# *Consumer Financial Protection Bureau Independent Audit of Selected Operations and Budget*

December 18, 2015

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

# Table of Contents

**KPMG LLP**
Suite 12000
1801 K Street, NW
Washington, DC 20006

## EXECUTIVE SUMMARY

December 18, 2015

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

Dear Mr. Cordray:

This report presents the results of our work conducted to address the performance audit objectives relative to the Consumer Financial Protection Bureau (hereinafter referred to as "CFPB" or "Bureau"). Our work was performed during the period June 15, 2015 to November 24, 2015, and our results, reported herein, are as of December 18, 2015.

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and recommendations based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and recommendations based on our audit objectives.

As specified by CFPB, our audit objectives were to evaluate CFPB's (1) Investment Review Board (IRB) process relative to CFPB's policies and procedures; (2) budget process relative to its policies and procedures established over budget formulation, execution, and monitoring; (3) information privacy function relative to CFPB policies and procedures over the compliance with Privacy laws and applicable regulations and guidance, and (4) corrective actions taken to resolve the findings and recommendations included in CFPB's *2014 Independent Audit of Selected Operations and Budget* , which was performed by KPMG.

As our report further describes, we identified the following finding as a result of the work performed to meet our audit objectives:

A. Information privacy policies and procedures need to be updated.

We recommend that the Bureau:

- Complete its automated data cataloguing activities within the documented project timeframe, which should include evaluating CFPB data sets maintained, and the establishing policies and procedures to regularly review the data set inventory.
- Update current privacy policies, to include enhanced procedures and options available to assure positive destruction of storage that contains personally identifiable information when legally permitted.

As a result of our procedures, we noted that the control deficiencies noted in our prior year audit have been remediated. In addition, we also identified certain observations, as presented in ***Appendix A – Additional Improvement Observations.*** We determined that these observations are not reportable findings. However, understanding these observations may be useful to CFPB for consideration in strengthening the IRB and budget practices.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards* or *U.S. Generally Accepted Auditing Standards.* KPMG LLP was not engaged to and did not render an opinion on the CFPB's internal controls over financial reporting or over financial management systems (for purposes of OMB Circular No. A-127, *Financial Management Systems*, December 1, 2009, as revised).

This report is intended solely for the information and use of the Consumer Financial Protection Bureau, and is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

KPMG LLP

## BACKGROUND

The Consumer Financial Protection Bureau (CFPB) was established on July 21, 2010 under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act Public Law No. 111-203 (Dodd-Frank Act) as an independent bureau within the Federal Reserve System. The Bureau is an Executive agency, as defined in Section 105 of Title 5, United States Code, with a mission to make markets for consumer financial products and services work for Americans – whether they are applying for a mortgage, choosing among credit cards or using any number of other consumer financial products. To accomplish its mission, the CFPB seeks to educate consumers, enforce Federal consumer financial laws, and gather and analyze information to better understand consumers, financial service providers and consumer financial markets.

The CFPB has a diverse mandate and roles that were previously covered by seven different agencies responsible for rulemaking, supervision, and enforcement relating to consumer financial protection. The agencies which previously administered statutes transferred to the CFPB are the Board of Governors of the Federal Reserve System (Federal Reserve); the Office of the Comptroller of the Currency (OCC); the Office of Thrift Supervision (OTS); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); the Federal Trade Commission (FTC); and the Department of Housing and Urban Development (HUD).

To accomplish its mission, the CFPB developed and is continuing to build a workforce with a broad and diverse depth of public and private industry experience that is spread across the country, with its headquarters in Washington, D.C. and regional offices in Chicago, New York City and San Francisco. The CFPB is organized into six primary divisions:

- *Consumer Education and Engagement* – Responsible for providing, through a variety of initiatives and methods, information to consumers that will allow them to make decisions that are best for them.
- *Supervision, Enforcement, and Fair Lending* – Responsible for ensuring compliance with Federal consumer financial laws by supervising market participants and bringing enforcement actions when appropriate.
- *Research, Markets, and Regulations* – Responsible for understanding consumer financial markets and consumer behavior, evaluating whether there is a need for regulation, and determining the costs and benefits of potential or existing regulations.
- *Legal Division* – Responsible for the CFPB's compliance with all applicable laws, and provides advice to the Director and the Bureau's divisions.

- *External Affairs* – Responsible for managing the CFPB's relationships with external stakeholders and ensuring that the Bureau maintains robust dialogue with interested stakeholders to promote understanding, transparency, and accountability.
- *Operations Division* – Responsible for building and sustaining the CFPB's operational infrastructure to support the entire organization.

## OBJECTIVES, SCOPE, AND METHODOLOGY

### *Objectives and Scope*

As specified by the CFPB, the objectives of our performance audit were to evaluate CFPB's:

1. Investment Review Board (IRB) process relative to CFPB's policies and procedures;
2. Budget process relative to its policies and procedures established over budget formulation, execution, and monitoring;
3. Information privacy function relative to CFPB policies and procedures over the compliance with federal privacy laws and applicable regulations and guidance; and
4. Corrective actions taken to resolve the findings and recommendations included in CFPB's *2014 Independent Audit of Selected Operations and Budget*.

### *Methodology and Approach*

We conducted our performance audit in accordance with the performance audit standards in *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and recommendations based on our audit objectives. Our responsibility is to provide findings and recommendations based on the results of our audit. We believe that the evidence obtained provides a reasonable basis for our findings and recommendations based on our audit objectives.

Our methodology consisted of the following four-phased approach:

1. *Project Initiation and Planning* – We met with CFPB key personnel to (1) reaffirm CFPB's and our collective understanding of the performance audit objectives and scope, (2) highlight our methodology and approach to meet the audit objectives, (3) request certain information from CFPB needed to perform our audit, and (4) gain an understanding of the status of corrective actions plans related to our prior year findings and recommendations.
2. *Data Gathering* – We interviewed key CFPB personnel to obtain an understanding of processes, controls, and available documentation for each audit objective. For each audit objective, we (1) researched leading practices, (2) obtained and reviewed relevant documentation, (3) selected samples

for detailed testing and further analysis, when appropriate, and (4) documented the work performed and results of our audit procedures.

3. *Analysis Using Established Criteria* – Our evaluation criteria was developed from a variety of sources, including requirements and technical guidance published by the Office of Management and Budget (OMB) and used by CFPB as leading practices[1] at the time of our audit (e.g., OMB Circular No. A-123, *Management's Responsibility for Internal* Control; OMB Circular No. A-11, *Preparation, Submission and Execution of the Budget)*, OMB Memorandum (M) 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*); the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: *Privacy Control Catalog*; applicable laws and regulations, such as the E-Government Act of 2002[2]; and CFPB's policies and procedures.
4. *Findings and Recommendations* – The results of our audit work were the basis for our audit findings and recommendations. These findings and recommendations were formally communicated to CFPB management through our Notice of Findings and Recommendation process. We met with CFPB management to discuss our findings, recommendations, the content of the auditor's report, and steps related to the final reporting process.

The sections below present an overview of each of the audit objectives and the key procedures performed with respect to each area.

### *CFPB's Investment Review Board*

The IRB is CFPB's executive advisory body for all major investment decisions. Its mission is to ensure that investments maximize value through robust project planning, cross-departmental communication, and alignment with CFPB mission, vision, and strategic goals. Through its review of business cases supporting investment requests, the IRB seeks to foster data-driven analysis and decision-making, promote project management best practices to support the success of innovative solutions, and provide a forum for cross-departmental communication regarding major investments. There are four primary roles in the IRB process with the following responsibilities:

- IRB Chair: The Chair sets the IRB schedule, agenda, and makes decisions regarding the approval of IRB investments.

[1] While not required to comply with OMB regulations, CFPB uses OMB requirements and guidance as indicators of leading practices.
[2] Public Law No. 107-347, section 208, 116 Stat. at 2921, December 17, 2002

- IRB Board Members: Board Members review investments and make informed enterprise-level investment recommendations to the Chair, based upon their subject-matter expertise and leadership roles at the CFPB, as well as through analysis of submitted business case documentation
- Office of the Chief Financial Officer (OCFO): The OCFO supports the Chair through administrative assistance, analytical reviews, technical recommendations, documentation gathering, maintenance of IRB records, and communications with Board Members and CFPB investment owners.
- Investment Owners: Owners of major investments are responsible for developing, documenting, and presenting the business case(s) for their respective investment(s), as well as keeping track of their investment's approval status and progress throughout the IRB process.

The IRB process involves evaluating the business case for an investment to determine whether the investment owner's plan implements CFPB priorities and is grounded in sound project management practices. This process is in alignment with the CFPB mission and strategic plan, as the IRB will review investments in the context of supporting the CFPB mission and priorities in the most current CFPB Strategic Plan. The IRB process also works in conjunction with CFPB's annual financial plan, as the administration of IRB documentation and review will generally be aligned with the development of the annual financial plan, although IRB documentation, review, and approval may occur throughout the fiscal year as necessary. During fiscal year 2015, the IRB reviewed over 85 individual investment business cases.

The IRB process applies to new investments and continuing investments that meet the IRB thresholds. The process supports the execution of the annual financial plan and provides a forum to review significant developments in the lifecycles of major investments. The structure of the IRB process can be broken down into three key areas: investment documentation, review process, and approval process.

*Investment Documentation*

The approval process requires that all major investments must have supporting documentation that outlines the business case for making the investment. The format of that documentation is determined by the OCFO in consultation with Board Members and approval by the Chair. After the initial documentation, IRB investments require an annual update. Investments with significant variations in scope, cost, or strategies may require updated documentation prior to commitment of additional funds. The CFPB has developed a series of templates for documentation updates, which vary according to the lifecycle stage of the investment.

All investment business cases and updates must be pre-approved by a business sponsor before being considered at the IRB. Documentation required for IRB review will also be rescreened by OCFO, who may consult with the business owners and other IRB members as appropriate.

*IRB Review Process*

IRB Review is the process by which the Chair assesses the IRB business case to make an approval decision. The format of the review may vary according to the nature of the investment, and may include the investment owner presenting the investment at an IRB meeting. IRB Review may also occur outside of the IRB meeting, primarily for annual business case updates, as deemed appropriate by the Chair. This may involve consultation with various IRB Members, business case owners, and/or OCFO staff.

The purpose of IRB meetings is to provide a forum for IRB Members to make enterprise-level recommendations to the Chair based upon the information presented in IRB documentation, as well as the individual member's subject-matter expertise and leadership roles at the CFPB. Meetings occur periodically throughout the year, as needed (e.g., quarterly). Ad hoc meetings may be scheduled at the Chair's discretion, and meetings may be cancelled if there are no major investments requiring IRB review. Furthermore, IRB board meetings may be conducted by telephone, email, or other forms of virtual communication, primarily if a time sensitive request cannot be accommodated in a regularly scheduled meeting.

Investments may undergo continued review in order to enhance accountability over the proposed business case, evaluate the performance of investments, and assess plans to address gaps in performance as necessary. In order to ensure that IRB documentation continues to reflect business cases presented to the IRB, the OCFO will reference IRB approval and cost estimates whenever an office submits an IRB-related Control Sheet that tracks the process of the IRB review. Therefore, procurement actions that require funding requests, such as new contracts, exercise of contract option periods, and cost-related contract modifications, will be subject to constraints identified in both the Office's financial plan and the IRB business case. Significant differences may require IRB documentation updates, review, and IRB approval by the Chair.

*IRB Approval Process*

Full IRB approval indicates that investment owners have made a sound business case for the planned investment and that the requesting office may continue with implementation of the investment as documented until the approval of the investment expires. As mentioned above, previously approved IRB investments with significant cost variances or significant qualitative changes may require updated IRB documentation and may be subject to further IRB review before further investment is made.

Our methodology for evaluating the IRB process included the following procedures:

- Interviewing CFPB key budget personnel within the individual division/program offices and the OCFO regarding the documentation, review, and approval components of the IRB process;
- Reviewing the policies and procedures for IRB documentation, review, and approval;

- Obtaining further understanding of the IRB documentation, review, and approval process through discussions with management of CFPB's OCFO and select CFPB divisions/program offices;
- Reviewing documents prepared by the CFPB divisions/program offices to support the IRB documentation process;
- Comparing the CFPB IRB documentation, review, and approval process to the applicable requirements and guidance in OMB Circular A-11 as an indicator of leading practice, and
- Obtained an understanding of the IRB review and approval process through discussions with OCFO management and select CFPB divisions/program offices.

Our current audit procedures did not identify any findings related to the IRB process. However as a result of our procedures, we reported certain observations for CFPB's consideration in further enhancing the IRB process, which are included in ***Appendix A – Additional Improvement Observations***. These observations are related to our 2015 audit of selected operations and budget, and are presented for the purpose of finalizing the results of that audit.

### *CFPB's Budget Process*

Pursuant to the Dodd-Frank Act ("the Act"), the CFPB is funded principally by transfers from the Federal Reserve System, up to a limit set forth in the Act. In addition, pursuant to the Act, the CFPB is also authorized to collect and use, for specified purposes, civil penalties collected from any person or entity in any judicial or administrative action brought under federal consumer financial law. During fiscal years 2014 and 2015, the CFPB's annual transfers from the Board totaled approximately $534 million and $485 million, respectively. The CFPB budget process consists of budget formulation (including budget submission and approval), budget execution, and budget monitoring (including reporting). The CFPB and the Federal Reserve have entered into an inter-agency agreement for the continued funding of the operations of the CFPB as set forth in Section 1017(b) of the Dodd-Frank Act. Under this agreement, the Federal Reserve will transfer funds quarterly to the CFPB based on notification by the Director of the amounts needed.

The annual budget formulation process begins approximately 18 months before the beginning of the fiscal year in which the budget will be executed. This is a collaborative effort between the OCFO and CFPB divisions and their offices. To facilitate a standardized and consistent budget formulation process, the OCFO has developed policies and procedures, including templates for gathering relevant data. The program or division is required to support the amounts requested and link to the CFPB goals set by the Director.

The CFPB's Operations Division is responsible for coordinating activities for budget formulation across the Bureau. Working in collaboration with other CFPB divisions, the OCFO has primary responsibility for developing the budget (including staffing estimates) consistent with statutory requirements, performance goals, and CFPB priorities.

The CFPB Director has final approval authority over the budget. Once the annual budget is approved by the Director, it is distributed internally, communicated to OMB (but not subject to approval by OMB) and posted on the CFPB website.

To execute its budget, CFPB exercises administrative control of funds through several measures. A financial plan is developed for each division and distributed at the beginning of each fiscal year. Within the financial plan, each division is allocated a target staffing headcount and personnel and non-personnel funding for the fiscal year. Divisions are expected to adhere to their financial plan allocations and to work collaboratively with the OCFO to request any additional funding and/or staffing if needed throughout the year. The OCFO has established policies and procedures for the approvals of requisitions and commitments related to CFPB's funds.

To process budgetary transactions and enforce fund controls, CFPB has entered into an inter-agency agreement for accounting services with the U.S. Department of the Treasury's Bureau of the Fiscal Service. Accounting services provided to CFPB include recording financial transactions, such as budget authority, allocations, collections, accounts receivable, commitments, obligations, accruals, accounts payable, disbursements, and journal entries. The Bureau of the Fiscal Service's automated accounting systems provide the budgeting and funds control at various organizational and spending levels, which are established at the request of the customer agency. To complement these fund controls, the CFPB has established a number of additional monitoring controls, such as monthly budget execution summary reports, quarterly OCFO reviews, and the mid-year budget review. In addition, the OCFO has established policies and procedures to perform a quarterly accrual analysis of obligations of $100,000 or greater to determine if goods and services were received.

Our methodology and approach for evaluating the budget process included the following procedures:

- Interviewing CFPB key budget personnel within the individual division/program offices and the OCFO regarding formulation, execution, and monitoring;
- Reviewing the policies and procedures for budget formulation, execution, and monitoring;
- Obtaining a further understanding of the budget formulation, execution and monitoring process through discussions with management of the OCFO and select CFPB divisions;

- Reviewing documents used to support the budget formulation process;
- Comparing the CFPB budget formulation, execution, and monitoring process to the applicable requirements and guidance in OMB Circular A-11 as an indicator of leading practice;
- Reviewing documents to support the fact that the fiscal year 2015 budget was discussed with the program offices, was reviewed and approved by CFPB's Director, and was widely communicated throughout the organization;
- Obtaining an understanding of the budget execution and monitoring process through discussions with OCFO management and select CFPB offices;
- Reviewing CFPB's support for its mid-year budget review, and
- Reviewing the user controls noted in the Bureau of Public Debt Service Organization Control report under Statement on Standards for Attestation (SSAE) No. 16: *Report on the Bureau of the Public Debt Administrative Resource Center's Description of its Financial Management Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2014 to June 30, 2015*, issued by KPMG, which performed this SSAE No. 16 attestation for the Bureau of Public Debt.

Our procedures did not identify any findings related to CFPB's budget process. However as a result of our procedures, we reported certain observations for CFPB's consideration in further enhancing it budget process in ***Appendix A – Additional Improvement Observations***. These observations are related to our 2015 audit of selected operations and budget, and are presented for the purpose of finalizing the results of that audit.

### *CFPB's Information Privacy Program*

Given the nature of CFPB's mission to make markets for consumer financial products and services work for Americans, and in consideration of the privacy issues related to these products, protecting PII maintained by CFPB is integral to its mission. The Bureau can be more effective in its mission where trust exists between consumers and the agency that works to protect them. The Chief Privacy Officer ("CPO") is responsible for all of the CFPB's privacy compliance and operational activities.

The CPO has created a privacy plan to address (1) the integration of privacy into all CFPB activities, (2) the provision of appropriate privacy training, (3) the management of incident response activities, and (4) on-going auditing and monitoring. Integration activities can range from participation in project planning, to contract reviews, to reviewing regulations for privacy impacts, and to integrating NIST controls. Privacy training is critical to educate all employees about the role they play in protecting the information the CFPB is charged with collecting. Each employee must understand their role in incident response activities and

the importance of reporting suspected incidents immediately. Finally, auditing and monitoring enables the CFPB to track and improve the effectiveness of these activities.

The privacy team has developed compliance documents, policies, procedures, guidance, training, and other staff resources. These governance documents help ensure accountability in the collection and handling of PII. Because the Bureau's work focuses on financial matters, PII often relates to financial products or services. This type of information is a subcategory of PII called personally identifiable financial information (PIFI). The CFPB's privacy plan addresses PIFI under the more general term PII.

Our methodology and approach for evaluating CFPB's privacy program included the following procedures:

- Conducted a kickoff and interviews with CFPB key privacy personnel within the privacy office and the OCFO regarding information privacy;
- Reviewed the policies and procedures for information privacy;
- Obtained an understanding of the privacy process through discussions with management of CFPB's OCFO and privacy team with in the Technology and Innovation divisions;
- Reviewed documents used to support the comprehensive privacy plan;
- Compared the CFPB privacy process to OMB Memorandum 03-22 *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, and the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* Appendix J: *Privacy Control Catalog* as an indicator of leading practice.

Refer to **Finding A** in the *Findings and Recommendations* section of this report for our findings and recommendations related to our privacy audit objective.

### *Corrective Actions Taken to Resolve the FY2014 Audit Report Findings and Recommendations*

CFPB developed corrective action plans to address the four prior year findings included in the *2014 Independent Audit of Operations and Budget* report.[3] Our methodology and approach for the corrective actions process included the following procedures:

- Reviewed the findings and related recommendations included in the *2014 Independent Audit of Operations and Budget*, which were defined as either a risk of deficiency or non-compliance or a deficiency in internal control;
- Obtained and reviewed the corrective action plan (CAP) developed by CFPB for the four findings mentioned above;

[3] *2014 Independent Audit of Selected Operations and Budgets, KPMG, February 25, 2014.*

- Reviewed documentation supporting the CFPB actions specified in the CAP and how the actions taken address the prior year findings, and
- Obtained management's approach for the disposition of the performance improvement observations identified in the above 2014 performance audit report.

The table below captures the status of the prior year findings based on the results of our 2015 performance audit procedures:

| 2014 Findings | 2014 Finding Type | 2015 Status |
|---|---|---|
| Oversight of SSAE 16 report for contractor responsible for payment processing | Control Deficiency | **Remediated** |
| Records management annual self-assessment process | Control Deficiency | **Remediated** |
| CFPB's OMB Circular A-123 procedures for centrally tracking of CFPB-wide deficiencies | Control Deficiency | **Remediated** |
| Improvements needed in the mid-year review process | Control Deficiency | **Remediated** |
| Controls over COR function need continued improvement | Control Deficiency | **Remediated** |

***Findings and Recommendations***

Our 2015 performance audit identified one internal control deficiency[4] finding, which is presented below. We discussed the results of the performance audit with CFPB's CFO, Deputy CFO, Budget Director, Counsel to the CFO, audit focus area leads, Chief Information Officer, Chief Privacy Officer, and Contracting Officer Representative for the audit contract. We held an exit conference on December 18, 2015.

**A. Information Privacy policies and procedures need to be updated**

*Condition:*

Based on the results of our procedures over CFPB's information privacy program, we noted the following conditions:

1. The Bureau currently has documented processes and procedures for assessing and obtaining data sets utilized by the program offices to ensure compliance with CFPB privacy policies. The current process for maintaining the inventory of these data sets is manually intensive. In an effort to improve transparency, the CFPB's Chief Data Office is transitioning from this manual process of tracking these data sets to an automated tool, referred to as the Data Catalog. However, the Bureau has not completed a full reconciliation between the data set records maintained by the Data Team and the actual data sets residing on CFPB systems.
2. While we noted that the Bureau plans to conform to National Archives and Records Administration (NARA) requirements for destruction of records at end-of-life, further detail in Bureau policies and procedures do not describe or require positive destruction of hardware that previously stored PII.

*Criteria:*

NIST SP 800-53, Revision 4, Appendix J, Control DM-1 *Minimization of Personally Identifiable Information* and Control DM-2 *Data Retention and Disposal* requires that agencies:

- Conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings to ensure that only PII identified in Appendix J, Control DM-1 is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

[4] *Government Auditing Standards*, 2011 Revision – Paragraph 6.2. **"**In performance audits, a deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met."

- Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- Ensure secure deletion or destruction of PII (including originals, copies, and archived records).

*Effect and Cause:*

Without a completely reconciled inventory of data sets in place, there is an increased risk that the Bureau may not be in compliance with its privacy policies and procedures. By not informing Bureau personnel of the expected methods of destroying storage that contains or contained PII, such storage may not be erased or destroyed at the appropriate level to assure "positive destruction," risking uncontrolled exposure of such data.

*Recommendations:*

To enhance control of information privacy in line with NIST and NARA requirements, we recommend that CFPB:

a. Complete its automated data cataloguing activities within the documented project timeframe, which should include evaluating the CFPB data sets maintained, and establishing policies and procedures to regularly review the data set inventory.

b. Update current privacy policies to include procedures and options available to assure positive destruction of storage that contains personally identifiable information.

## *Appendix A – Additional Improvement Observations*

Our current audit procedures did not identify any findings related to the IRB or the budget process. However as a result of our procedures, we reported certain observations for CFPB's consideration in further enhancing these processes, which are included here. These observations are related to our 2015 audit of selected operations and budget, and are presented for the purpose of finalizing the results of that audit.

Our additional observations are as follows:

1. *Investment Review Board:* CFPB division/program management could benefit from adopting certain guidance outlined in OMB Circular A-11, Appendix K, *Selected OMB Guidance and Other References Regarding Capital Assets* which includes a business case template and instructions for planning, budgeting, acquisition, and management of non-IT capital assets. The IRB's cost estimate process essentially follows OMB Circular A-11, with three exceptions, which we believe would further strengthen the IRB process. The three areas are alternative analysis, risk management, and performance information.

    a. CFPB's IRB may consider requiring in its policies and procedures guidance that division/program offices provide more robust alternatives analysis with each investment request. Such alternatives analysis could be used to evaluate the costs and the benefits of at least three alternatives and the status quo more effectively.

    b. CFPB may consider requiring a documented Risk Management Plan for each investment request. The Risk Management Plan could include a list of risks, the probability of occurrence of each risk, the impact of each risk, a mitigation strategy for each risk, and how the division/program office intends to actively manage risk throughout the lifecycle of the investment.

    c. CFPB may further improve the mapping of specific strategic goals or performance information to clearly identify how the investment support the agency's strategic goals.

2. *Budget Function:* We reviewed the fiscal year 2015 mid-year budget reviews and any resulting budget modifications for a sample CFPB's program offices. CFPB could benefit from introducing improvements to its cost estimation methodology and expanding the use of program performance information in its budget activities.

a. CFPB may consider using the Government Accountability Office (GAO) *Cost Estimating and Assessment Guide* (Cost Guide), March 2009 as a leading practice or otherwise improving its cost estimation methodologies. The GAO developed the Cost Guide to establish a consistent methodology that is based on best practices and that can be used across the federal government for developing, managing, and evaluating capital program cost estimates. Areas of improvement include development of assumptions and factors; look back analysis; and short and long term consideration of funding implications associated with cost estimates.

b. CFPB may consider expanding the use of program performance information, such as program evaluations, to better determine if programs are producing desired results with resources provided and improve the Bureau decisions during the budget and formulation and implementation.

## *Appendix B – CFPB's Management Response*

**Management Responses**

We provided a draft of this report to CFPB management for review and comment. CFPB's responses to our findings and recommendations are included in a letter from CFPB's Chief Financial Officer dated December 18, 2015. CFPB's responses were not subjected to the auditing procedures applied in the performance audit objectives relative to CFPB; accordingly, we expressed no opinion on these responses.

Consumer Financial Protection Bureau
1700 G Street, N.W., Washington, DC 20552

December 18, 2015

Mr. Jorge Asef-Sargent
KPMG, L.L.P.
1801 K Street, NW
Suite 12000
Washington, DC 20006

Dear Mr. Asef-Sargent,

Thank you for the opportunity to review and comment on KPMG, L.L.P.'s report *"Consumer Financial Protection Bureau Independent Audit of Selected Operations and Budget,"* for Fiscal Year 2015 dated December 18, 2015. We have reviewed the audit report and concur with the recommendations contained therein. As noted in the report, CFPB has successfully remediated all conditions from the 2014 and 2013 Independent Audits conducted by your firm.

We agree with the two identified conditions and accompanying recommendations in the 2015 audit report. My colleagues are already preparing to implement the proposed recommendations from the Privacy audit focus area. The comments on each condition and its associated recommendation in this letter provide additional detail on planned actions to enhance the processes and controls in the Privacy audit focus area.

Furthermore, in an effort to enhance the Bureau's operations and to address the performance improvement opportunities in the audit focus areas that KPMG studied, the Bureau will evaluate how best to incorporate the observed opportunities for improvement in the Budget and Investment Review Board (IRB) audit focus areas into the existing policies and procedures of these audit focus areas.

Thank you again for your review.

Sincerely,

Stephen J. Agostini

Stephen J. Agostini
Chief Financial Officer

**Auditor Condition 1: CFPB's Privacy Function**

*Condition: The Auditor noted that the CFPB currently has documented processes and procedures for assessing and obtaining data sets utilized by the program offices to ensure compliance with CFPB privacy policies. The current process for maintaining the inventory of these data sets is manually intensive. In an effort to improve transparency, the CFPB Data Team is transitioning from this manual process of tracking these data sets to an automated tool, referred to as the "Data Catalogue". However, the Bureau has not completed a full reconciliation between the data set records maintained by the Data Team and the actual data sets residing on CFPB systems.*

**CFPB Response:** The CFPB agrees with the Condition described above.

**Auditor Recommendation(s) Related to Condition 1: CFPB's Privacy Function**

*Recommendation: The Auditor recommends that CFPB complete its automated data cataloguing activities within the documented project timeframe which should include conducting an evaluation of CFPB data sets maintained and the establishment of policies and procedures to regularly review the inventory of those data sets.*

**CFPB Response:** The CFPB agrees with the recommendation described above. The Chief Data Officer's team will complete the cataloging of data set records maintained by the Bureau in an automated system. By the end of FY 2016, CFPB will establish policies and procedures with respect to the regular review of data set inventory.

**Auditor Condition 2: CFPB's Privacy Function**

*Condition: The Auditor noted that the Bureau plans to conform to National Archives and Records Administration (NARA) requirements for destruction of records at end-of-life. However, the current Bureau policies and procedures do not describe or require positive destruction of hardware that previously stored PII.*

**CFPB Response:** The CFPB agrees with the Condition described above.

**Auditor Recommendation(s) Related to Audit Condition 2: CFPB's Privacy Function**

*Recommendation: The Auditor recommends that CFPB update current privacy policies to include procedures and options available to assure positive destruction of storage that contains personally identifiable information.*

**CFPB Response:** The CFPB agrees with the auditor's recommendation to update its Privacy policies, including the documentation of data destruction. The data sets referenced by this audit must generally be maintained by the Bureau for 10 years after the date of intake. By the end of FY 2016, the CFPB will finalize and document these policy and procedural revisions, which should remediate the observed condition.