

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927

Minority (202) 225-3641

October 16, 2017

Mr. Timothy O. Horne
Acting Administrator
General Services Administration
1800 F Street, N.W.
Washington, DC 20405

Dear Acting Administrator Horne:

We are writing to request information about the General Services Administration's (GSA) consideration of data security practices when vetting vendors and awarding government contracts. As a Federal government agency, GSA has a responsibility to act in the best interests of the American public, including ensuring that their personal information is secure.

It has come to our attention that GSA has awarded contracts to Equifax to provide data-related services handling Americans' personal information at multiple Federal agencies, including the Internal Revenue Service (IRS), Social Security Administration, and Center for Medicare and Medicaid Services.¹

As you are aware, on September 7, 2017, Equifax announced that hackers stole the personal information of 143 million Americans (this number was later updated to 145.5 million).² The stolen information included names, birth dates, addresses, Social Security numbers, and in some cases driver's license numbers.³ Although investigations into the Equifax breach are ongoing, early reports indicate that the breach was made possible by failures of basic

¹ www.wsj.com/articles/equifax-work-for-government-shows-companys-broad-reach-1505781393; www.politicopro.com/tax/story/2017/10/irs-defends-equifax-contract-amid-hill-outcry-162981.

² www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forensic-investigation-cybersecurity-incident/; <https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/>.

³ time.com/4932921/equifax-data-breach-social-security/.

<https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/>.

data protection practices and general cybersecurity hygiene at Equifax.⁴ Moreover, this breach was not the first serious data breach at Equifax; it was not even the first one this year.⁵

On September 15, 2017, the company publicly disclosed further details of the cybersecurity incident, including that the Equifax security team was aware of the vulnerability in March 2017. On September 26, Equifax announced the retirement of CEO and Chairman Richard Smith and the designation of an interim CEO. On September 29, 2017, the IRS awarded the contract to Equifax. Three days following the IRS contract award, Equifax announced cybersecurity firm Mandiant concluded its forensic investigation of the data breach and identified 2.5 million additional Americans affected—bringing the total to 145.5 million.

On October 3, 2017, former Equifax CEO and Chairman Richard Smith testified about the breach before the Digital Commerce and Consumer Protection Subcommittee. At a hearing before the Committee on Ways and Means the next day, the IRS explained that it had signed a long-term contract with an Equifax competitor but Equifax filed an objection to that contract with the U.S. Government Accountability Office (GAO) in July 2017. We understand that GAO has until October 16, 2017, to resolve that protest and that the IRS argued during the hearing that it granted a bridge contract to ensure its services could continue.⁶

This Committee wrote to Internal Revenue Service Commissioner John Koskinen on October 10, 2017, to request information on the identity verification contract with Equifax.

In recent years, we have seen that poor data security practices at companies and within the Federal government leave Americans vulnerable to theft of personal information. We, therefore, request written responses to the following questions no later than October 26, 2017:

1. Do you consider consumer protection issues, including data security practices, when vetting vendors and awarding government contracts? What data security requirements or controls are generally enumerated relating to the protection of personal information held by the Federal government and security incident response and notification procedures in the contract solicitation?
2. Are subcontractors subject to the same vetting process, including any consumer protection and data security considerations, as the business that directly contracted with GSA? Is the primary contractor or GSA responsible for vetting subcontractors?
3. Do you consider past breaches (including past breaches of personal information held by the Federal government) and businesses' responses to past breaches when determining to whom contracts are awarded?

⁴ www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947; Richard Smith written testimony to E&C.

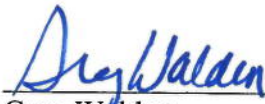
⁵ krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-tax-payroll-division/;
krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/

⁶ <http://www.gao.gov/docket/B-414907.1>

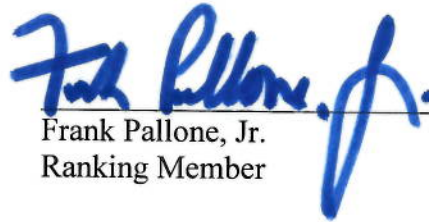
4. What are the circumstances under which you would choose to award a contract to a business that has suffered previous breaches?
 - a. How do you verify that the business has addressed any underlying issues that contributed to the breach?
 - b. Do you require the business to have any additional safeguards in place to guard against future breaches? If so, does GSA penalize them if the safeguards fail?

Thank you for your attention to this matter. If you have questions, please contact Melissa Froelich or Paul Jackson of the Majority staff at (202) 225-2927 and Michelle Ash or Lisa Goldman of the Minority staff at (202) 225-3641.

Sincerely,



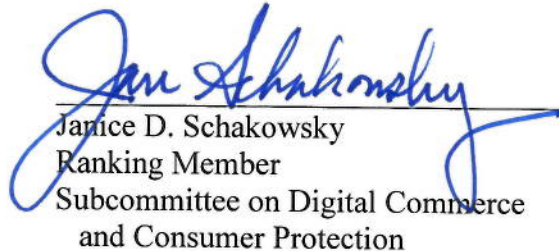
Greg Walden
Chairman



Frank Pallone, Jr.
Ranking Member



Joe Barton
Vice Chairman



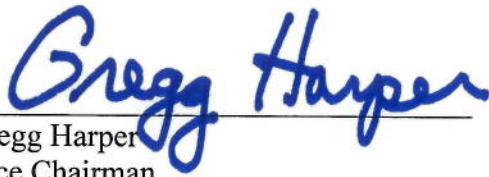
Janice D. Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection



Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection



Gene Green
Member of Congress




Gregg Harper
Vice Chairman
Subcommittee on Digital Commerce
and Consumer Protection



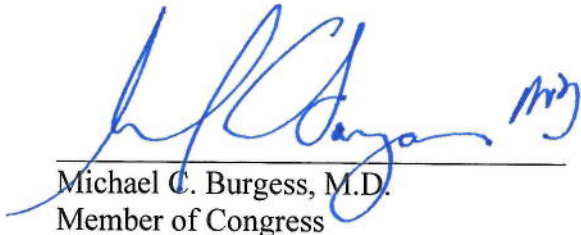
Doris O. Matsui
Member of Congress



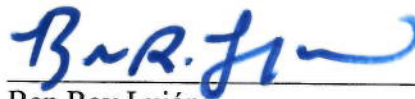
Fred Upton
Member of Congress



Peter Welch
Member of Congress



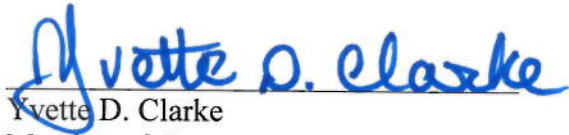
Michael C. Burgess, M.D.
Member of Congress



Ben Ray Luján
Member of Congress



Leonard Lance
Member of Congress



Yvette D. Clarke
Member of Congress



Brett Guthrie
Member of Congress



Joseph P. Kennedy, III
Member of Congress



David B. McKinley
Member of Congress



Tony Cárdenas
Member of Congress



Adam Kinzinger
Member of Congress



Debbie Dingell
Member of Congress



Gus M. Bilirakis
Member of Congress



Larry Bucshon
Member of Congress



Markwayne Mullin
Member of Congress



Mimi Walters
Member of Congress



Ryan A. Costello
Member of Congress