Congress of the United States
Washington, DC 20515

June 23, 2017

The Honorable Richard Cordray
Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, D.C. 20552

Dear Director Cordray,

We write to you regarding the exploration of alternative data and its impact on consumers' access to credit being conducted by the Consumer Financial Protection Bureau (the CFPB or the Bureau.) As you know, alternative data presents a virtually limitless scope of information on consumers, including payment history of rent, utilities, cell phone bills, small dollar loans, check cashing, and bank account records. Additional, non-traditional sources of alternative data may include Facebook posts, capitalization of text messages, email addresses, brand of vehicle, and educational background.[1] In the era of hacking and identity theft, we are concerned about the Bureau's collection of alternative data and urge you to refrain from collecting personally identifiable information (PII) in order to ensure that consumers' sensitive information is secure.

As you know, the U.S. Government Accountability Office (GAO) and the CFPB's Inspector General have, in the past, identified deficiencies in the CFPB's data security controls and privacy protections.[2] At the time, the GAO found weaknesses in the Bureau's ability to evaluate cybersecurity risks and protect consumers' PII. While we appreciate the steps the Bureau has taken to strengthen its cybersecurity practices, any vulnerability is concerning given the CFPB's large scale collection of consumer data in the areas of vehicle sales, credit reports, credit cards, credit scores, student loans, and mortgages.[3] Clearly, alternative data presents numerous additional fields of PII, and if this data falls into the wrong hands, the damage to consumers could be significant.

The Bureau has stated that as part of its analysis of alternative data, it will examine access to credit, complexity of the credit access process, impact of alternative data on credit costs and

---

[1] Gregory Roberts, *Consumer Protection Bureau Wades Into Big Data Credit Swamp,* BLOOMBERG GOVERNMENT, Apr. 19, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OONY9Y3H0JK0.
[2] *Consumer Financial Protection Bureau: Some Privacy and Security Protections for Data Collections Should Continue Being Enhanced,* GOVERNMENT ACCOUNTABILITY OFFICE, September 2014, *available at* http://www.gao.gov/products/GAO-14-758.
[3] Trey Garrison, *CFPB Collecting Data on 600 Million Credit Accounts Despite Privacy, Security Risks,* HOUSING WIRE, Sept. 22, 2014, *available at* http://www.housingwire.com/articles/31444-cfpb-collecting-data-on-600-million-credit-accounts-despite-privacy-security-risks.

service, implications for privacy and security, and impact on specific groups.[4] Given the numerous past data breaches that have taken place at other federal financial regulatory agencies, including the Federal Reserve,[5] FDIC,[6] and OCC,[7] CFPB data security is of the utmost concern. This concern continues to grow as the CFPB is significantly expanding its already vast collection of consumer data in areas it has not previously explored. Reports have indicated that the Bureau already conducts at least 13 mass collection programs of consumer financial data, including 546-596 million individual credit card accounts per month, covering 87% of the credit card market; 11 million consumers' credit reports per month; 195 million mortgages per month; and 700,000 auto sales per month. Additionally, on May 10, the Bureau announced the start of its rulemaking on the collection of vast sums of new data on small business lending pursuant to Section 1071 of the Dodd-Frank Act. Institutions that are expected to be part of these new data collection requirements include bank and nonbank lenders, regulators, consumer organizations, and other individual businesses.[8] This future collection of untold amounts of data by the Bureau further increases our concern about the security of consumers' and businesses' sensitive information. Furthermore, we are not the first lawmakers to express concern. In a 2014 Financial Services Committee hearing, regarding another database that the CFPB maintains, it was rightfully stated that a breach of this database could result in significant harm to consumers by the very agency that claims to be protecting them.[9]

Furthermore, the Office of Inspector General of the CFPB and the Board of Governors of the Federal Reserve System (IG) recently released a report revealing significant data security vulnerabilities at the CFPB Office of Enforcement.[10] These vulnerabilities further increase our concern with any collection of consumers' sensitive data, such as confidential investigative information (CII), which may also include PII. While we appreciate the Bureau's efforts to strengthen its cybersecurity posture, it is deeply troubling that sensitive information belonging to the CFPB Office of Enforcement has been accessible to 113 of the Bureau's employees who no longer needed access to that data for the performance of their job duties. These concerns and others raised by GAO, the IG, and other lawmakers raise the question of whether the risks of collecting and maintaining such sensitive data outweigh the benefits gained for those who are credit invisible. Additionally, the IG recently released a report addressing security deficiencies with the CFPB's public website, and identified risks to the integrity and confidentiality of the

---

[4] *CFPB Explores Impact of Alternative Data on Credit Access for Consumers Who Are Credit Invisible*, CONSUMER FINANCIAL PROTECTION BUREAU, Feb. 16, 2017, *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-explores-impact-alternative-data-credit-access-consumers-who-are-credit-invisible/.

[5] Jason Lange & Dustin Volz, *Fed Records Show Dozens of Cybersecurity Breaches*, REUTERS, Jun. 1, 2016, *available at* http://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM.

[6] Carten Cordell, *FDIC Stalls in Reporting Another Cyber Breach, Committee Says,* FEDERAL TIMES, Oct. 21, 2016, *available at* http://www.federaltimes.com/articles/fdic-stalls-in-reporting-another-cyber-breach-committee-says.

[7] Donna Borak, *U.S. Bank Regulator Notifies Congress of Major Data Security Breach,* WALL STREET JOURNAL, Oct. 28, 2016, *available at* https://www.wsj.com/articles/u-s-bank-regulator-notifies-congress-of-major-data-security-breach-1477684445.

[8] Jeff Bater, *CFPB Starts Inquiry of Small-Business Lending,* BLOOMBERG GOVERNMENT, May 10, 2017, *available at* https://www.bgov.com/core/news/#!/articles/OPQM5P3H65TS.

[9] Garrison, "*CFPB Collecting Data*"

[10] *The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information*, OFFICE OF INSPECTOR GENERAL OF THE CONSUMER FINANCIAL PROTECTION BUREAU AND THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, May 15, 2017, *available at* https://oig.federalreserve.gov/reports/cfpb-enforcement-confidential-investigative-information-may2017.pdf.

contents of the website.[11] Any weaknesses of the website are extremely concerning given the nature of sensitive personal information, such as account numbers, that are stored in the Consumer Complaint Database. More broadly, the IG's 2016 annual report highlights ongoing challenges at the Bureau regarding its contingency planning activities.[12] At a time when the Bureau continues to experience gaps in its information security controls, it is unacceptable for the CFPB to be collecting vast new sums of sensitive consumer data. Given the Bureau's ongoing challenges with updating access rights, migrating its information technology systems, and failing to restrict employee access to the network drive containing sensitive information, we believe the Bureau must refrain from collecting PII for market monitoring, supervisory functions, and enforcement actions. As you know, the Bureau is explicitly prohibited from obtaining PII by Section 1022 of the Dodd-Frank Act.

In light of these concerns, we request a response to the following questions by July 21:

1. The Bureau states on its website that "we only collect the minimum amount of personally identifiable information (PII) we need."[13] On what factors does the Bureau make the calculation of the minimum amount of PII needed? What cybersecurity measures does the Bureau take to protect the PII that it does collect?
2. Will the Bureau be collecting any additional PII as part of its exploration of alternative data? If so, in which areas of alternative data will the Bureau be collecting PII?
3. What are the most pressing cybersecurity challenges that the Bureau is currently working to address?
4. As you know, in its 2016 annual report, the IG recommended that the CFPB "formalize insider threat activities through an agency-wide insider threat program strategy, ensure that user access forms and rules of behavior for privileged users are maintained, and ensure that a business impact analysis is conducted and used to guide contingency planning activities."[14] Can the Bureau confirm that all of the sensitive data it is collecting is secure while it is implementing these recommendations? If not, we urge the Bureau to cease collecting any sensitive consumer data until all IG and GAO cybersecurity recommendations are fully implemented.
5. What other steps is the Bureau taking to protect against insider threats?
6. Have any "major breaches" occurred under the standards of the Federal Information Security Modernization Act of 2014?

---

[11] *Security Control Review of the CFPB's Public Website*, OFFICE OF INSPECTOR GENERAL OF THE CONSUMER FINANCIAL PROTECTION BUREAU AND THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, MAY 22, 2017, *available at* https://oig.federalreserve.gov/reports/cfpb-public-website-may2017.htm.

[12] *2016 Audit of the CFPB's Information Security Program*, OFFICE OF INSPECTOR GENERAL OF THE CONSUMER FINANCIAL PROTECTION BUREAU AND THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, Nov. 10, 2016, *available at* https://oig.federalreserve.gov/reports/cfpb-enforcement-confidential-investigative-information-may2017.pdf.

[13] *Privacy*, CONSUMER FINANCIAL PROTECTION BUREAU, *available at* https://www.consumerfinance.gov/privacy/.

[14] "*Security Control Review*"

7. Does the CFPB maintain any server or database on the cloud? If so, are they FedRAMP compliant?

We look forward to working with you to ensure that consumers' sensitive, personally identifiable information remains secure. Thank you for your attention to this important matter.

Sincerely,

Barry Loudermilk
Member of Congress

Ann Wagner
Member of Congress

French Hill
Member of Congress

Bill Posey
Member of Congress

Dave Trott
Member of Congress

Keith Rothfus
Member of Congress

Tom MacArthur
Member of Congress

Claudia Tenney
Member of Congress

Trey Hollingsworth
Member of Congress

Dennis A. Ross
Member of Congress

Alex Mooney
Member of Congress

Tom Emmer
Member of Congress

Scott Tipton
Member of Congress

David Kustoff
Member of Congress