JONES DAY

555 CALIFORNIA STREET • 26TH FLOOR • SAN FRANCISCO, CALIFORNIA 94104.1500
TELEPHONE: +1.415.626.3939 • FACSIMILE: +1.415.875.5700

Direct Number: (415) 875-5850
jrabkin@jonesday.com

JP020437 April 29, 2015

VIA EMAIL AND OVERNIGHT MAIL

Mike Davis

Re: Intellectual Property

Dear Mike:

As discussed today, Jones Day is outside counsel for , Inc. In that regard, I write on behalf of in response to IOActive's recent communication regarding "the system," IOActive's claim that is has "discovered a number of serious vulnerabilities," and IOActive's plans for a "public advisory on April 30 where [it] will release [its] findings to the general public."

Specifically, requests that IOActive refrain from the public reporting of any security vulnerabilities relating to the system or products until has had an opportunity to identify these supposed security vulnerabilities, and, if appropriate, take any necessary remedial steps.

I note that your correspondence to states that IOActive prefers to "release vulnerabilities (security flaws) responsibly by sharing them with prior to a public advisory." Yet, when I reached out to discuss this matter with you today, you declined to share any information about your activities concerning the products, what products IOActive allegedly researched, the nature of the supposed vulnerabilities, or how you uncovered such vulnerabilities. I understand your reluctance may have been based on a need to verify our relationship to and hopefully this letter satisfies those concerns.

Of course, as you know, the public reporting of security vulnerabilities can have significant consequences. also takes the protection and enforcement of its intellectual property rights seriously and, prior to any public reporting, wants to ensure that there has been no violation of those rights, including 's license agreements or other intellectual property laws such as the anticircumvention provision of the Digital Millennium Copyright Act. Presumably, IOActive is also aligned with ensuring responsible disclosure and compliance with the laws.

JONES DAY

555 CALIFORNIA STREET • 26TH FLOOR • SAN FRANCISCO, CALIFORNIA 94104.1500
TELEPHONE: +1.415.626.3939 • FACSIMILE: +1.415.875.5700

Direct Number: (415) 875-5850
Email: jrabkin@jonesday.com

May 4, 2015

VIA EMAIL AND OVERNIGHT DELIVERY

Re:

Dear :

is committed to continually improving its products and values the security research community's thoughtful and responsible contributions. The company strives to ensure that only objective, complete, and accurate information is reported about its products, and we hope that IOActive has a similar goal. For this reason, I write to advise you that the "Security Advisory" provided to me on Thursday, April 30 contains material inaccuracies and omissions regarding 's technology, mischaracterizes the severity of the purported vulnerabilities, and unfairly depicts the overall relevance of your findings to 's product lines.

sells a broad range of products for use in a variety of security applications. While IOActive apparently reverse engineered one product, your findings are not applicable to all of the products and software sold by In addition, continually updates its firmware to address many types of security threats, including the potential attack theorized in your report. The provided draft of the report omits these facts, and therefore distorts the characterization of the risk posed by the attack to 's products as a whole.

Moreover, IOActive's reverse engineering process required the use of skilled technicians, sophisticated lab equipment, and other costly resources not generally available to the public to extract 's firmware from an embedded semiconductor chip. Leaving aside the question of whether IOActive's methodology violated 's legal rights, your process appears to have included at least the following steps: (1) forcibly disassembling a to remove the cylinder using "a few sharp strikes to the mechanical retainer"; (2) shaving off the semiconductor chip's packaging; (3) connecting leads onto the depackaged chip; (4) extracting the firmware from the depackaged chip; and (5) reverse engineering a portion of the source code for the extracted firmware. does not claim, and never has, that a door protected by one of its products is impregnable. It is simply common sense that anyone with the time,

sophistication and resources to engage in IOActive's methodology could more simply defeat a product by drilling the lock off the door, or for that matter chopping the door down with an axe. To suggest, as your report does, that 's products suffer from "severe" vulnerabilities simply because you were able to develop a bypass in your lab ignores the fact that the exploit in question was not possible without the use of costly and sophisticated lab equipment and highly skilled technicians—not exactly a real-world scenario for the intended use of products.

Under the circumstances, we are surprised by IOActive's aggressive stance and tight deadlines on the publication of its report. IOActive's own disclosure policy states that IOActive "will work with" a party like "to define a course of action for remediation and will determine a future disclosure date for publishing a security advisory." Yet when I contacted IOActive researcher Mike Davis on April 29, I was initially told that IOActive would only push back its publication deadline if made its technical staff available for a meeting with IOActive that same day. After discussions with you on Friday May 1, you indicated that after discussions with IOActive's CEO now must make its technical staff available for a meeting with IOActive before Monday at noon. IOActive's tactics—to threaten disclosure of alleged product vulnerabilities unless nakes its technical staff available within a matter of days—is simply making this process more difficult for all of us.

Even if we could arrange such a meeting by the deadline you have set for us, we do not appear to have been provided with the information necessary to prepare for such a meeting. I wrote you an email on Friday, May 1, to ask whether IOActive has any additional information beyond what is contained the report you sent me (which has only two pages of text and three pages of photographs). You wrote me back and indicated there was no additional information. Yet in our discussion by phone later that day, you indicated that IOActive may publish information that goes beyond the scope of the report you have provided—including a version of an exploit IOActive has developed as a result of its lab work that could be deployed from a hand-held open source electronics platform such as an Arduino. Given that IOActive has not provided us with any written information regarding this exploit, we are not in a position to assess the accuracy of the information you intend to make public. Why IOActive has not provided with all of the information it intends to make public is unclear given that the company's policies apparently state that you will do so.

Finally, I note that, based on our conversation on Friday, May 1, it appears IOActive's treatment of is driven at least in part by the fact that IOActive researcher Mike Davis was offended when I asked whether the company's is the same individual who was prosecuted by federal authorities for wire fraud in 2010 as suggested by publicly-available news reports.[1] While at the time it seemed relevant to determine whether

[1] See http://www

the individual who attempted to contact via email had a criminal history relating to fraud, I understand that Mr. Davis unfortunately took offense at the inquiry; that was certainly not my intent.

cannot and will not meet arbitrary deadlines to make its technical staff available to IOActive on a few days notice, especially since we do not have all of the information that you intend to make public. Given our sincere concerns regarding the objectivity, accuracy and fairness of the information contained in the report you did provide, and also given our concerns regarding the legality of IOActive's reverse engineering process, we ask that you seriously reconsider publication of the report as drafted. If IOActive does publish information about we ask that IOActive ensure such information is complete, accurate, and objective. We expect that IOActive would hold itself to such a professional standard and believe is entitled to fair treatment.

Yours very sincerely,

Jeffrey Rabkin

cc: