

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ONE HUNDRED THIRTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DesJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DeSANTIS, FLORIDA

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

November 12, 2014

Jonathan M. Nelson
CEO
Providence Equity Partners LLC
50 Kennedy Plaza, 18th Floor
Providence, RI 02903

Jeffrey S. Campbell
President and CFO
Altegrity
7799 Leesburg Pike
Suite 1100 North
Falls Church, VA 22043

Dear Mr. Nelson and Mr. Campbell:

I am writing to request information about a significant data breach that occurred at USIS in August. I am directing this request to you because our investigation has shown that USIS is a wholly-owned subsidiary of Altegrity, and because principals at Providence Equity Partners own a majority share of Altegrity, sit on its Board of Directors, and provide direction and supervision to top managers at USIS. Despite multiple requests for information to USIS executives and their attorneys, the company has refused to provide information or answer questions about this breach.

In August, hackers successfully broke into the network of USIS, the largest private provider of background investigations for the federal government. This breach reportedly compromised the personally identifiable information of at least 27,000 federal employees who were in the process of obtaining, or who had recently obtained, security clearances in order to conduct classified work for federal government agencies. Federal cyber security experts believe that number is a floor, not a ceiling, and that many more records from other federal agencies may have been compromised.

In March, hackers broke into the network of Federal Investigative Services, a division of the Office of Personnel Management and the largest government provider of background investigations, but no personally identifiable information reportedly was compromised. It is unclear why USIS data protections were not as robust as the government's protections or why USIS was not better prepared since the August incident occurred nearly six months after the unsuccessful breach attempt at Federal Investigative Services.

As the owners and directors of USIS and other subsidiaries that have similar government contracts, you have the ultimate responsibility to ensure that all of your companies properly safeguard the information they obtain through the course of their work on behalf of the American people.

For these reasons, I request that you provide the following information:

- (1) all data security requirements applying to USIS and other Altegrity subsidiaries pursuant to federal contracts in effect at the time of the August data breach;
- (2) a complete log of all successful cyber intrusions into USIS and other Altegrity subsidiaries' networks in the last four years;
- (3) documents relating to any weaknesses or vulnerabilities in USIS data security identified by the United States Computer Emergency Readiness Team;
- (4) a list of all federal customers that may have been compromised in the August incident;
- (5) an estimate of the total possible number of PII records that may have been compromised in the August incident;
- (6) the date range of records that may have been compromised in the August incident, including when the records were created and last updated prior to the August incident;
- (7) an explanation of why your company retained PII of federal workers;
- (8) an explanation of whether system log capabilities were sufficient to determine whether or not PII was removed or altered by the hackers;
- (9) an explanation of whether Altegrity subsidiaries share proprietary IT characteristics and software with USIS and, if so, whether the August incident allowed hackers access to PII retained by other Altegrity subsidiaries; and
- (10) an explanation of whether PII of any private sector clients of Altegrity subsidiaries may have been compromised in the August incident and, if so, whether you notified those clients.

Please provide this information by December 5, 2014. If you have questions about this request, please contact Lena Chang at (202) 225-5051.

Mr. Jonathan M. Nelson and Mr. Jeffrey S. Campbell
Page 3

Thank you for your consideration of this request.

Sincerely,

A handwritten signature in blue ink that reads "Elijah E. Cummings". The signature is written in a cursive, flowing style with a large, prominent "E" at the beginning.

Elijah E. Cummings
Ranking Member

cc: The Honorable Darrell E. Issa, Chairman