



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 21, 2012

The Honorable Richard Cordray
Director
Bureau of Consumer Financial Protection

Subject: *Management Report: Opportunities for Improvement in the Bureau of Consumer Financial Protection's Internal Controls and Accounting Procedures*

Dear Mr. Cordray:

In November 2011, we issued our opinion on the Bureau of Consumer Financial Protection's (CFPB) fiscal year 2011 financial statements. Our report also included our opinion on the effectiveness of CFPB's internal control over financial reporting as of September 30, 2011, and our evaluation of CFPB's compliance with provisions of selected laws and regulations for the fiscal year ended September 30, 2011.¹

Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act,² referred to as the Consumer Financial Protection Act of 2010, created CFPB. The act charged it with the responsibility of regulating the offering and provision of consumer financial products or services under the federal consumer financial laws. The act also requires CFPB to annually prepare financial statements, and further requires GAO to audit these statements. The Full-Year Continuing Appropriations Act, 2011, also requires that GAO audit CFPB's financial statements. While CFPB began operations in 2010, fiscal year 2011 was its first full year of operations. As a newly established entity, CFPB spent the majority of fiscal year 2011 forming its structure and commencing operations.

The purpose of this report is to present additional information on the internal control and accounting procedure issues we identified during our audit of CFPB's fiscal year 2011 financial statements and to provide our recommended actions to address those issues. We are making 10 recommendations for strengthening CFPB's internal controls and accounting procedures.

¹ GAO, *Financial Audit: Bureau of Consumer Financial Protection's Fiscal Year 2011 Financial Statements*, GAO-12-186 (Washington, D.C.: Nov. 15, 2011).

² Pub. L. No. 111-203, Title X, 124 Stat. 1955 (July 21, 2010).

In addition, because of the sensitive nature of some of our findings related to CFPB information security, we will present our findings and recommendations setting out corrective actions to address issues we identified concerning CFPB's internal control over information security in a separate letter to CFPB management with limited distribution.

Results in Brief

During our audit of CFPB's fiscal year 2011 financial statements, we identified seven internal control issues that could adversely affect CFPB's ability to meet its internal control objectives. We do not consider these issues to represent material weaknesses or significant deficiencies³ in relation to CFPB's financial statements. Nonetheless, we believe they warrant management's attention and action. These issues concern necessary controls to ensure

- complete and finalized documentation of CFPB's accounting processes and procedures,
- an effective internal control assessment process supporting management's internal control assertion,
- security over CFPB's data and information systems,
- accurate calculation and timely recording of CFPB undelivered orders balances,
- accurate calculation and timely disbursement of CFPB payroll transactions,
- proper prior approval of CFPB travel transactions, and
- timely recording of CFPB prepaid expenses as assets.

These issues increase the risk of CFPB not preventing or promptly detecting and correcting (1) misappropriation of assets because of reliance on insufficient internal controls; (2) unauthorized access, modification, or both of its data; and (3) misstatements in its financial statements. At the end of our discussion of each of these issues in the sections that follow, we present our related recommendations. These recommendations are intended to improve management's oversight and controls and minimize the risk of misappropriation of assets, misstatements in CFPB's accounts and financial statements, and unidentified vulnerabilities over the security of its data.

³ A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. 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, misstatements on a timely basis.

In providing written comments on a draft of this report, CFPB concurred with our findings and corresponding recommendations. While CFPB stated that it has implemented, or is in the process of implementing, actions to address the issues discussed in this report, it did not specifically address each finding and recommendation in its written comments. CFPB's comments are summarized at the end of this report and reproduced in their entirety in enclosure I.

Scope and Methodology

As part of our audit of CFPB's fiscal year 2011 financial statements, we evaluated CFPB's internal controls and tested its compliance with selected provisions of laws and regulations. We designed our audit procedures to test relevant controls over financial reporting, including those designed to provide reasonable assurance that transactions are properly recorded, processed, and summarized to permit the preparation of CFPB's financial statements in conformity with U.S. generally accepted accounting principles.

We performed our audit of CFPB's fiscal year 2011 financial statements in accordance with U.S. generally accepted government auditing standards. We believe that our audit provided a reasonable basis for our conclusions in this report. Further details on our audit methodology are presented in enclosure II.

Accounting Policies and Procedures

As fiscal year 2011 was CFPB's first full year of operations, our audit found that CFPB's policies and procedures were not yet fully documented and finalized, which is typical of any newly established entity. Specifically, many of CFPB's policies and procedures were in draft form and had not yet been approved by CFPB management. Furthermore, they did not include all steps and personnel involved in initiating, authorizing, approving, recording, and summarizing and reporting CFPB's various transactions, nor were all of CFPB's accounting policies and procedures documented. This increased the difficulty of assessing CFPB's control environment for management, led to deficiencies in CFPB's performance and evaluation of certain information system security internal control activities, and contributed to errors in the processing of CFPB's undelivered orders and expense transactions.

For example, CFPB's documented accounting policies and procedures as of fiscal year-end did not include all of the accounting policies and procedures governing the activities that the Bureau of the Public Debt Administrative Resource Center (BPD-ARC), a Department of the Treasury (Treasury) franchise fund⁴, performed for CFPB

⁴ A franchise fund is a type of statutorily established intragovernmental revolving fund that operates as a self-supporting entrepreneurial entity to provide common administrative services benefiting other

pursuant to an agreement. In September 2010, CFPB entered into a reimbursable services agreement with BPD-ARC for certain accounting services.⁵ While BPD-ARC staff process CFPB transactions, CFPB is ultimately responsible for ensuring that the amounts, transactions, and balances are properly recorded, complete, and fairly presented in its financial statements and other financial reports. Therefore, CFPB's policies and procedures should include, or incorporate by reference, BPD-ARC's accounting policies and procedures. Furthermore, CFPB's documented policies and procedures should clearly delineate BPD-ARC's roles and responsibilities for processing CFPB's transactions and CFPB's roles and responsibilities for monitoring the work performed by BPD-ARC.

*Standards for Internal Control in the Federal Government*⁶ provides that control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. The standards also provide that internal control activities are to be clearly documented and that the documentation should appear in management directives, administrative policies, or operating manuals.

The lack of finalized policies and procedures could lead to transactions being inaccurately recorded in, or omitted from, CFPB's general ledger and ultimately its financial statements. Furthermore, without finalized policies and procedures, CFPB cannot ensure that control activities are carried out in accordance with management's intent or in accordance with applicable laws and regulations.

Recommendation

We recommend that you direct the Chief Financial Officer to finalize and approve CFPB's documented accounting policies and procedures to include requirements for thoroughly documenting all key accounting policies and procedures, clearly defining those performed by BPD-ARC and those performed by CFPB, and identifying the personnel responsible for executing these processes to ensure accountability.

federal entities. Franchise funds function entirely from the fees charged for the services they provide consistent with their statutory authority. The Consolidated Appropriations Act, 2005, established Treasury's franchise fund as a permanent indefinite appropriation. See Pub. L. No. 108-447, § 219, 118 Stat. 2809, 3242 (Dec. 8, 2004) (reprinted in 31 U.S.C. § 322 note).

⁵ BPD-ARC provides CFPB with accounting services in several areas, including procurement, accounts payable, accounts receivable, budget execution, travel, and financial reporting.

⁶ GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

Internal Control Assessment Process

During our audit of CFPB's fiscal year 2011 financial statements, the entity's first full year of operations, we found that CFPB's process for assessing the effectiveness of its internal control over financial reporting was not sufficient to fully support management's conclusions regarding the effectiveness of CFPB's internal control over financial reporting. Specifically, we identified deficiencies regarding CFPB's internal control testing, consideration of certain information security controls to CFPB's control environment, and CFPB's review of its compliance with laws and regulations. Such weaknesses are not unexpected for any entity in its first year of operation.

The Consumer Financial Protection Act requires CFPB to provide to the Comptroller General of the United States an assertion as to the effectiveness of its internal controls over financial reporting based on the standards established in 31 U.S.C. § 3512 (c), commonly known as the Federal Managers' Financial Integrity Act of 1982. Furthermore, the Office of Management and Budget's (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, provides that federal agencies are to assess the extent to which their internal control provides reasonable assurance that the following objectives are being achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations.

In August 2011, CFPB executed a 2-year contract for accounting and internal control support services and awarded a task order under the contract for the contractor to (1) develop an inventory of CFPB programs and associated risks and control activities, (2) perform a risk assessment for each key process, (3) determine and document existing controls, (4) determine whether existing controls were sufficient, (5) identify any policies or procedures in place to offset potential risks, and (6) provide specific recommendations to improve controls. As of fiscal year-end, the contractor was not able to complete its planned testing on four of the nine key process areas identified. Because the contractor did not begin work until August and CFPB's fiscal year-end is September 30, the time allotted for the contractor to perform the internal control review was limited. However, for the testing that was not complete, the contractor concluded that the open issues were minor and that for the processes for which it completed work, CFPB's internal control over financial reporting was operating effectively.

CFPB also developed an internal control review plan for assessing its internal control. As part of the plan, CFPB incorporated elements of the GAO *Internal Control Management and Evaluation Tool*⁷ with respect to the five components of internal

⁷ GAO, *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.: August 2001). This tool is intended to assist agencies in maintaining or implementing effective internal controls and, when needed, to help determine what, where, and how improvements can be implemented.

control: the control environment, control activities, risk assessment, information and communication, and monitoring. However, our review determined that CFPB's analysis of the five components of internal control did not consider all key internal controls related to CFPB's information security. Specifically, CFPB determined that it did not need to assess control activities related to an entity-wide security management program, including access controls, application software development, system software controls, service continuity, and control over integrity of processing and data files, because the systems related to these control activities were owned and operated by another agency under a service agreement.⁸ However, OMB Circular No. A-123, in reference to the Federal Information Security Management Act of 2002 (FISMA),⁹ provides that agency heads are required to annually report on the effectiveness of their agency's information security programs, including systems and data controlled and carried out by service providers on behalf of that agency. Therefore, the design and effectiveness of these control activities should have been evaluated by CFPB.

Further CFPB's internal control review plan for assessing compliance with key laws and regulations applicable to the bureau's operations was not comprehensive as it did not include all key laws related to CFPB's operations with respect to financial reporting. CFPB explained that the compliance schedule was not compiled until September 2011, which did not allow adequate time to review it to ensure its completeness.

Standards for Internal Control in the Federal Government provides that internal control should provide for an assessment of the risks an agency faces from both external and internal sources and that internal control should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. While CFPB did provide an assertion as to the effectiveness of its internal control over financial reporting, our review found areas in which CFPB needs to enhance and strengthen the process and documentation supporting its assertion. Deficiencies in CFPB's processes for assessing internal controls can lead to inappropriate conclusions as to the effectiveness of its internal controls, which could in turn lead to CFPB relying on insufficient internal controls over financial reporting.

⁸ As a newly established entity, CFPB spent the majority of fiscal year 2011 forming its structure and commencing operations. To assist in this process, in September 2010 CFPB entered into an interagency agreement with the Treasury's departmental offices for administrative and operational support in a variety of areas, including information system infrastructure. Also, in September 2010, CFPB entered into a reimbursable services agreement with BPD-ARC to provide administrative accounting services.

⁹ FISMA was enacted as Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002), and the FISMA requirements for agencywide security programs are codified at 44 U.S.C. § 3544.

Recommendation

We recommend that you direct the Chief Financial Officer to augment CFPB's internal control review procedures to include (1) all components of CFPB controls (including controls over financial reporting services provided to CFPB), (2) all key laws and regulations governing CFPB's financial reporting functions, and (3) monitoring steps to ensure procedures are completed in time for management to consider in its required annual internal control assertion.

Information Security Program

During our audit of CFPB's fiscal year 2011 financial statements, we found that CFPB, contrary to the provisions of FISMA, had not developed, documented, and implemented an agencywide program to provide information security for the information and information systems that support the financial reporting, operations, and assets of the bureau, including those systems provided or managed by its service provider organizations.¹⁰ We identified several information systems vulnerabilities related to its controls over financial reporting. Specifically, CFPB had not ensured that its service providers consistently or fully implemented controls for (1) authenticating users, (2) authorizing access to resources, (3) managing system configurations, and (4) protecting system and network boundaries on information systems owned and operated on behalf of CFPB by service provider organizations. In addition, CFPB had not yet established an information security program that included a clear delineation of the roles and responsibilities of CFPB and those of its service providers. In our review, we found the following vulnerabilities resulting from the lack of an overall information security program:

- **Controls were not consistently implemented for authenticating users.** A computer system needs to be able to identify and authenticate each user so that activities on the system can be linked and traced to a specific individual. An organization does this by assigning a unique user account to each user, and in so doing, the system is able to distinguish one user from another—a process called identification. The system also needs to establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as

¹⁰ FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets to strengthen the security of information systems within federal agencies. The agency's information security program required under FISMA applies not only to information systems used or operated by an agency but also to information systems used or operated by a contractor or other service provider on behalf of an agency. Security requirements for service providers should be expressed in appropriate contracts or agreements. The level of trust an agency can apply to the external provider depends on a variety of factors, including the extent to which the agency can monitor and verify the security controls of the provider. If the level of trust in the external provider does not meet expectations, the agency must employ compensating security controls, accept a greater degree of risk, or not use the service provider. Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of service providers remains with the authorizing official of the originating agency.

authentication. The combination of identification and authentication—such as user account-password combinations—provides the basis for establishing individual accountability and for controlling access to the system. However, CFPB did not ensure that appropriate password management controls were implemented on key systems we reviewed. As a result, an increased risk exists that accounts could be compromised and used by unauthorized individuals to access sensitive information.

- **Weaknesses in authorization controls limited their effectiveness.** Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of “least privilege.” Least privilege is a basic principle for securing computer resources and data that means that users are granted only those access rights and permissions that they need to perform their official duties. However, users were granted excessive levels of access privileges and permissions that were not required to perform their job. As a result, data could be inappropriately modified, either inadvertently or deliberately.
- **Systems were not always securely configured.** Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit a software vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against systems at another organization. Nevertheless, servers for systems used by CFPB had not been routinely and consistently patched in a timely manner. In addition, network vulnerabilities existed on multiple network devices. Failing to apply critical patches and the appropriate configuration settings for systems and network devices increases the risk of exposing systems to vulnerabilities that could be exploited.
- **System boundaries were not sufficiently protected.** Boundary protection involves the protection of a logical or physical boundary around a set of information resources and implementation of measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology at the network level. However, firewalls operating on systems we reviewed did not appropriately restrict access to the systems. These weaknesses increase the risk that malicious activity could occur and escape detection.

FISMA states that agencies should develop, document, and implement an agency-wide information security program that includes periodic risk assessments; policies and procedures that include related security plans; periodic management testing and evaluation of all major systems; a remedial action process to address any deficiencies found during monitoring and testing; procedures for detecting, reporting, and responding to security incidents; security awareness training for agency employees, contractors, and other service providers; and continuity of operations plans and procedures for information systems. However, CFPB did not have a program in place that addressed these requirements. For example, CFPB did not assess the risks associated with the information systems of its service providers, including BPD-ARC, which serves as CFPB's accounting service provider. Moreover, in September 2010 CFPB entered into an interagency agreement with Treasury's departmental offices for administrative and operational support in a variety of areas, including information system infrastructure. For example, CFPB utilized Treasury's wide area and local area network communications services and desktop computer resources. However, CFPB did not perform a risk assessment of its service providers because it did not consider certain internal controls related to information security to be applicable to the bureau since it did not own these systems. Because it was newly established, CFPB was in the process of drafting policies and procedures addressing the security of its information systems; however, none had been finalized as of September 30, 2011. Until CFPB develops, documents, and fully implements its information security program, including clearly delineating the roles and responsibilities of its service providers, its financial systems and the information they contain will be subject to increased risk of unauthorized access, use, disclosure, modification, disruption, and destruction.

Recommendation

We recommend that you direct the Chief Information Officer to establish an agency-wide information security program in accordance with FISMA guidance. Such a program should clearly delineate the roles and responsibilities of CFPB and its service providers in maintaining effective security over the systems and information CFPB relies on for its financial reporting. Specifically, this program should include provisions for periodic CFPB risk assessments; policies and procedures that include related security plans; periodic management testing and evaluation of all major systems; a remedial action process to address any deficiencies found during monitoring and testing; procedures for detecting, reporting, and responding to security incidents; security awareness training for agency employees, contractors, and other service providers; continuity of operations plans and procedures for information systems; and a process for evaluating the information system security of any and all service providers.

Additionally, in a separate letter with limited distribution, we are providing specific details of the technical weaknesses identified above and are making additional recommendations to enhance CFPB's internal control over information security.

Undelivered Orders

During our audit of CFPB's fiscal year 2011 financial statements, we found that the bureau's controls, and those of its service provider, were not fully effective in ensuring that certain budgetary transactions were accurately and timely recorded. Specifically, we found that transactions affecting the bureau's undelivered orders¹¹ balances were not always recorded accurately and timely in the general ledger.

For example, we found that CFPB executed a procurement contract for the purchase of computer equipment in the amount of nearly \$1.2 million on July 22, 2011, but the obligation¹² amount was not included in the undelivered orders balance at July 31, 2011. As discussed previously, CFPB entered into a reimbursable services agreement with BPD-ARC for certain accounting services, including procurement services. With respect to procurement services, BPD-ARC staff serve as CFPB's contracting officers and input CFPB's obligations into the accounting system. BPD-ARC officials explained that funds are to be obligated at the time the award document is signed and that the obligation is recorded in the accounting system when transactions are approved in the Procurement Request Information System Management (PRISM) system.¹³ However, in this instance a BPD-ARC contracting officer erroneously released the award transaction. Consequently, the obligation was not recorded in the accounting system and not included in the July 31, 2011, undelivered orders balance. The error was found in August 2011 when CFPB received the first invoice to be paid on this obligation. The BPD-ARC contracting officer determined that the obligation had not been recorded in the accounting system and subsequently approved the award in PRISM. BPD-ARC contracting officers are not explicitly required to compare the contract award date and the date the obligation is recorded in PRISM to ensure that they are consistent.

In addition, we found that the undelivered orders balance for a travel relocation transaction was overstated by nearly \$145,000 at fiscal year-end. BPD-ARC officials explained that the error occurred when a travel relocation technician was amending the obligation. The relocation technician inaccurately obligated additional funds to the travel authorization's September 30, 2011, balance. The relocation technician realized the error on the same day that the amount was posted and deobligated¹⁴ the \$145,000. However, the deobligation was incorrectly recorded in fiscal year 2012, and thus did not correct the overstatement to the 2011 fiscal year-end undelivered orders balance caused by the initial error. According to BPD-ARC, relocation technicians are instructed to review amendments to obligations to ensure the accuracy of the obligation balance. However, the relocation technicians' review

¹¹ Undelivered orders are the value of goods and services ordered and obligated but not received.

¹² An obligation is a definite commitment that creates a legal liability of the government for the payment of goods and services ordered or received.

¹³ Oracle contains CFPB's general ledger system, and PRISM is used to record CFPB's procurement transactions. Obligations are recorded in the general ledger through a real-time interface between PRISM and Oracle.

¹⁴ Deobligation refers to an agency's cancellation or downward adjustment of previously incurred obligations.

does not require the technicians to ensure that the amendments are recorded in the proper period.

Standards for Internal Control in the Federal Government provides that control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives. The standards also provide that agencies are to ensure accurate and timely recording of transactions. Deficiencies with respect to the accurate and timely recording of contract/obligation activity can lead to misstatements in undelivered orders balances reported in CFPB's financial statements.

Recommendations

We recommend that you direct the Chief Financial Officer to

- implement procedures to ensure that contracting officers verify that the date an obligation is recorded in PRISM corresponds to the date that the contracting officer signed the official obligating document and
- implement procedures to ensure that amendments to travel relocation obligations are recorded in the proper period as part of ensuring the accuracy of obligation balances.

Calculation of Payroll Transactions

The Consumer Financial Protection Act permits certain CFPB employees transferred from other federal agencies to elect to remain enrolled in their existing defined benefit and defined contribution retirement plans; further, for those employees who so elect, the act requires CFPB to make any required employer contributions to the employees' retirement plans.¹⁵ During our testing of payroll transactions conducted as part of our fiscal year 2011 audit, we found that CFPB did not have controls in place to ensure that required retirement benefit contributions were made. Specifically, we found that CFPB did not originally make the required agency contributions, nor in some instances the employee deductions, to the Thrift Savings Plan (TSP), other non-TSP defined contribution retirement plans (non-TSP retirement plans), or the Federal Insurance Contributions Act (FICA) tax for eight employees.

CFPB has entered into a reimbursable services agreement with BPD-ARC to assist with hiring employees and recording payroll disbursements, and with the Department of Agriculture's (USDA) National Finance Center (NFC), a USDA working capital

¹⁵ 12 U.S.C. § 5584(i), Benefits for Certain Transferred Personnel.

fund,¹⁶ to process payroll disbursements. Employees transferred from several other agencies to work at CFPB. The Consumer Financial Protection Act provided employees who transferred from other agencies¹⁷ with the option to continue participation in some of the transferring agencies' non-Title 5 retirement and other benefits programs,¹⁸ such as medical, vision, dental, long-term disability, and life insurance plans, for a defined period of time. Unless they elected otherwise, employees who transferred to CFPB were to remain enrolled in their respective retirement plans as of the date of transfer. The transferring agencies would continue to administer the non-Title 5 benefit programs for those transferred employees, and upon conclusion of the defined period of time, the employees had the option to enroll in non-Title 5 benefits programs sponsored by CFPB. Furthermore, CFPB was required to pay any employer contributions to the existing retirement plan of each transferred employee. These requirements created a complex payroll structure for CFPB.

During our testing of CFPB's payroll expense transactions, we identified a contribution problem with an employee who transferred from the Federal Deposit Insurance Corporation (FDIC) and was enrolled in both the TSP and the FDIC Savings Plan, a non-TSP retirement plan, at the time of transfer. We found that CFPB did not make the mandatory 1 percent contribution and the matching 4 percent contribution to this employee's TSP.¹⁹ We also found that CFPB did not make the matching contribution to the employee's FDIC Savings Plan (the non-TSP retirement plan). According to FDIC, the FDIC Savings Plan required matching agency contributions up to 5 percent of the employee's adjusted basic pay. According to CFPB, year-to-date contribution amounts were entered incorrectly into the NFC system by FDIC personnel for both retirement plans, causing it to appear as though the employee's contribution total exceeded the annual tax deferral limit for retirement plan contributions. Consequently, NFC did not withhold the employee deductions or agency matching contributions for the two pay periods affected. BPD-ARC became aware of the agency contribution errors while processing payroll transactions for CFPB. Prior to our testing, CFPB worked with BPD-ARC and NFC to

¹⁶ A working capital fund is a type of agency intragovernmental revolving fund, which conducts a regular cycle of businesslike activities and operates entirely from the proceeds of fees charged to federal entities for their goods or services. NFC is a USDA working capital fund that provides administrative and financial services to many federal agencies, including CFPB. CFPB forwards personnel and payroll data to NFC so that NFC can process CFPB's payroll.

¹⁷ The agencies from which CFPB employees were transferred include the Board of Governors of the Federal Reserve System, the Federal Reserve Banks, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Department of Housing and Urban Development.

¹⁸ Title 5 of the U.S. Code outlines benefit programs for the majority of the federal workforce, in which programs are typically administered by the Office of Personnel Management. Non-Title 5 benefits are those benefits not covered under Title 5. For those CFPB employees participating in non-Title 5 benefit programs, CFPB states that it contracts directly with vendors to provide those services.

¹⁹ For employees in the Federal Employees Retirement System, an agency will contribute an amount equal to 1 percent of an employee's basic pay each pay period to a TSP account. These are called Agency Automatic 1% Contributions, and the employee does not need to be making employee contributions to receive them. In addition, based on the employee's contribution election, the agency will also provide matching contributions on the first 5 percent of an employee's basic pay each pay period to a TSP account.

correct these issues. By the end of November 2011, CFPB had retroactively collected the employee contributions and made the missed agency contributions to the transferred FDIC employee's TSP. However, as of February 2012, CFPB had not collected the employee contributions or made the matching agency contributions to the employee's non-TSP retirement plan.

Similarly, we found that CFPB did not make the mandatory 1 percent contribution to two other transferred employees' non-TSP retirement plans. According to CFPB, NFC's system was not programmed to process certain codes assigned to transferred employees, resulting in missed agency contributions. During February 2012, CFPB paid the missed contributions to the two transferred employees' non-TSP retirement plans.

In addition, we found that CFPB did not make FICA contributions, as required by the Social Security Act of 1935, for five employees transferred from the Federal Reserve System for two pay periods tested. Also, for these five employees, CFPB did not properly deduct the employee portion for FICA contributions from each of their pay. According to CFPB, NFC had not modified its procedures to enable its systems to process FICA contributions for the group of employees that transferred from the Federal Reserve System. BPD-ARC was aware of the FICA errors prior to our testing and worked with CFPB and NFC to resolve the programming issues. However, throughout October 2011, CFPB paid the missed FICA payments for four of the employees who transferred from the Federal Reserve System.²⁰ By December 2011, CFPB ensured that the employee portion of the missed FICA payments was retroactively collected from each of these employees.

Moreover, we reviewed the entire population of employees who transferred from the Federal Reserve System for the two pay periods affected by the programming issue and identified additional employees for whom CFPB did not make FICA contributions. For these employees, CFPB also did not properly deduct the employee portion for FICA contributions from these employees' pay. Since BPD-ARC was aware of the FICA errors, it worked with CFPB and NFC to identify employees who transferred from the Federal Reserve System for the two pay periods affected by the programming issue. By December 2011, CFPB paid the corresponding missed FICA contributions. CFPB also recouped the employee portion of the missed FICA payments from the employees affected.

Standards for Internal Control in the Federal Government provides that agencies are to ensure accurate and timely recording of transactions. The standards also state that monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. In addition, USDA's Office of Inspector General (IG) conducts an annual audit of NFC's internal control structure in accordance with the American Institute of Certified Public

²⁰ The fifth employee had already reached the maximum contribution amount required for FICA. Therefore, no collection for missed FICA payments was necessary.

Accountants Statement on Standards for Attestation Engagements (SSAE) No. 16 and issues a report (an SSAE 16 report). In its 2011 SSAE 16 report on NFC, the IG issued an unqualified opinion and reported no material weaknesses in internal control.²¹ However, the IG reported that user entities should establish controls or procedures to complement those at NFC. Although CFPB had draft payroll policies and procedures, these policies and procedures did not include controls that would have promptly detected these types of errors. Given CFPB's complex payroll structure and the significant amount of hiring that occurred at the end of fiscal year 2011, CFPB should have established controls to verify the accuracy of its payroll transactions.

Deficiencies with respect to controls over CFPB's payroll processing procedures can increase the risk of misstating expenses in its financial statements. In addition, deficiencies in payroll processing can lead to inaccurate employee compensation, withholdings, and accumulation of benefits.

Recommendation

We recommend that you direct the Chief Financial Officer to strengthen payroll policies and procedures by including steps to follow to (1) test individual payroll transactions to ensure that transactions processed by NFC are properly programmed and disbursed and (2) ensure that NFC promptly corrects any identified errors in payroll disbursements.

Documentation to Support the Approval of Travel Expenses

During our testing of expense transactions conducted as part of our fiscal year 2011 audit, we found that CFPB employees did not always obtain prior written approval for all reimbursed travel expenses. Specifically, we found that a senior CFPB employee was reimbursed nearly \$4,000 for fees paid for two individuals to attend a conference that were not included on the related travel authorization. In this instance, the travel voucher for the traveling CFPB employee included a reimbursement claim in the amount of nearly \$2,000 for the conference fees of another CFPB employee. A CFPB official explained that the employee received oral approval from a senior executive to attend the conference along with another CFPB employee. We identified another instance for the same senior CFPB employee where a conference fee in the amount of about \$500 was omitted from the travel authorization, but the employee was still reimbursed for the expense.

²¹ Department of Agriculture, Office of Inspector General, *Audit Report: Statement on Standards for Attestation Engagements No. 16 Report on Controls at the National Finance Center*, Report No. 11401-2-11 (Washington, D.C.: Sept. 23, 2011).

Standards for Internal Control in the Federal Government provides that internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. In reviewing CFPB's travel policy, entitled "Use of Limited Open Travel Authorizations and Travel Cards for Temporary Duty Travel," which was still in draft at the time of our testing, we found that it did not specifically include requirements for obtaining prior written approval for all travel expenses. However, the draft policy also incorporates by reference the Federal Travel Regulation (FTR),²² which under part 301-71, provides that conference rates are to be included on the travel authorizations and approved prior to travel.

Deficiencies with respect to requiring the prior approval and maintenance of related written documentation to support prior authorization of travel expenses can result in CFPB incurring inappropriate expenses.

Recommendations

We recommend that you direct the Chief Financial Officer to

- enhance CFPB's travel policies and procedures to expressly state that prior written approval be obtained for all reimbursed travel expenses and
- issue a memorandum to all staff on CFPB's policy on obtaining prior written approval for all reimbursed travel expenses.

Process for Recording Prepaid Expenses

During our testing of expense transactions conducted as part of our fiscal year 2011 audit, we found that CFPB's process for recording prepaid expenses did not ensure that assets and expenses were recorded in the proper period in a timely manner. Specifically, we found that a CFPB subscription with a period of performance spanning 2 fiscal years was initially fully expensed in fiscal year 2011. Prepaid expenses represent future economic benefits that are paid in advance of their use or consumption. The subscription we identified was for access to financial information for fiscal years 2011 and 2012, beginning at the end of May 2011. Accordingly, the subscription needed to be allocated on a systematic basis to recognize the cost over the entire period of benefit.

During fiscal year 2011, CFPB's procedure for identifying prepayments was through a post-payment review process conducted at fiscal year-end during which CFPB reviewed its expense accounts to identify any transaction that should be reclassified as a prepayment. Therefore, under this process, prepaid expenses that should have

²² The FTR, 41 C.F.R. chs. 300 to 304, is the regulation that implements statutory requirements and executive branch policies for travel by federal civilian employees and others authorized to travel at government expense.

been reclassified as assets would incorrectly be recorded and reported as expenses in CFPB's accounts and interim financial statements throughout the fiscal year. In this instance, the fiscal year 2012 portion of the subscription expense, nearly \$206,000, was eventually reclassified as an asset in October 2011.

Furthermore, the initial recording of a transaction should be to the correct general ledger account. BPD-ARC accounting technicians process invoices for payment on behalf of CFPB. A BPD-ARC accounting technician sends a copy of the invoice and an invoice approval form to the assigned CFPB contracting officer technical representative (COTR)²³ for review and approval prior to payment. However, CFPB's COTRs are not required to inform the BPD-ARC accounting technician that the transaction amount should be recorded as a prepayment as part of this review and approval process. Therefore, when an invoice is paid, the prepaid portion of the expense is initially recorded to an expense account rather than to an asset account.

Standards for Internal Control in the Federal Government provides that agencies are to ensure the timely recording of transactions. Furthermore, in accordance with the Consumer Financial Protection Act, CFPB is required to submit quarterly financial statements to the Director of OMB. Deficiencies with respect to the timely recording of prepayment transactions can lead to misstatements in asset balances and expense amounts reported in CFPB's interim accounts and financial statements.

Recommendations

We recommend that you direct the Chief Financial Officer to

- modify CFPB's existing procedures over the post-payment review process to require that CFPB conduct such reviews at least quarterly and
- incorporate into CFPB's policies and procedures the requirement for its COTRs to indicate on the invoice approval form whether a transaction should be classified as a prepayment.

Agency Comments

In the written comments provided on a draft of this report, CFPB stated that it is committed to continuously improving its internal control environment as the agency continues to build its staffing, structure, and processes. CFPB concurred with our recommendations and further stated that it has implemented, or is in the process of implementing, actions to address the issues discussed in this report. Such actions include developing and implementing policies and procedures, working with service providers to ensure that their controls are complementary to those of CFPB,

²³ COTRs perform critical acquisition and technical functions, and contracting officers rely on them to ensure that contracts and other acquisition agreements are managed properly.

monitoring the timely correction of identified errors, and implementing additional information security controls. We will evaluate CFPB's actions to address these issues as part of our fiscal year 2012 audit. CFPB's written comments are reprinted in enclosure I.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on actions taken on these recommendations. You should submit your statement to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform within 60 days of the date of this report. A written statement must also be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

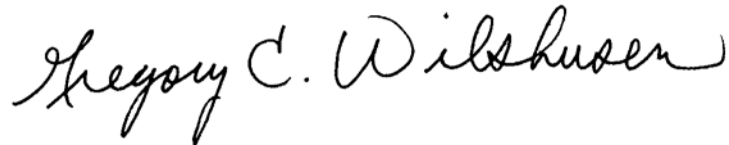
This report is intended for use by CFPB management. We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Banking, Housing, and Urban Affairs; the House Committee on Financial Services; the Senate Committee on Appropriations; and the House Committee on Appropriations, and to the Secretary of the Treasury, the Director of the Office of Management and Budget, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

We acknowledge and appreciate the cooperation and assistance provided by CFPB management and staff during our audit of CFPB's fiscal year 2011 financial statements. If you have any questions about this report or need assistance in addressing these issues, please contact Steven J. Sebastian at (202) 512-3406 or sebastians@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Sincerely yours,



Steven J. Sebastian
Managing Director
Financial Management and Assurance



Gregory C. Wilshusen
Director
Information Security Issues

Enclosures – 2

Enclosure I: Comments from the Bureau of Consumer Financial Protection



1700 G Street NW, Washington, DC 20552

May 10, 2012

Mr. Steven Sebastian
Managing Director
Financial Management and Assurance

Mr. Gregory C. Wilshusen
Director
Information Security Issues

U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Mr. Sebastian and Mr. Wilshusen,

We have received a copy of your draft *Management Report: Opportunities for Improvement in the Bureau of Consumer Financial Protection's Internal Controls and Accounting Procedures*, covering the Consumer Financial Protection Bureau's (CFPB) financial statement audit as of September 30, 2011. We appreciate the cooperation of the Government Accountability Office (GAO) during the CFPB's first annual financial statement audit, and we recognize very clearly how the work you are doing will improve our performance and accountability, which we take very seriously.

The CFPB is proud that in its first year of preparing financial statements, we received an "unqualified" or "clean" opinion of those financial statements and that the GAO noted that the CFPB's internal control was found to be effective, with no material weaknesses or significant deficiencies. This is a significant accomplishment, since the CFPB did not even become an independent executive agency until July 21, 2011, approximately two months before the end of the fiscal year.

The CFPB is committed to continuously improving its internal control environment as we continue to build out our staffing, structure, and processes. We concur with the draft recommendations from the GAO intended to improve management's oversight and controls as well as to minimize risk to the Bureau. The recommendations were made for issues identified or for potential risks as of September 30, 2011. Since the conclusion of the audit in November 2011, the CFPB has implemented, or is in the process of implementing, actions that address issues identified by the GAO audit, which are further detailed in the recommendations in the report. Such actions include developing and implementing policies and procedures, working with our service providers to ensure that their controls are complementary to those of the CFPB, monitoring the timely correction of identified errors, and implementing additional information security controls. We are

consumerfinance.gov



1700 G Street NW, Washington, DC 20552

glad to have the opportunity to work with you and to benefit from your expertise in addressing these issues.

As the CFPB continues to mature as an agency, so will our internal control environment. We are investing significant resources to enhance our internal control program, information security program, awareness throughout the Bureau, and collaboration with our service providers. The CFPB is dedicated to upholding our fiscal responsibilities and ensuring that proper management oversight and controls are implemented to minimize risk to the Bureau. We have found that the GAO audit process is especially helpful and important to our work in this area.

Thank you again for the opportunity to comment on the draft report and for the careful and conscientious work that you and your staff are doing with us.

Sincerely,

Richard Cordray
Director

consumerfinance.gov

Enclosure II: Details on Audit Scope and Methodology

To fulfill our responsibilities as auditor of the financial statements of the Bureau of Consumer Financial Protection (CFPB), we did the following:

- examined, on a test basis, evidence supporting the amounts and disclosures in the financial statements;
- assessed the accounting principles used and significant estimates made by management;
- evaluated the overall presentation of the financial statements;
- obtained an understanding of the entity and its operations, including its internal control over financial reporting;
- considered CFPB's process for evaluating and reporting on internal control over financial reporting that CFPB is required to perform by the Federal Managers' Financial Integrity Act of 1982 and the Consumer Financial Protection Act;
- assessed the risk that a material misstatement exists in the financial statements and the risk that a material weakness exists in internal control over financial reporting;
- evaluated the design and operating effectiveness of internal control over financial reporting based on the assessed risk;
- tested relevant internal control over financial reporting; and

- tested compliance with selected provisions of the following laws and their related regulations: 31 U.S.C. § 3902 – Interest penalties under the Prompt Payment Act; 31 U.S.C. § 3904 – Limitations on Discount Payments Under the Prompt Payment Act; 5 U.S.C. § 8334 (a)(1), (2) – Civil Service Retirement Act; 5 U.S.C. §§ 8422, 8423, 8432 – Federal Employees’ Retirement System Act of 1986; Social Security Act of 1935, as amended; 5 U.S.C. §§ 8905-8909 – Federal Employees Health Benefits Act of 1959, as amended; and Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

(196254)

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

