1391, 10/29/14).

The federal district court said the domain names were transferred with the requisite bad faith intent to profit from the plaintiff's marks because the unknown hacker registered the domain names under false contact information, attempted to sell them back to Acme for financial gain and did not make a bona fide use of the marks. The unauthorized transfer, the court added, prevented Acme from exercising control over its domain names and caused confusion as to the source of the associated e-commerce websites.

In adopting a magistrate judge's recommendation, the court ordered the transfer of the domain names back to Acme based only on its ACPA claim.

David Weslow, a partner at Wiley Rein LLP in Washington, told Bloomberg BNA that claims under the ACPA have not been filed until this past year because victims of domain theft, for the most part, simply do not have the resources to file a lawsuit. He added that a claim under the CFAA is the best alternative to a federal cybersquatting claim in cases where a plaintiff's domain name does not qualify as a protected trademark under the ACPA.

Unauthorized Access to Steal Domain Violates CFAA. In *Consumer Source Holdings Inc. v. Does 1-24*, E.D. Va., No. 1:13cv1512, 6/30/14, the same district court held that the unauthorized access of a digital media company's domain name accounts for purposes of obtaining ownership of its domain names constituted a violation of the CFAA.

The court said that as a result of the unauthorized access and subsequent domain name transfer, the plaintiff lost control over its websites, spent resources investigating the incident and suffered damage to its goodwill and reputation.

Consumer Source Holdings Inc. alleged that unknown hackers unlawfully gained access to its domain name registration accounts and transferred its domain names to a registrar in China. The unknown John Doe defendants then added a registrar lock to the domain names to prevent their transfer back to Consumer Source.

Consumer Source alleged violations of both the ACPA and CFAA, but the court only addressed its CFAA claim.

Weslow recently filed a similar suit June 29, alleging violations of both the CFAA and ACPA for the illegal transfer of an individual's 256.com domain name to a Chinese registrar, resulting in the disabling of his control of the domain's associated website (*Watson v. Doe*, E.D. Va. , No. 1:15-cv-00831, complaint filed 6/29/15).

UDRP Not Envisioned for Theft. Prior to these decisions, some domain holders have pursued a different avenue to regain ownership of their stolen domains: ICANN's UDRP procedure.

In December 2014, a UDRP panel at the WIPO Arbitration and Mediation Center ruled that a hijacked domain name identical to a paint company's registered CIN mark was registered and used in bad faith because the domain name did not resolve to an active webpage (*Corporacao Industrial do Norte SA v. Huhan*, WIPO, No. D2014-1865, 12/30/14). The panel added that in its view, ‘‘proof of misappropriation of a domain name is sufficient proof by itself that the domain name has been registered and used in bad faith.’’

In May, a panel at the National Arbitration Forum held that an individual’s wrongful acquisition of a domain name identical to a software company’s GPZ mark did constitute bad faith registration and use because the disabling of the company’s website resulted in significant disruption of its e-mail access and ability to communicate with potential clients (*GPZ Technology Inc. v. Vedmidskiy*, Nat’l Arb. Forum, No. FA1504001612935, 5/11/15). ‘‘Previous panels have found that disruption of a Complainant’s business activities leads to a finding of bad faith,’’ the panel observed.

In contrast, a separate WIPO panel dismissed a claim that a hijacked domain name was registered and used in bad faith due to the facts that the case revolved around the question of who rightfully owned the domain name and that the primary purpose of the complaint was to recover stolen property (*Prince v. Echternach*, WIPO, No. D2010-1661, 11/26/10).

‘‘The Policy was designed to combat cybersquatting, the abusive registration and use of a domain name which is identical or confusingly similar with a trade mark to which the Complainant has rights... [It] was not designed nor is it equipped to decide whether the domain name was taken without the complainant’s knowledge or consent, involving as it does legal issues outside the Policy and credibility of competing testimony that a Policy panel is incapable of resolving,’’ the panel said.

Although at least two domain name owners succeeded in using this dispute resolution mechanism, Weslow said he does not believe the UDRP to be an appropriate vehicle for domain theft due to the sophistication of thieves and the difficulty in proving bad faith registration and use. Because hackers are aware that offering to sell their acquired domain names at exorbitant prices or putting up pay-per-click sites could be used as evidence against them, most of the time they do no more than disable the domain names.

It is not clear that panels would consistently deem this action bad faith use, he said, adding that domain victims may be risking both wasted time and money to pursue a claim under this mechanism. ‘‘Theft clearly is not envisioned as something that would be covered under the UDRP in its current form,’’ Weslow said.

Transfer Policy Compliance. ICANN’s Inter-Registrar Transfer Policy (IRTP), which provides standardized requirements for registrar handling of domain name transfer requests, requires the gaining registrar to obtain express authorization from the registered domain name holder before proceeding with a transfer. If a dispute arises as to whether authorization was obtained, the registrars can settle the issue informally or through a Registrar Transfer Dispute Resolution Policy (TDRP) proceeding.

Under the TDRP, a losing registrar may elect to file a claim with the relevant registry operator or an independent dispute resolution provider. It may also appeal decisions made by the registry made at the first level of the dispute resolution process.

Allen Grogan, ICANN’s Chief Contract Compliance Officer, told Bloomberg BNA that if the losing registrar invokes the TDRP, the gaining registrar must comply with the procedure. Although there is no formal obligation for registrars to engage in a TDRP proceeding at the request of a registrant, he said that ‘‘most of the time registrars will try to work with the registrant to get the name back if they can.’’

If a registrar fails to comply with its contractual obligations under the IRTP, ICANN will ask the contracted parties to mitigate the problem, which usually includes undoing the transfer. ‘‘The goal is to bring the contracted parties into compliance,’’ Grogan said.

Victims Lack Standing Under TDRP. Weslow said in cases of domain theft, he often tells his clients to contact their registrar to take action under the TDRP. However, because this mechanism only permits registrars, not registrants, to attempt to resolve disputes related to inter-registrar domain name transfers, he said that the remedy may not be very effective.

If registrars were required to invoke the TDRP at a registrant’s request or if ICANN changed the policy to also give registrants standing to file a claim, Weslow said that ‘‘would go a long way towards stopping domain theft.’’

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