

July 29, 2016

*Via Email and U.S. Mail*

Maryland Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Idtheft@oag.state.md.us

Re: Notification of Information Security Breach

Dear Office of the Attorney General:

We represent Zero Gravity Solutions, Inc. ("Zero Gravity"), an agricultural biotechnology company headquartered in Boca Raton, Florida. Zero Gravity is focused on commercializing technology derived from and designed for space with significant applications on Earth. More information about Zero Gravity can be found at [www.zerogsi.com](http://www.zerogsi.com).

I write regarding a data incident involving personal information maintained by Zero Gravity concerning investors in the company. On July 1, 2016, a person falsely claiming to offer information technology support to one of Zero Gravity's employees obtained administrative access via remote login to the employee's laptop computer and its hard drive, which contained data including personal information of investors in the company. Zero Gravity learned of this incident on July 1, 2016, and its investigation concluded that the laptop in question was not connected to the company's network or information technology systems at the time of the incident.

At the time of the unauthorized access, it was unclear if any information in the computer was compromised based on the connection type and duration of the unauthorized remote access. As a result, on July 8, 2016, Zero Gravity sought from a third party forensic analysis of the computer and the incident to determine whether the information contained on the computer had likely been compromised. While there is no evidence that the third party actually accessed the personal information in question, Zero Gravity is operating with the utmost caution and notifying affected individuals of this potential breach.

Based on the results of the forensic analysis, Zero Gravity has taken further steps to protect personal information maintained by it. The company has taken custody of and secured the affected laptop and instituted additional staff training on privacy and cybersecurity (including specific training regarding attempts by third parties to acquire personal information by masquerading as a trustworthy entity). Zero Gravity also is in the process of reconfiguring all

July 29, 2016

Page 2

staff computers to prevent the downloading and use of remote access software, and such process should be complete in approximately a week. In addition, the company has destroyed the hard drive that had been accessed, after analyzing and copying the data that had been stored on it.

Based upon the information available to it, Zero Gravity believes the personal information of approximately 13 Maryland residents were contained in the affected laptop. While the types of personal information contained on the affected laptop varied from investor to investor, the information on the computer's hard drive included name, address, phone number, email address, citizenship, and social security number or other government-issued identification number. In the case of 13 Maryland residents, the laptop contained their social security number or other government-issued identification number.

A sample copy of the notice being sent to Maryland residents is enclosed with this notice.

Zero Gravity takes this matter seriously, and is continuing to work to protect the personal information procured by its services. Please let me know if you would like to discuss the incident further.

Sincerely,



Craig A. Foster

---