DAY PITNEY LLP

BOSTON CONNECTICUT NEW JERSEY NEW YORK WASHINGTON, DC

**STEVEN A. CASH**
Attorney at Law

1100 New York Ave., NW, Suite 300
Washington, DC 20005
[redacted]
[redacted].com

October 23, 2015

**VIA E-MAIL**

[redacted]
Federal Bureau of Investigation
Special Agent
Federal Bureau of Investigation
Washington Field Office
601 4th Street, N.W.
Washington, D.C. 20535

Dear Agent [redacted]:

I write in advance of our telephone conference scheduled for this afternoon at 4:00 p.m. I anticipate that Spencer Mortensen and Robert Gibbons will be on the call, and will be prepared to address technical questions.

In addition, I wanted to outline four issues that have been identified during our internal inquiry. I do not know whether, and to what extent, they are significant to your ongoing investigation, but believe it would be prudent to provide you with a summary. If needed, we can address one or more of them in greater detail when we speak.

**"Check-in" data and previously unknown host name [redacted]**

On October 3, 2015 an S2000 SIRIS device, serial number [redacted] (host name: [redacted]) "checked-in" with the Datto administrative webserver through a secure internet connection. This was the last check-in of that device. As you know, Datto advised Platte River on August 13 of concerns that the then-operating S2000 local device (with the serial number above) contained unencrypted data sets, and, as such, were potentially vulnerable. Datto provided a replacement device to Platte River to allow it to address this concern. We do not know if the replacement was used as recommended. In addition, our logs show the device with serial number [redacted], which is the replacement device, connected to Datto's administrative webserver. These logs reference device [redacted] as the host name attached to that serial number.

**Manual and Automatic removal of "recovery points"**

Datto technical experts have reviewed administrative files. Based on that review Datto has identified 182 "recovery points" which were subject to delete requests through the "recovery point page" of the Partner Portal website available to the Platte River Network-located Local Device. These manual requests were requested from the Local Device's web interface for the [redacted] agent, and all occurred on March 31, 2015 between 11:27:14 a.m. and 12:41:12 am. The 182 recovery points had a date range of January 28, 2015 to March 24, 2015. In addition, there were another 2650 recovery points that were deleted automatically based on the Local Device's then-configured pruning parameters. These automatic operations were performed for 3 agents: [redacted]

**Unauthorized Access to Datto Administrative Server**

We advised you earlier this week of the recent potential third party access to Datto's administrative server, revealed to us by the unsolicited communication from [redacted], an individual known to SSA [redacted]. We have investigated that incident, and it appears that an unidentified individual or individuals accessed the system using logon credentials associated with a Datto employee. It appears that the access was confined to efforts to search data held in the administrative server (with permissions associated with the employees account) using a set of search terms, including: "Exchange, apple, backup, Chase, coin, coi, FBI, finance, financial, .gov, invest, JP, Law, Morgan, municipal, Target, Traget, Walmart, police, Glencore." Our internal inquiry is continuing.

**Fourth data set and aggregate Data volume on Storage Node**

In reviewing administrative logs, we have identified what appears to be a fourth data set associated Local Devise [redacted] named [redacted]. According to Datto, this data set, was removed from the Local Device at some point. We are unable to determine the date. This data set may exist on the Storage Node in FBI possession. This data set is approximately 1.2 TB.

Please let me know whether follow up is necessary with respect to any of these issues.

Best regards,

*Steven A. Cash*

Steven A. Cash