CONFIDENTIAL AND PROPRIETARY

datto

August 13, 2015

Via e-mail only: [redacted].com
Kim L. Ritter, Esq.
Minor & Brown, P.C.
650 South Cherry Street Plaza II, Suite 1100
Denver, CO 80247

Attorney Ritter:

This is a follow up to our telephone call of yesterday afternoon, and in advance of our 4:00 p.m. conference call.

On Tuesday, August 11, 2015 Datto learned that Platte River Networks utilizes Datto's hybrid cloud solution in connection with its provision of managed services to Secretary Hillary Clinton. We have been following the news reports concerning various investigations related to Secretary Clinton's emails, including Platte River's provision of IT related services to her. We have some concerns that we have identified to you on the phone and that we will re-iterate here.

It is our understanding that as the system is currently configured, data is automatically deleted as it reaches 60 days in age from the both the offsite node and the Datto device currently in your possession. This deletion process is currently ongoing, and will continue until and unless the retention settings are altered, or the offsite data node is disconnected. Because it may be possible that information contained on either the Datto device or the node is subject to legal retention requirements, we are concerned that if no immediate action is taken to modify these retention settings to prevent them from any further data deletion, information may be improperly deleted. Accordingly, we intend to disconnect the offsite node.

In addition, we have some concerns relative to data security. Platte has not enabled encryption at the local device. Given the sensitive, high-profile nature of the data which is alleged in press reports to potentially reside on the Datto device, it may be the target of cyber attack from a multitude of highly sophisticated and capable entities or individuals. We believe such an event could place the unencrypted data itself at risk, as well as expose both Datto and Platte River systems to collateral damage. To enable encryption on the device, Platte would first have to delete the data on the device and re-image it from scratch. Given the discussion above, this is not an option. As we discussed, we will, of course, be happy to provide a replacement Datto device to support ongoing backup requirement for your client. We would recommend you enable encryption on a replacement device. In its current state, however, the device, and the data that is stored thereon, which is also replicated to the node, is more vulnerable to cyberattack than Datto believes is prudent under the circumstances.

Accordingly, in the interest of preserving the data as potential evidence and minimizing cybersecurity risk, we intend to immediately take the node offline, and again strongly recommend that you do the same with the device.

Sincerely,

Michael Fass,
General Counsel