Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one go to http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

California Court Permits Company to Subpoena Yahoo, Google and ISPs to Identify Anonymous Computer Hacker

A federal court in San Jose California last week permitted SolarBridge Technologies, Inc. ("SolarBridge") to serve subpoenas on Yahoo, Google and various Internet Service Providers to identify the sender of an email containing SolarBridge's confidential and trade secret protected data including schematics and other product designs of current and future products. *SolarBridge Technologies, Inc. v. John Doe*, 2010 WL 3419189 (N.D. Ca. Aug. 27, 2010). With criminals hiding behind the anonymity provided by the Internet this case has widespread application to companies willing to take aggressive action to protect their data and provides an excellent blueprint for going after anonymous computer hackers.

A Mark Tatley ostensibly sent the email at issue from his Yahoo email address to a competitor of SolarBridge. The competitor responsibly notified SolarBridge of the receipt of the email. In response SolarBridge conducted its own investigation into the email, including an effort to locate Mark Tatley through the Yahoo email address and a search of public records and concluded that there was "no real individual named "Mark Tatley" and that the email address was created anonymously with fake information." *Id*. at *1. Having exhausted all means to identify the person who had stolen its competitively sensitive data, SolarBridge filed a John Doe lawsuit alleging, among other things, violations of the Computer Fraud and Abuse Act ("CFAA") and asked the court for limited discovery so it could identify the proper defendant to be served in the action.

While recognizing that "[t]he practice of suing Doe defendants is generally disfavored in the Ninth Circuit," the court stated that "where the identity of the alleged defendant will not be known prior to the filing of a lawsuit, 'the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds.'" *Wakefield v. Thompson,* 177 F.3d 1160, 1163 (9th Cir.1999) (quoting *Gillespie v. Civiletti,* 629 F.2d 637, 642 (9th Cir.1980)).

Thus, the court stated that limited discovery to identify "an anonymous Internet user" is permitted when the plaintiff:

> (1) identifies the missing party with sufficient specificity such that the court can determine that defendant is a real person or entity who could be sued in federal court;

> (2) identifies all previous steps taken to locate the elusive defendant;
>
> (3) establishes to the court's satisfaction that the lawsuit against defendant could withstand a motion to dismiss; and
>
> (4) states reasons justifying the specific discovery requested, and identifies a limited number of persons or entities upon whom discovery might be served and for which there is a reasonable likelihood that the discovery will lead to identifying information about defendant that would make service of process possible.

The court concluded that SolarBridge had met its burden –

1) John Doe "is an individual or entity that accessed SolarBridge's confidential information and disclosed that information to one of its competitors, and the email sent by Defendant is associated with San Jose-based company Yahoo!, Inc,"

2) SolarBridge had "undertaken a diligent investigation to identify Defendant without the use of third party discovery, to no avail,"

3) "SolarBridge's action would likely withstand a motion to dismiss, as it appears to have sufficiently alleged claims for violations of the CFAA" and other causes of action, and

4) "SolarBridge has shown that there is a reasonable likelihood that its requested discovery will lead to information to identify Defendant and make service on Defendant possible." *Id*. at *2.

When a hacker strikes, the procedures outlined in *SolarBridge* should be considered as a proactive option to sue the perpetrator for damages and an injunction to prevent further intrusions into the company computers. Every hacker leaves behind an IP address or a trail of IP addresses. It is virtually impossible, however, to identify the owner of an IP address from the public record. Given privacy concerns, companies like Yahoo and Google are harder to penetrate than a Swiss bank and will not voluntarily turn over the identities or records associated with IP or email addresses unless subpoenaed or ordered to do so by a court. Thus, as I have found in my own practice, a well-planned John Doe lawsuit, like that in *SolarBridge*, can provide a powerful strategic tool to retrieve stolen data and prevent its dissemination.