

United States Senate

WASHINGTON, DC 20510

June 10, 2015

BY FIRST-CLASS AND ELECTRONIC MAIL

The Honorable Richard Cordray
Director
Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552

Dear Director Cordray:

On May 26, the Internal Revenue Service (IRS) revealed that identity thieves had downloaded over 100,000 taxpayer records through a feature on the IRS's own website known as "Get My Transcript." Just a few days later, the Office of Personnel Management (OPM) revealed that the personal data of approximately four million federal employees was stolen by hackers believed to be aligned with the Chinese government. While these investigations remain ongoing, we believe that now is a critical time to examine the measures other government agencies take to secure personal data they collect on Americans.

Under the Dodd-Frank Act, the CFPB has begun accumulating loan-level data "covering approximately 80% of the credit card marketplace"—hundreds of millions of credit card accounts.¹ A recent Government Accountability Office (GAO) report also confirms that CFPB is collecting: arbitration case records; vehicle transaction-level data from departments of motor vehicles; credit scores; information on deposit advance products; data on overdraft fees; and numerous other types of consumer financial data.² We are gravely concerned by the CFPB's inability to confirm that the massive amount of data it collects and stores could not be reverse-engineered and traced back to one of our constituents.³

¹ CONSUMER FINANCIAL PROTECTION BUREAU, STRATEGIC PLAN, BUDGET, AND PERFORMANCE PLAN AND REPORT 64 (Mar. 2014), available at <http://files.consumerfinance.gov/f/strategic-plan-budget-and-performance-plan-and-report-FY2013-15.pdf>

² U.S. GOV'T ACCOUNTABILITY OFFICE, CONSUMER FINANCIAL PROTECTION BUREAU: SOME PRIVACY AND SECURITY PROCEDURES FOR DATA COLLECTIONS SHOULD CONTINUE BEING ENHANCED, Rept. No. GAO-14-758, 15-17 [hereinafter "GAO REPORT"].

³ *The Semi-Annual Report of the Consumer Financial Protection Bureau: Hearing Before the House Committee on Financial Services*, 113th Cong. 28 (2014) (you testified, "[t]here may be information-gatherings that the government has done across many sectors that at one time could not be reverse-engineered but may become more capable of having that happen. That is something we are very careful about and mindful of and thinking about.")

To be sure, we disagree about the extent, manner, and usefulness of CFPB's data collection efforts.⁴ Nevertheless, the IRS and OPM data breaches are useful reminders that the CFPB must take great care to safeguard any and all personally identifiable information it collects on Americans. Unfortunately, the GAO Report documented numerous deficiencies with data security at the CFPB:

- “CFPB lacks written procedures for its data intake process, including for evaluating whether statutory restrictions related to collecting personally identifiable financial information apply to large-scale data collections”;
- “CFPB has not yet developed a comprehensive privacy plan that brings together existing policies and guidance”; and
- “CFPB did not sufficiently document its consultation with [the Office of Management and Budget] about an information-sharing agreement CFPB has with the Office of the Comptroller of the Currency.”⁵

These findings echo the deficiencies noted in a prior review of the CFPB's IT framework by the Office of the Inspector General at the Board of Governors of the Federal Reserve System entitled “Security Control Review of the CFPB's Cloud Computing-Based General Support System.”⁶ As a result of these findings, GAO made several recommendations to better “protect and secure collected consumer financial data” at the CFPB.⁷

Our constituents have an absolute right to the security of their personal information, whether contained in a tax return at the IRS, personnel records at OPM, or in the bulk data that the CFPB is collecting on an ongoing basis. Despite having spent over \$10 billion on information technology and related services over the past decade and a half, the IRS was unable to prevent identity thieves from walking right through the front door of the IRS's computer system and stealing tax returns. We are concerned that without adequate safeguards, the computer systems that store personally identifiable information at the CFPB and its vendors are equally vulnerable.

⁴ See generally *The Consumer Financial Protection Bureau's Semi-Annual Report to Congress: Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, 113th Cong. (2013).

⁵ GAO REPORT at 64-65.

⁶ OFFICE OF THE INSPECTOR GENERAL OF THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, EXECUTIVE SUMMARY: SECURITY CONTROL REVIEW OF THE CFPB'S CLOUD COMPUTING-BASED GENERAL SUPPORT SYSTEM (2014), available at <http://oig.federalreserve.gov/reports/cfpb-it-cloud-computing-summary-jul2014.pdf>.

⁷ GAO REPORT at 65-66.

So that our constituents may better understand how the CFPB handles and stores their data, we respectfully request that you respond to the following questions not later than June 26, 2015.

1. What concrete steps is the CFPB taking in response to the recommendations in the GAO Report, and how much progress has the CFPB made? Please provide a separate answer for each of the GAO's 11 recommendations.
2. In January 2014, the CFPB published an advisory for consumers who are victims of data breaches in the private sector. Does the CFPB have a plan, *ex ante*, for notifying individuals in the event of a breach of or unauthorized access to data held by the CFPB or its vendors, some of which may be traceable to a particular individual?
3. At a 2013 House Finance Services Subcommittee hearing, CFPB's then-Acting Deputy Director Stephen Antonakes testified that CFPB has "robust security systems, IT systems that are constantly being reviewed and audited."⁸ The CFPB relies on third-party vendors for data collection (*e.g.* for the consumer complaint database), for data storage, and for other purposes. What steps does the CFPB take to ensure the robustness of the security of its own IT systems and those of its third-party vendors? How many and what type of data incidents, events, or breaches have there been on the IT systems of CFPB and at third-party vendors? Have any of those data incidents, events, or breaches involved personally identifiable information (PII), such as information collected through the consumer complaint database? What specific steps has CFPB taken to notify individuals whose PII may have been subject to unauthorized access? How does the CFPB hold its vendors accountable for any such incidents?
4. At the same hearing, Mr. Antonakes said that CFPB was "in the process of developing . . . our data destruction schedules," and confirmed that until such destruction protocol was in place, that CFPB would be holding all the data it has ever collected.⁹ Please (a) provide an update on this process, and (b) please describe the CFPB's data retention policy, inclusive of any arrangements CFPB has with third-party vendors for data collection and destruction.

⁸ See generally *Examining How the Consumer Financial Protection Bureau Collects and Uses Consumer Data: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services*, 113th Cong. 34 (2013).

⁹ *Id.* at 11-12.

Hon. Richard Cordray

June 10, 2015

Page 4

We look forward to your timely reply.

Sincerely,



TIM SCOTT

United States Senator

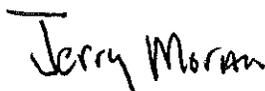
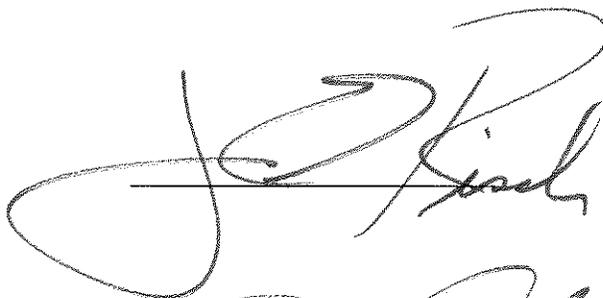
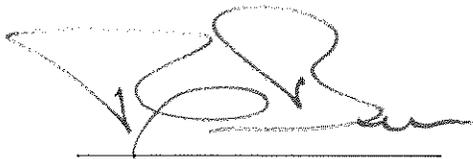
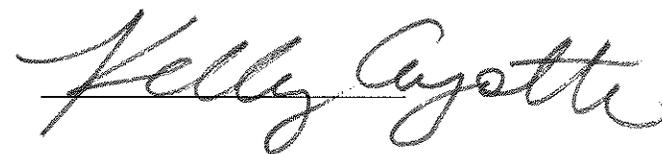


MIKE CRAPO

United States Senator



Dan Sullivan



Ad Long

Michael McConnell

Bill Cassidy

M. J. B. R.

Jeff Flake

Shelley Moore Capito

Chris Hatch

[Signature]

John Cornyn

[Signature]
