UNITED STATES | Office of Personnel Management

OFFICE OF THE INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

October 1, 2014 –March 31, 2015

Office of the Inspector General

INDICATORS

FINANCIAL IMPACT:

Audit Recommendations for Recovery of Funds	$9,799,095
Management Commitments to Recover Funds	$9,876,685
Recoveries Through Investigative Actions	$4,188,783

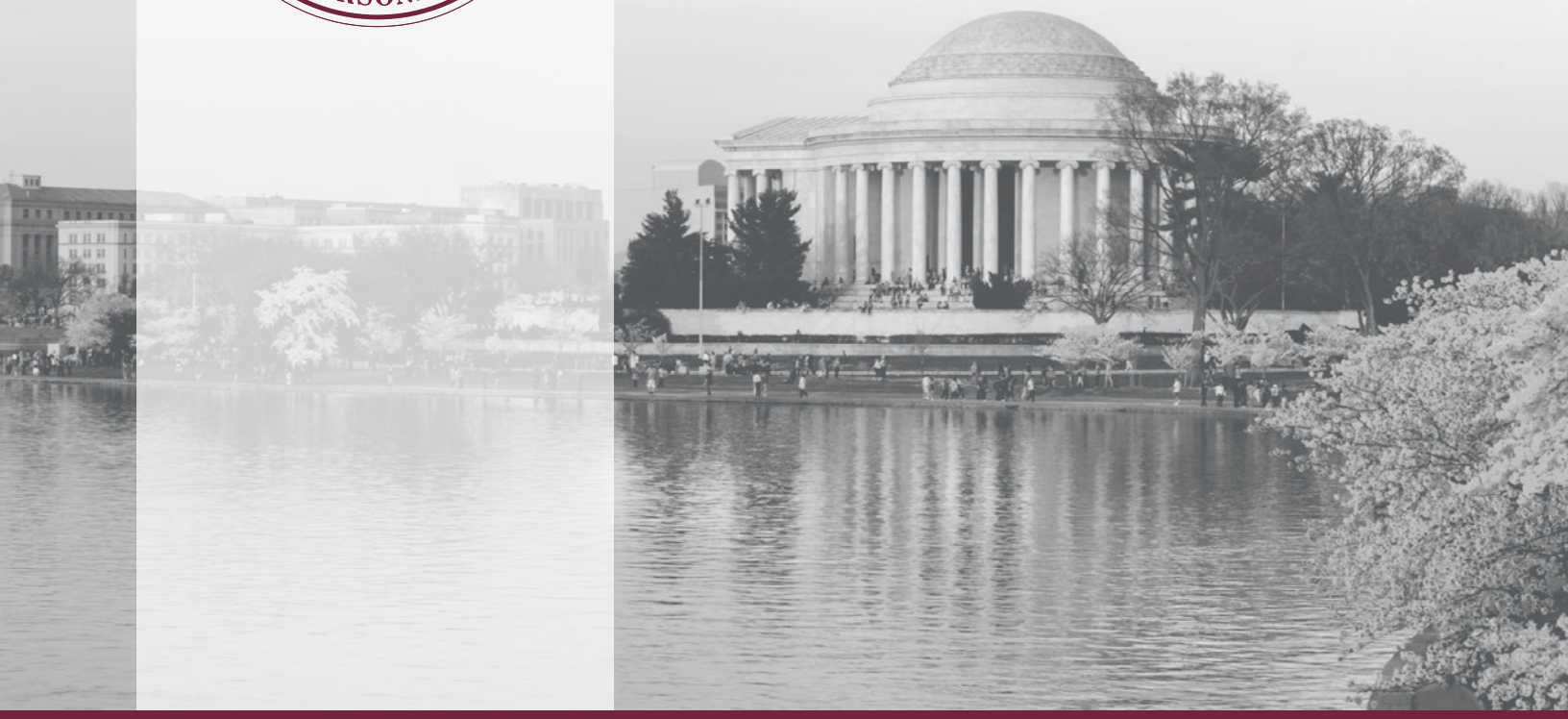
Note: OPM management commitments for recovery of funds during this reporting period reflect amounts covering current and past reporting period audit recommendations.

ACCOMPLISHMENTS:

Audit Reports Issued	34
Evaluation Reports Issued	1
Investigative Cases Closed	21
Indictments and Informations	16
Arrests	10
Convictions	17
Hotline Contacts and Preliminary Inquiries Complaints	1,480
Health Care Provider Debarments and Suspensions	366
Health Care Provider Debarment and Suspension Inquiries	2,904

UNITED STATES | Office of Personnel Management

OFFICE OF THE INSPECTOR GENERAL



SEMIANNUAL REPORT TO CONGRESS

October 1, 2014 –March 31, 2015

MESSAGE FROM THE INSPECTOR GENERAL

One of our most important responsibilities is to Federal employees, their families, and the American people, to help make sure that their personal information is protected against the growing threat of cybercrime. The health insurance claims of active and retired Federal employees and their families are kept by health plans participating in the Federal Employees Health Benefits Program administered by the U.S. Office of Personnel Management (OPM). In addition, OPM maintains sensitive data submitted by applicants for Federal jobs. We cannot accept any situation that results in a loss of this information.

But from the mundane to the spectacular, there is a steady stream of reports about various attacks against companies and individuals. Twitter accounts are hacked, cell phone data is stolen, credit card and information at large companies is exposed. The consequences range from embarrassing revelations about corporate politics and public figures, to devastating effects on innocent people dealing with the consequences of identity theft. It seems no one is immune. Indeed, this past year there were several major security incidents involving OPM and its contractors that may cause great harm to the people whose information we are entrusted to protect.

There are many ways that cybercrime is carried out. From disgruntled insiders, to amateurs using pre-scripted malware, to so-called 'hacktivists', to well-funded and highly sophisticated state-sponsored actors, the threats can come from almost anywhere. This latter group of individuals is perhaps the most concerning. They tend to have the time, patience, and resources necessary to carefully research their target, tailor an effective strategy, and execute their attack. Their methods are designed to mask their presence, and they cautiously avoid any activity that might raise a red flag.

This type of attacker was responsible for several recent attacks involving OPM and its contractors. In March 2014, OPM systems involved in Federal background investigations were compromised. A former OPM contractor, United States Investigative Services, was also attacked and records on applicants for federal employment may have been exposed. Another incident occurred at a second OPM contractor, KeyPoint Government Solutions, which may have resulted in a similar exposure.

Earlier this year we learned of two computer security incidents involving insurance companies participating in the FEHBP. At Anthem BlueCross BlueShield (BCBS), hackers executed a sophisticated attack in which they managed to compromise the account of a system administrator

and steal almost 80 million records, including names, addresses, social security numbers, and dates of birth. The breach at Premera BCBS may have been even worse because clinical medical information, in addition to personally identifiable information (PII), was improperly disclosed.

Health plans, in particular, are primary targets of cybercriminals because health care data is worth far more than credit card data on the identity theft black market. Credit card numbers can be changed, but names, social security numbers, and medical data cannot; therefore, the shelf life of this information is much longer, and hence more valuable. As a result, attacks like the ones on Anthem and Premera are likely to increase. In these cases, the risk to Federal employees and their families will probably linger long after the free credit monitoring offered by these companies expires.

Identity theft is not the only concern. Information obtained from these attacks can also be used to perpetrate fraudulent schemes against Federal health care programs. The cybercriminals can use member identification numbers, provider information, and clinical health data to set up phantom providers and submit bogus claims for reimbursement. There may also be national security implications – it is not that far-fetched to envision the information being used for espionage or blackmail.

We have an information technology (IT) audit group that audits OPM and contractor systems to find the kinds of weaknesses in their IT systems that these cybercriminals can exploit. This group takes a holistic approach to evaluating the total security environment surrounding systems – policy, training, access controls, network settings, and system configuration. The group also uses advanced technology to identify misconfigured systems and ineffective processes that can result in a security breach. Unfortunately, it is a challenge to audit all of the applicable systems on a reasonable schedule.

The oversight work of our office is a critical element of protecting citizens seeking employment with the Federal Government, and Federal employees and their families who are enrolled in the FEHBP, from these growing threats and the real consequences that can happen. Nonetheless, even a favorable outcome in a review we conduct cannot ensure that the systems and processes we examine will be immune from determined and sophisticated cyberattacks. In this light, we will continue to work with OPM, the Administration, and Congress to obtain adequate resources to address the oversight needs of OPM programs and to bring the highest possible level of professional expertise to bear on this critical challenge to personal privacy and the integrity of Federal data systems.

Patrick E. McFarland
Inspector General

MISSION STATEMENT

Our mission is to provide independent and objective oversight of OPM services and programs.

We accomplish our mission by:

- Conducting and supervising audits, evaluations, and investigations relating to the programs and operations of the U.S. Office of Personnel Management (OPM).
- Making recommendations that safeguard the integrity, efficiency, and effectiveness of OPM services.
- Enforcing laws and regulations that protect the program assets that are administered by OPM.

GUIDING PRINCIPLES

We are committed to:

- Promoting improvements in OPM's management and program operations.
- Protecting the investments of the American taxpayers, Federal employees and annuitants from waste, fraud, and mismanagement.
- Being accountable to the concerns and expectations of our stakeholders.
- Observing the highest standards of quality and integrity in our operations.

STRATEGIC OBJECTIVES

The Office of the Inspector General will:

- Combat fraud, waste, and abuse in programs administered by OPM.
- Ensure that OPM is following best business practices by operating in an effective and efficient manner.
- Determine whether OPM complies with applicable Federal regulations, policies, and laws.
- Ensure that insurance carriers and other service providers for OPM program areas are compliant with contracts, laws, and regulations.
- Aggressively pursue the prosecution of illegal violations affecting OPM programs.
- Identify, through proactive initiatives, areas of concern that could strengthen the operations and programs administered by OPM.

TABLE OF CONTENTS

PRODUCTIVITY INDICATORS . . . . . Inside Cover

MESSAGE FROM THE INSPECTOR GENERAL' i

MISSION STATEMENT iii

FIELD OFFICES vii

AUDIT ACTIVITIES 1
Health Insurance Carrier Audits 1
Information Systems Audits 7
Internal Audits 12
Special Audits 15
Combined Federal Campaign Audit 17

ENFORCEMENT ACTIVITIES 21
Investigative Cases 21
Administrative Sanctions of FEHBP Health Care Providers 30

STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES 33

APPENDIX I - A:
Final Reports Issued With Questioned Costs for Insurance Programs 35

APPENDIX I - B:
Final Reports Issued With Recommendations for All Other Audit Entities 36

APPENDIX II:
Final Reports Issued With Recommendations for Better Use of Funds 36

APPENDIX III:
Insurance Audit Reports Issued 37

TABLE OF CONTENTS

APPENDIX IV:
Internal Audit Reports Issued 38

APPENDIX V:
Combined Federal Campaign Audit Reports Issued 39

APPENDIX VI:
Information Systems Audit Reports Issued 39

APPENDIX VII:
Evaluation Reports Issued 39

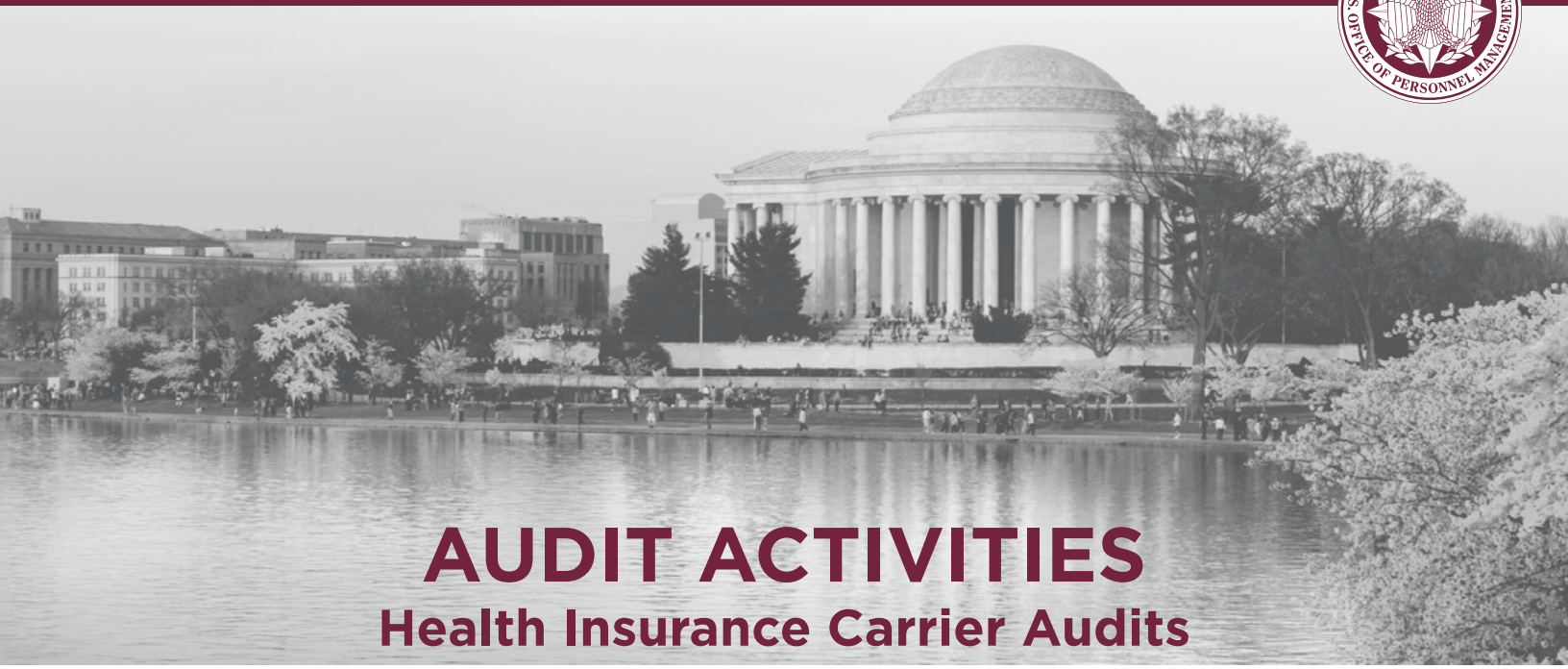
APPENDIX VIII:
Summary of Reports More Than Six Months Old Pending Corrective Action 40

APPENDIX IX:
Most Recent Peer Review Results Investigative Recoveries 43

APPENDIX X:
Investigative Recoveries 44

INDEX OF REPORTING REQUIREMENTS 46

FIELD OFFICES



AUDIT ACTIVITIES

Health Insurance Carrier Audits

The United States Office of Personnel Management (OPM) contracts with private sector firms to provide health insurance through the Federal Employees Health Benefits Program (FEHBP). Our office is responsible for auditing the activities of this program to ensure that the insurance carriers meet their contractual obligations with OPM.

The Office of the Inspector General's (OIG) insurance audit universe contains approximately 250 audit sites, consisting of health insurance carriers, sponsors, and underwriting organizations. The number of audit sites is subject to yearly fluctuations due to the addition of new carriers, non-renewal of existing carriers, or health insurance plan mergers and acquisitions. The premium payments for the health insurance program are over $45.8 billion annually.

The health insurance plans that our office audits are either community-rated or experience-rated carriers.

> ***Community-rated carriers*** *are comprehensive medical plans, commonly referred to as health maintenance organizations (HMOs) or health plans.*

> ***Experience-rated carriers*** *are mostly fee-for-service plans, the largest being the BlueCross and BlueShield health plans, but also include experience-rated HMOs.*

The two types of carriers differ in the way they calculate premium rates. Community-rated carriers generally set their rates based on the average revenue needed to provide health benefits to each member of a group. Rates established by experience-rated plans reflect a given group's projected paid claims, administrative expenses, and service charges for administering a specific contract.

During the current reporting period, we issued 25 final audit reports on organizations participating in the FEHBP, of which 10 contain recommendations for monetary adjustments in the amount of $9.8 million due the OPM administered trust funds.

COMMUNITY-RATED PLANS

The community-rated carrier audit universe covers approximately 142 health plans located throughout the country. Community-rated audits are designed to ensure that the premium rates health plans charge the FEHBP are in accordance with their respective contracts and applicable Federal laws and regulations.

Federal regulations require that the FEHBP rates be equivalent to the rates a health plan charges the two employer groups closest in subscriber size, commonly referred to as *similarly sized subscriber groups (SSSGs)*. The rates are set by the health plan, which is also responsible for selecting the SSSGs. When an audit shows that the rates are not equivalent, the FEHBP is entitled to a downward rate adjustment to compensate for any overcharges.

Community-rated audits focus on ensuring that:

- The health plans select the appropriate SSSGs;
- The FEHBP rates are equivalent to those charged the SSSGs; and,
- The loadings applied to the FEHBP rates are appropriate and reasonable.

> ***Loading*** *is a rate adjustment that the FEHBP makes to the basic benefit package offered by a community-rated health plan. For example, the FEHBP provides coverage for Federal annuitants. Many Federal annuitants may also be enrolled in Medicare. Therefore, the FEHBP rates may be adjusted to account for the coordination of benefits with Medicare.*

Beginning in 2013, OPM implemented a new rating methodology that eliminated the SSSG requirements for non-traditional community rated carriers and set a Medical Loss Ratio (MLR) threshold.

> ***Medical Loss Ratio (MLR)*** *is the proportion of health insurance premiums collected by a health insurer that is spent on clinical services and quality improvement. The MLR for each insurer is calculated by dividing the amount of health insurance premiums spent on clinical services and quality improvement by the total amount of health insurance premiums collected. The MLR is important because it requires health insurers to provide consumers with value for their premium payments.*

Starting in 2011, the Affordable Care Act (ACA) requires each large group health insurer to spend at least 85 percent of collected health insurance premiums on clinical services and quality improvement each year or provide a rebate. This is often explained as a health plan spending a minimum of $0.85 of every $1.00 paid in health insurance premiums on clinical services and quality improvements, and a maximum of $0.15 of every $1.00 on administrative costs. Each health insurer must reimburse policyholders any difference between the MLR and the 85 percent minimum expenditure.

For the FEHBP, the basic MLR calculation equals FEHBP claims plus expenses related to quality health improvements divided by premiums. Since the claims cost is a major factor in the MLR calculation, we are now focusing our efforts on auditing the FEHBP claims used in the MLR calculation.

During this reporting period, we issued 18 final audit reports on community-rated health plans and recommended approximately $2.8 million in premium recoveries to the FEHBP. A report summary is provided below to highlight notable audit findings.

Health Plan of the Upper Ohio Valley, Inc.

SAINT CLAIRSVILLE, OHIO

Report No. 1C-U4-00-14-038

FEBRUARY 20, 2015

The Health Plan of the Upper Ohio Valley, Inc. (Plan) has participated in the FEHBP since 1991, and provides health benefits to FEHBP members in Northeast and Eastern Ohio, and Northern and Central West Virginia. The audit covered contract years 2008 through 2010. During this period, the FEHBP paid the Plan approximately $27 million in premiums.

Inappropriate Charges Amount to Over **$1.9 Million**

In 2008 and 2010, we identified inappropriate health benefit charges to the FEHBP totaling $1,940,249. In addition, we determined the FEHBP is due $203,858 for lost investment income as a result of the overcharges.

Lost investment income (LII) *represents the potential interest earned on the amount the plan overcharged the FEHBP as a result of defective pricing.*

The overcharges occurred due to the Plan:

- Using unsupported data in its 2008 FEHBP rate development;
- Not applying the largest SSSG discount to the 2008 and 2010 FEHBP rates;
- Not fully complying with the records retention clause of its FEHBP contract; and,
- Not having adequate rating system controls in place to ensure that the FEHBP and the groups closest in subscriber size are rated consistently and in accordance with the Plan's standard rating methodology.

EXPERIENCE-RATED PLANS

The FEHBP offers a variety of experience-rated plans, including a service benefit plan and health plans operated or sponsored by Federal employee organizations, associations, or unions. In addition, experience-rated HMOs fall into this category. The universe of experience-rated plans currently consists of approximately 100 audit sites. When auditing these plans, our auditors generally focus on three key areas:

- Appropriateness of FEHBP contract charges and the recovery of applicable credits, including health benefit refunds and drug rebates;
- Effectiveness of carriers' claims processing, financial, cost accounting and cash management systems; and,
- Adequacy of carriers' internal controls to ensure proper contract charges and benefit payments.

During this reporting period, we issued three experience-rated final audit reports. In these reports, our auditors recommended that the plans return $6.98 million in inappropriate charges and lost investment income to the FEHBP.

BlueCross BlueShield Service Benefit Plan

The BlueCross BlueShield Association (Association), on behalf of participating BlueCross BlueShield (BCBS) plans, entered into a Government-wide Service Benefit Plan with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS plans throughout the United States to process the health benefit claims of its Federal subscribers.

The Association has established a Federal Employee Program (FEP) Director's Office, in Washington, D.C., to provide centralized management for the Service Benefit Plan. The FEP Director's Office coordinates the administration of the contract with the Association, BCBS plans, and OPM. The Association has also established an FEP

Operations Center. The activities of the FEP Operations Center are performed by CareFirst BlueCross BlueShield, located in Washington, D.C. These activities include acting as fiscal intermediary between the Association and member plans, verifying subscriber eligibility, approving or disapproving the reimbursement of local plan payments of FEHBP claims, maintaining a history file of all FEHBP claims, and an overall accounting for all program funds.

The Association, which administers a fee-for-service plan known as the Service Benefit Plan, contracts with OPM on behalf of its member plans throughout the United States. The participating plans independently underwrite and process the health benefits claims of their respective Federal subscribers and report their activities to the national BCBS operations center in Washington, D.C. Approximately 64 percent of all FEHBP subscribers are enrolled in BCBS plans.

We issued three BCBS experience-rated reports during the reporting period. Experience-rated audits normally address health benefit payments, miscellaneous payments and credits, administrative expenses, cash management activities, and/or Fraud and Abuse Program activities. Our auditors identified $6.98 million in questionable costs charged to the FEHBP contract. BCBS agreed with $6.94 million of the identified overcharges. Summaries of two of these final reports are provided below, pages 4 through 5, to highlight our notable audit findings.

BlueCross BlueShield of Tennessee

CHATTANOOGA, TENNESSEE

Report No. 1A-10-15-14-030

DECEMBER 24, 2014

Our audit of the FEHBP operations at BlueCross BlueShield of Tennessee (Plan) covered miscellaneous health benefit payments and credits from 2009 through September 2013, as well as administrative expenses, and statutory reserve payments from 2008 through 2012. In addition, we reviewed the Plan's cash management activities and practices related to FEHBP funds from 2009 through September 2013 and the Plan's Fraud and Abuse Program for 2013. For contract years 2008 through 2012, the Plan processed approximately $1.8 billion in FEHBP health benefit payments and charged the FEHBP $81 million in administrative expenses and $36 million in statutory reserve payments.

Our auditors questioned $5,824,432 in health benefit charges, administrative expense overcharges, cash management activities, and applicable lost investment income (LII); and identified a procedural finding regarding the Plan's Fraud and Abuse Program. The monetary findings included the following:

- $5,776,229 in excess FEHBP funds held by the Plan in the dedicated FEP investment account as of December 31, 2013;
- $29,580 for administrative expense overcharges and $1,442 for applicable LII on these overcharges; and,
- $16,547 for an unreturned medical drug rebate and $634 for applicable LII.

Auditors Question Nearly **$5.8 Million** in Cash Management Activities

Regarding the procedural finding, we determined that the Plan is not in compliance with the communication and reporting requirements for fraud and abuse cases contained in the FEHBP contract and the applicable FEHBP Carrier Letters. Specifically, the Plan did not report, or report judiciously, all fraud and abuse cases to OPM's OIG. The Plan's non-compliance may be due in part to:

- Incomplete or untimely reporting of fraud and abuse cases to the FEP Director's Office; and,
- Inadequate controls at the FEP Director's Office to monitor and communicate the Plan's cases to us.

Without notification of the Plan's probable fraud and abuse issues, we cannot investigate the impact of these potential issues on the FEHBP.

The Association and Plan agreed with our questioned amounts, but generally disagreed with the procedural finding regarding the Fraud and Abuse Program.

Regence

PORTLAND, OREGON

Report No. 1A-10-69-14-012

JANUARY 20, 2015

Regence includes the BlueCross and/or BlueShield (BCBS) plans of Idaho, Oregon, Utah, and Washington. For contract years 2010 through 2012, Regence processed approximately $1.8 billion in FEHBP health benefit payments and charged the FEHBP $127 million in administrative expenses for these four BCBS plans.

Our audit of the FEHBP operations at Regence covered miscellaneous health benefit payments and credits from 2010 through September 2013 for the four BCBS plans; as well as administrative expenses from 2010 through 2012. We also reviewed Regence's cash management activities and practices related to FEHBP funds from 2010 through September 2013, and Regence's Fraud and Abuse Program for 2013. For administrative expenses, we only reviewed the expenses relating to pension and post-retirement benefits for these plans; and gains from the sale of buildings by the Oregon and Washington plans.

We questioned $1,066,072 in health benefit charges, cash management activities, and LII; and our auditors identified procedural findings regarding Regence's cash management activities and Fraud and Abuse Program. The monetary findings included the following:

- $507,922 for duplicate bank fee charges and $38,799 for applicable LII on these duplicate charges;
- $407,374 for credit adjustment amounts not deposited into the dedicated FEP investment accounts and $28,798 for applicable LII on these funds; and,
- $81,849 for unreturned medical drug rebates and $1,330 for LII on medical drug rebates returned untimely to the FEHBP.

Regarding the procedural finding for cash management activities, our auditors determined that Regence held a total of $8,327,444 in corporate funds in the dedicated FEP investment accounts (as of September 30, 2013) for the four plans. Most of these corporate funds represented approved pension cost reimbursements that were deposited into the dedicated FEP investment accounts almost two years prior. Regence should not maintain excess corporate (non-FEHBP) funds in these dedicated FEP investment accounts.

For the procedural finding regarding the Fraud and Abuse Program, we determined that Regence is not in compliance with the communication and reporting requirements for fraud and abuse cases contained in the FEHBP contract and the applicable FEHBP Carrier Letters. Specifically, Regence did not report, or report timely, all fraud and abuse cases to us. Regence's non-compliance may be due in part to:

Auditors Question Over **$1 Million** in Health Benefit Charges, Cash Management Activities, and Lost Investment Income

- Incomplete or untimely reporting of fraud and abuse cases to the FEP Director's Office; and,
- Inadequate controls at the FEP Director's Office to monitor and communicate Regence's cases to us.

Without awareness of Regence's probable fraud and abuse issues, we cannot investigate the impact of these potential issues on the FEHBP.

The Association and Regence agreed with $1,029,469 of the questioned amounts, partially agreed with the procedural finding for cash management activities, and generally disagreed with the procedural finding for Regence's Fraud and Abuse Program.

EMPLOYEE ORGANIZATION PLANS

Employee organization plans fall into the category of experience-rated plans. These plans either operate or sponsor participating Federal health benefits programs. As fee-for-service plans, they allow members to obtain treatment through facilities or providers of their choice.

The largest employee organizations are Federal employee unions and associations. Some examples are the: American Postal Workers Union; Association of Retirees of the Panama Canal Area; Government Employees Health Association, Inc.; National Association of Letter Carriers; National Postal Mail Handlers Union; and, Special Agents Mutual Benefit Association.

We did not issue any audit reports on employee organization plans during this reporting period.

EXPERIENCE-RATED COMPREHENSIVE MEDICAL PLANS

Comprehensive medical plans fall into one of two categories: community-rated or experience-rated. As we previously explained on page 1 of this report, the key difference between the categories stems from how premium rates are calculated.

Members of experience-rated plans have the option of using a designated network of providers or using out-of-network providers. A member's choice in selecting one health care provider over another has monetary and medical implications. For example, if a member chooses an out-of-network provider, the member will pay a substantial portion of the charges and covered benefits may be less comprehensive.

We did not issue any reports on experience-rated comprehensive medical plans during this reporting period.

Information Systems Audits

OPM relies on computer technologies and information systems to administer programs that distribute health and retirement benefits to millions of current and former Federal employees. OPM systems also assist in the management of background investigations for Federal employees, contractors, and applicants as well as provide Government-wide recruiting tools for Federal agencies and individuals seeking Federal jobs. Any breakdowns or malicious attacks (e.g., hacking, worms, or viruses) affecting these Federal systems could compromise the privacy of the individuals whose information they maintain, as well as the efficiency and effectiveness of the programs that they support.

Our auditors examine the computer security and information systems of private health insurance carriers participating in the FEHBP by performing general and application controls audits. *General controls* refer to the policies and procedures that apply to an entity's overall computing environment. *Application controls* are those directly related to individual computer applications, such as a carrier's payroll system or benefits payment system. General controls provide a secure setting in which computer systems can operate, while application controls ensure that the systems completely and accurately process transactions.

In addition, the Information Systems Audits Group evaluates historical health benefit claims data for appropriateness, and makes audit recommendations that erroneous payments be returned to OPM. We are also responsible for performing an independent oversight of OPM's internal information technology and security program, including focused audits of major OPM information systems and system development projects.

Summaries of the audit reports issued during this period are provided below.

Federal Information Security Management Act Audit

WASHINGTON, D.C.

Report No. 4A-CI-00-14-016

NOVEMBER 12, 2014

The Federal Information Security Management Act of 2002 (FISMA) is designed to ensure that the information systems and data supporting federal operations are adequately protected. FISMA emphasizes that agencies implement security planning as part of the life cycle of their information systems. A critical aspect of security planning involves annual program security reviews conducted or overseen by each agency's inspector general.

We audited OPM's compliance with FISMA requirements defined in the Office of Management and Budget's fiscal year (FY) 2014 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Over the past several years, the Office of the Chief Information Officer (OCIO) made noteworthy improvements to OPM's information technology (IT) security program. However, some problem areas that had improved in past years have resurfaced.

Our FY 2014 FISMA audit report upgrades one longstanding material weakness to a significant deficiency, but also reports a new material weakness related to information system security assessment and authorization.

In the FY 2007 FISMA report, we noted a material weakness related to the lack of IT security policies and procedures. In FY 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT security policies. Little progress was made in the subsequent years to address these issues. However, in FY 2014 the OPM Director approved and funded a plan to restructure the OCIO to further centralize IT security duties under a team of information system security officers that reports to the OCIO. Because of these planned changes, we reduced the severity of the issue from a material weakness to a significant deficiency.

However, our audit also determined that of the 21 OPM systems due for a security assessment and authorization (Authorization) in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization. The drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

Longstanding Material Weakness Upgraded, New Material Weakness Added

We identified the following additional opportunities for improvement:

- Key elements are still missing from OPM's approach to managing risk at an agency-wide level including: conducting a risk assessment, maintaining a risk registry, and communicating the agency-wide risks down to the system owners;
- Configuration baselines have not been created for all operating platforms;
- All operating platforms are not routinely scanned for compliance with configuration baselines;
- OPM does not maintain a comprehensive inventory of servers, databases, and network devices. In addition, we are unable to independently attest that OPM has a mature vulnerability scanning program;
- Program offices are not adequately incorporating known weaknesses into plans of action and milestones (POA&M) and the majority of program office POA&Ms have weaknesses that are over 120 days overdue;
- OPM continues to implement its continuous monitoring plan. However, security controls for all OPM systems are not adequately tested in accordance with OPM policy;
- Several OPM program offices did not conduct contingency plan tests for its systems in FY 2014. In the event of an unplanned system outage, these program offices may experience difficulty recovering their systems in a timely manner;
- Several information security agreements between OPM and contractor-operated information systems have expired; and,
- Multi-factor authentication (the use of a token such as a smart card, along with an access code) is not required to access OPM systems in accordance with Office of Management and Budget (OMB) Memorandum M-11-11. This is a significant concern because multi-factor authentication is a key defense against unauthorized access.

Information System General and Application Controls at Premera BlueCross

MOUNTLAKE TERRACE, WASHINGTON

Report No. 1A-10-70-14-007

NOVEMBER 28, 2014

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for Premera BlueCross (Plan), and the various processes and IT systems used to support these applications.

We documented the controls in place and opportunities for improvement in each of the areas below.

Security Management

Premera has implemented a security management program with adequate IT security policies and procedures.

Access Controls

The Plan has implemented controls to grant or prevent physical access to its data center, as well as logical controls to protect sensitive information. However, Premera's data center does not have controls we typically observe at similar facilities, such as multi-factor authentication and piggybacking prevention. Since the issuance of the draft report, the Plan has installed multi-factor authentication, but has yet to implement piggybacking prevention. We also noted a weakness related to password settings.

Network Security

Premera has implemented a thorough incident response and network security program. However, we noted several areas of concern related to Premera's network security controls:

- A patch management policy is in place, but current scans show that patches are not being implemented in a timely manner;
- A methodology is not in place to ensure that unsupported or out-of-date software is not utilized; and,
- Insecure server configurations were identified in a vulnerability scan.

Configuration Management

Premera has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured, updated, and changes are controlled. However, Premera has not documented formal baseline configurations that detail the approved settings for its server operating systems, and therefore cannot effectively audit its security configuration settings.

Contingency Planning

We reviewed Premera's business continuity and disaster recovery plans and concluded that they contained the key elements suggested by relevant guidance and publications. However, the Plan does not perform a complete disaster recovery test for all information systems. As a result, there is a greater risk of problems associated with the timely recovery of critical systems following a disaster.

Opportunities for Improvement Exist in Network Security, Configuration Management, and Claims Adjudication

Claims Adjudication

Premera has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in Premera's claims application controls which could lead to improper claims payments.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that Premera is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Claims Audit at Independence BlueCross

PHILADELPHIA, PENNSYLVANIA

Report No. 1A-10-55-14-027

DECEMBER 2, 2014

The objective of our audit was to determine whether Independence BlueCross (IBC) appropriately charged costs to the FEHBP. From 2011 through 2013, IBC paid approximately $721 million in health benefits claims. We reviewed $6.8 million of these claims payments.

We found that IBC incorrectly paid 21 health benefit claims totaling $86,594. IBC did not properly price six claims by non-participating providers. These non-participating health care providers do not have a contractual relationship

FEHBP Overcharged **$86,594** for Claim Payment Errors

with IBC and they define pricing agreements for various claims types. IBC also failed to retroactively correct payment errors for four claims when it became aware of changes in enrollment coverage. Finally, IBC did not correctly process 11 claims involving dialysis treatment.

Information Technology Security Controls for OPM's Dashboard Management Reporting System

WASHINGTON, D.C.

Report No. 4A-CI-00-14-064

JANUARY 14, 2015

The Dashboard Management Reporting System (DMRS) is one of OPM's critical IT applications; therefore we evaluated the system's compliance with FISMA.

The DMRS web-based application is designed to support delivery of services to OPM's Federal Investigative Services (FIS), which is responsible for background investigations used to determine eligibility for security clearance or suitability for employment in sensitive positions. The system is operated and hosted by OPM, and owned by FIS.

Our objective was to perform an evaluation of the security controls for DMRS to ensure that FIS officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA. Although the system is generally compliant with FISMA requirements, we noted that FIS could improve its process for managing the DMRS plan of action and milestones.

We also tested approximately 50 specific information system security controls included in the National Institute of Standards and Technology's Special Publication 800-53, *"Security and Privacy Controls for Federal Information Systems and Organizations."* This test work determined that technical controls related to audit logging could be improved and that FIS does not currently conduct routine scans to identify security weaknesses for DMRS. FIS stated that a planned upgrade to the DMRS software will address audit logging requirements.

FIS disagreed with our recommendation to perform routine scans penetration testing on the system, and stated that a proposed update to OPM's Information Security and Privacy Policy will not require this type of testing. However, the current version of this policy does require penetration testing for systems with a high security categorization, such as DMRS. In addition, we consider this type of testing to be a critical aspect of system security, and we continue to make this recommendation.

FIS Disagrees with Recommendation to Perform Routine Penetration Testing on DMRS

Information System General and Application Controls at Horizon BlueCross BlueShield

NEWARK, NEW JERSEY

Report No. 1A-10-49-14-021

FEBRUARY 11, 2015

Our audit focused on the claims processing applications used to adjudicate FEHBP claims for Horizon BlueCross BlueShield (Horizon or Plan), in addition to the various processes and IT systems used to support these applications.

We documented the controls in place and opportunities for improvement in each of the areas below.

Security Management

Horizon has established an adequate security management program.

Access Controls

The Plan has implemented controls to prevent unauthorized physical access to its facilities, along with logical controls to protect sensitive information. However, we noted several areas of concern related to their access controls during our review. Specifically we noted that:

- The data center did not have controls we typically observe at similar facilities, such as multi-factor authentication and piggybacking prevention;
- The process to remove employees' physical access after termination could be improved; and,
- Some individuals had multiple active directory (AD) accounts, and some terminated employees still had active accounts.

Network Security

Horizon has implemented an incident response and network security program. However, we noted the following areas of concern related to the Plan's network security controls:

- A full scope vulnerability management program has not been implemented;
- A patch management policy is in place, but our test work indicated that patches are not being implemented in a timely manner; and,
- No procedures are in place to ensure that unsupported or out-of-date software is not utilized.

Configuration Management

Horizon has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured, updated, and changes are controlled. However, Horizon's baseline settings for the Windows operating system did not adequately reflect its configuration hardening policies or industry best practices. Horizon is currently revising these baselines to comply with Center for Internet Security (CIS) benchmarks. Currently, the Plan does not audit its servers against a formal Windows baseline configuration. Therefore, there is a higher risk that Windows systems may not be properly secured, which may lead to unauthorized access.

Contingency Planning

The Plan's business continuity and disaster recovery plans contain the key elements suggested by relevant guidance and publications. However, Horizon does not perform routine business continuity testing. Therefore, while systems may be recovered in the event of a disaster, there is a risk that business processes (e.g., processing of FEP members' claims) may not be restored.

Claims Adjudication

Horizon has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in the Plan's claims application controls that could lead to improper health benefit claim payments.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that Horizon is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Internal Audits

Our internal auditing staff focuses on improving the efficiency and effectiveness of OPM's operations and their corresponding internal controls. One critical area of this activity is the audit of OPM's consolidated financial statements required under the Chief Financial Officers Act (CFO) of 1990. Our staff also conducts performance audits covering other internal OPM programs and functions.

OPM'S CONSOLIDATED FINANCIAL STATEMENTS AUDITS

The CFO Act requires that audits of OPM's financial statements be conducted in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States. OPM contracted with the independent certified public accounting firm KPMG LLP (KPMG) to audit the consolidated financial statements as of September 30, 2014 and for the fiscal year (FY) then ended. The contract requires that the audit be performed in accordance with generally accepted government auditing standards (GAGAS) and the OMB Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, as amended.

OPM's consolidated financial statements include the Retirement Program, Health Benefits Program, Life Insurance Program, Revolving Fund Programs (RF), and Salaries and Expenses funds (S&E). The RF programs provide funding for a variety of human resource-related services to other Federal agencies, such as: pre-employment testing, background investigations, and employee training. The S&E funds provide the resources used by OPM for the administrative costs of the agency.

KPMG is responsible for, but is not limited to, issuing an audit report that includes:

- Opinions on the consolidated financial statements and the individual statements for the three benefit programs;
- A report on internal controls; and,
- A report on compliance with certain laws and regulations.

In connection with the audit contract, we oversee KPMG's performance of the audit to ensure that it is conducted in accordance with the terms of the contract and is in compliance with GAGAS and other authoritative references.

Specifically, we were involved in the planning, performance, and reporting phases of the audit through participation in key meetings, reviewing KPMG's work papers, and coordinating the issuance of audit reports. Our review disclosed no instances where KPMG did not comply, in all material respects, with GAGAS, the contract, and all other authoritative references.

In addition to the consolidated financial statements, KPMG performed the audit of the closing package financial statements as of September 30, 2014 and 2013. The contract requires that the audit be done in accordance with GAGAS and the OMB Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, as amended. The U.S. Department of the Treasury and the Government Accountability Office use the closing package in preparing and auditing the *Financial Report of the United States Government*.

OPM's FY 2014 Consolidated Financial Statements

WASHINGTON, D.C.

Report No. 4A-CF-00-14-039

NOVEMBER 10, 2014

KPMG audited OPM's balance sheets as of September 30, 2014 and 2013 and the related consolidated financial statements. KPMG also audited the individual balance sheets

of the Retirement, Health Benefits and Life Insurance programs (hereafter referred to as the Programs), as of September 30, 2014 and 2013 and the Programs' related individual financial statements for those years. The Programs, which are essential to the payment of benefits to federal civilian employees, annuitants, and their respective dependents, operate under the following names:

- Civil Service Retirement System;
- Federal Employees Retirement System;
- Federal Employees Health Benefits Program (FEHBP); and,
- Federal Employees' Life Insurance Program.

No Material Weaknesses Reported in FY 2014

KPMG reported that OPM's consolidated financial statements and the Programs' individual financial statements as of and for the years ended September 30, 2014 and 2013, were presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles. KPMG's audits generally include identifying internal control deficiencies, significant deficiencies, and material weaknesses.

> *An **internal control deficiency** 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.*
>
> *A **significant deficiency** is a deficiency, or combination of deficiencies, in an internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.*
>
> *A **material weakness** is a deficiency, or combination of deficiencies, in an 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.*

KPMG's report identified no material weaknesses in the internal controls. However, KPMG identified one significant deficiency that remains unresolved from prior years. The unresolved area identified by KPMG is:

The Information Systems Control Environment

In FY 2013, a significant deficiency was reported related to OPM's internal control environment due to persistent deficiencies in OPM's information system security program. These deficiencies included incomplete security authorization packages, weaknesses in testing of information security controls, and inaccurate Plans of Action and Milestones. During FY 2014, OPM management demonstrated progress in centralizing security program functions in an effort to address deficiencies noted in its security program; however, KPMG continued to observe control weaknesses.

OPM agreed to the findings and recommendations reported by KPMG.

KPMG's report on compliance with certain provisions of laws, regulations, and contracts disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements, as amended*.

OPM's FY 2014 Closing Package Financial Statements

WASHINGTON, D.C.

Report No. 4A-CF-00-14-040

NOVEMBER 17, 2014

The closing package financial statements are required to be audited in accordance with GAGAS and the provisions of OMB's Bulletin No. 14-02. OPM's Closing Package Financial Statements include:

- The reclassified balance sheets, the statements of net cost, the statements of changes in net position, and the accompanying financial report notes report as of September 30, 2014 and 2013;
- The Additional Note Nos. 28 and 29 (discloses other data necessary to make the Closing Package Financial Statements more informative); and,
- The Trading Partner balance sheets, the statements of net cost, and the statements of changes in net position (showing the funds due between OPM and other agencies) as of September 30, 2014.

KPMG reported that OPM's closing package financial statements are presented fairly, in all material respects.

KPMG noted no matters involving the internal control over the financial process for the closing package financial statements that are considered a material weakness or significant deficiency. In addition, KPMG disclosed no instances of noncompliance or other matters that are required to be reported. The objectives of KPMG's audits of the closing package financial statements did not include expressing an opinion on internal controls or compliance with laws and regulations, and KPMG, accordingly, did not express such opinions.

FY 2014 Closing Package Statements Receive Another Clean Opinion

Special Audits

In addition to health and life insurance, OPM administers various other benefit programs for Federal employees which include the: Federal Employees' Group Life Insurance (FEGLI) Program; Federal Flexible Spending Account (FSAFEDS) Program; Federal Long Term Care Insurance Program (FLTCIP); and, Federal Employees Dental and Vision Insurance Program (FEDVIP). Our office also conducts audits of Pharmacy Benefit Managers (PBMs) that coordinate pharmacy benefits for the FEHBP carriers. The objective of these audits is to ensure that costs charged and services provided to Federal subscribers are in accordance with the contracts and applicable Federal regulations. Additionally, our staff performs audits of the Combined Federal Campaign (CFC) to ensure that monies donated by Federal employees are properly handled and disbursed to charities according to the designations of contributing employees, and audits of Tribal enrollments into the FEHBP.

During this reporting period we issued three final audit reports, two of which are summarized below.

Federal Long Term Care Insurance Program as Administered by Long Term Care Partners, LLC for Contract Years 2010 through 2012

PORTSMOUTH, NEW HAMPSHIRE

Report No. 1G-LT-00-14-025

DECEMBER 23, 2014

The Federal Long Term Care Insurance Program (FLTCIP or the Program) was established by the Long Term Care Security Act (Public Law 106-265), which was signed by the President on September 19, 2000. The Act directed OPM to develop and administer a long term care insurance program for Federal employees and annuitants, current and retired members of the uniformed services, and qualified relatives.

In December 2001, OPM awarded a seven year contract to Long Term Care Partners (LTCP) to offer long term care insurance coverage to eligible participants. A new contract was awarded to John Hancock upon the expiration of the original contract. On October 1, 2009, John Hancock became the sole insurer and LTCP became a wholly-owned subsidiary of John Hancock. LTCP, with OPM oversight, is responsible for all administrative functions of the Program. These functions include marketing and enrollment, underwriting, policy insurance, premium billing and collection, and claims administration.

Our audit covered a review of LTCP's administrative expenses, cash management, claim benefit payments, profit and performance incentives, HIPAA policies and procedures, and fraud and abuse policies and procedures. We expanded the scope of the profit and performance incentives review through December 6, 2013, because we noted excess investment management fees charged to the FLTCIP Experience Fund.

The audit identified $34,524 in program overcharges, including $3,826 in LII, and an undercharge of $77,590. Specifically, we found:

- LTCP did not return $17,588 of LII on investment management fees that were incorrectly calculated from 2010 through 2013;

- LTCP charged the Program $13,110 in unallowable lodging expenses in excess of the General Service Administration's (GSA) per diem rates during contract years 2010 through 2012. Therefore, the FLTCIP is due $3,826 for LII related to the $13,110 in questioned administrative expenses, calculated from October 1, 2011 through June 23, 2014, when the $13,110 was returned by LTCP;

- LTCP did not properly apply its Management Allocation methodology used to allocate certain administrative expenses to the Program in 2012, resulting in a $77,590 undercharge. We noted that this issue also impacted another line of business that LTCP administers for OPM, resulting in a $77,590 overcharge to that program. The final report for this audit was also issued during this reporting period;

- LTCP erroneously understated the Program's administrative expenses reported in its 2010 audited financial statements by $114,591; and,

- LTCP did not properly void or credit one outstanding benefit check within 25 months of issuance.

LTCP agreed with all of the audit findings and implemented corrective actions sufficient to close the audit recommendations. A letter was sent by OPM to LTCP on March 4, 2015, officially closing the audit.

Limited Scope Audit of BlueCross and BlueShield's Pricing of Pharmacy Claims as Administered by Caremark PCS Health LLC for Contract Year 2012

WASHINGTON, D.C.

Report No. 1H-01-00-14-008

OCTOBER 6, 2014

We conducted a limited scope review of BlueCross and BlueShield's (BCBS) pricing of pharmacy claims as administered by Caremark PCS Health LLC (Caremark) for contract year 2012. New pharmacy transparency standards became effective January 2011 for all FEHBP carriers and their contracted PBMs. Contract year 2012 was the first year where these standards were included in the contracts between the BCBS Association (BCBSA) and Caremark. Therefore, the primary objective of our audit was to verify, on a limited basis, if the pharmacy claims processed and paid by Caremark on behalf of BCBSA were transparent and accurately priced. Additionally, our audit included a review of HIPAA policies and procedures, and fraud and abuse policies and procedures.

FEHBP Paid BCBSA **$7.8 Million** for Anti-Fraud Activities, Yet Reports Only 18 of 61 Pharmacy Fraud and Abuse Cases to the OIG

To further enhance Federal employees' benefits under the FEHBP, insurance carriers have contracted with PBMs to provide both mail order and retail prescription drug benefits. PBMs are primarily responsible for processing and paying prescription drug claims. For this particular audit, the PBM was used by BCBSA, on behalf of its participating BCBS plans, to develop, allocate, and control costs related to the pharmacy claims program. BCBSA's pharmacy operations and responsibilities under Contract CS 1039 are carried out by the PBM (Caremark), which is located in Scottsdale, Arizona.

The audit identified one procedural finding related to BCBS's fraud and abuse policies and procedures. Specifically, we found:

- The BCBSA did not report to OPM's Office of the Inspector General all of the suspected fraud and abuse cases that Caremark reported for contract year 2012; additionally,

- Of those cases that BCBSA reported to us, 50 percent were not reported within 30 working days as required by the contract.

BCBSA either partially or completely disagreed with our audit recommendations. However, they were willing to work with OPM to resolve the audit issues and recommendations addressed in this report. Ultimately, BCBSA implemented corrective actions sufficient to close the audit recommendations. A letter was sent by OPM to BCBSA on October 24, 2014, officially closing the audit.

COMBINED FEDERAL CAMPAIGN

The Combined Federal Campaign (CFC) is the only authorized charitable fundraising drive conducted in Federal installations throughout the world. OPM has the responsibility, through both law and executive order, to regulate and oversee the conduct of fundraising activities in Federal civilian and military workplaces worldwide.

CFCs are identified by geographical areas that may include only a single city, or encompass several cities or counties. Our auditors review the administration of local campaigns to ensure compliance with Federal regulations and OPM guidelines. In addition, all campaigns are required by regulation to have an independent public accounting firm (IPA) audit their respective financial activities for each campaign year. The audit must be in the form of an agreed-upon procedures engagement to be completed by an IPA. We review the IPA's work as part of our audits.

CFC audits do not identify savings to the government, because the funds involved are charitable donations made by Federal employees. Our audit efforts occasionally generate an internal referral to our criminal investigators for potentially fraudulent activity. OPM's Office of the Combined Federal Campaign (OCFC) works with the campaign to resolve the findings after the final audit report is issued.

Local CFC Audits

The local organizational structure consists of:

Local Federal Coordinating Committee (LFCC)

The LFCC is a group of Federal officials designated by the Director of OPM to conduct the CFC in a particular community. It organizes the local CFC; determines the eligibility of local charities; selects and supervises the activities of the Principal Combined Fund Organization (PCFO); encourages Federal agencies to appoint employees to act as Loaned Executives who work directly on the local campaign; ensures that Federal employees are not coerced to participate in the local campaign; and resolves issues relating to a local charity's noncompliance with the CFC policies and procedures.

Principal Combined Fund Organization (PCFO)

The PCFO is a federated group or combination of groups, or a charitable organization, selected by the LFCC to administer the local campaign under the direction and control of the LFCC and the Director of OPM. The primary goal of the PCFO is to administer an effective and efficient campaign in a fair and even-handed manner aimed at collecting the greatest amount of charitable contributions possible. Its responsibilities include collecting and distributing CFC funds, training volunteers, maintaining a detailed accounting of CFC administrative expenses incurred during the campaign, preparing pledge forms and charity lists, and submitting to and cooperating fully with audits of its operations. The PCFO is reimbursed for its administrative expenses from CFC funds.

Federations

A Federation is a group of voluntary charitable human health and welfare organizations created to supply common fundraising, administrative, and management services to its constituent members.

Independent Organizations

Independent Organizations are organizations that are not members of a federation for the purposes of the CFC.

Of continued concern to our auditors is the consistent identification of similar issues from audit to audit. The causes for these issues are, more often than not, attributed to one of the following program concerns:

- The PCFO was either not aware of, did not understand its responsibilities as defined in the regulations and CFC memoranda, or simply did not follow said regulations and memoranda;
- The LFCC was either not aware of or did not understand its responsibilities as defined in the regulations;
- The LFCC is inactive and does not perform the needed oversight of the PCFO; or,
- The IPAs hired to perform the agreed-upon procedures audit, which is paid for out of campaign funds, do not understand the requirements of the audit, which results in findings not being identified and communicated to the PCFOs and LFCCs.

During this reporting period, we issued four audit reports of local CFCs. Our audits revealed the following concerns:

- For three of the four audits, we identified a recurring issue related to special fundraising events that did not comply with CFC regulations. Specifically in all three cases, the agencies involved did not receive approval from their respective ethics officials before holding the events. For two of the three audits, this resulted in the awarding of raffle prizes to Federal employees, the value of which could violate Federal ethics regulations.
- Additionally, we identified a program concern for one of the four audits related to a lack of LFCC participation in CFC matters. Having an active LFCC is of the utmost importance to the running of an efficient and effective campaign, because the LFCC is responsible for overseeing the activities of the PCFO. We recommended that the current LFCC members be replaced with members who will be actively involved in the CFC.
- Finally, due to the nature and extent of the audit findings identified in one audit, we recommended that the Northern Lights CFC be merged with another geographically adjacent campaign more equipped to handle the responsibilities of the CFC. These issues are explained in more detail below.

Audit of the 2011 and 2012 Northern Lights Combined Federal Campaigns

ST. PAUL, MINNESOTA

Report No. 3A-CF-00-14-048

MARCH 23, 2015

We conducted an audit of the Northern Lights CFC to determine whether the PCFO and LFCC complied with the provisions of 5 CFR 950, the regulations governing CFC operations. Of the 18 issues identified, the following best illustrate the enormity of the issues uncovered during this audit.

Undisbursed CFC Receipts

The PCFO did not properly record all 2012 campaign receipts, which resulted in $10,532 not being disbursed to charities;

Administrative Expenses

The PCFO incorrectly charged the 2012 campaign $7,818 for expenses that were related to other campaigns or were unallowable to the CFC;

Separation of CFC Financial Records

The PCFO was not maintaining CFC financial records separate from its internal organization's financial records;

Improper Matching of Receipts and Expenses

The PCFO did not properly allocate indirect general overhead expenses to the CFC;

Untimely Initial Disbursement

The PCFO did not make the initial disbursement to all charities by OPM's OCFC deadline;

Lack of LFCC Involvement in CFC Matters

Only 7 of the 15 LFCC members attended at least 50 percent of the meetings at which attendance was recorded, and the LFCC did not achieve 50 percent attendance at any of these meetings. Additionally, the LFCC did not hold meetings regarding the 2012 campaign until August 2012, missing the opportunity to make important campaign decisions required by the Federal regulations such as the selection of or renewal of the PCFO and the approval of one-time disbursements;

Performance Review of the PCFO by the LFCC

The LFCC did not provide evidence of its review of the PCFO's performance prior to renewing a multi-year agreement;

LFCC Approval of Campaign Expense Reimbursement

The LFCC did not review or authorize the PCFO's reimbursement of actual campaign expenses; and,

Improper Authorization of One-Time Disbursements

The LFCC did not authorize one-time disbursements or approve a threshold amount for the 2012 campaign.

For each of the four audits, we provided the audit findings and recommendations to OPM's OCFC for corrective action. The OCFC notified those campaigns of our recommendations and are monitoring any corrective actions. If the PCFOs and LFCCs do not comply with the recommendations, the Director of OPM can deny future participation in the CFC.

Campaign Merger Recommended Due to Non-Compliance with CFC Regulations

It is because of all of the concerns mentioned above that we support the final CFC regulations published in April 2014. These regulations will result in much needed revisions to the current CFC program and should be effective for the 2016 campaign. Specifically, we believe these program revisions will help eliminate many of the recurring findings we identify and will help to ensure that a larger percentage of Federal employees' donations are benefiting the participating charitable organizations.

ENFORCEMENT ACTIVITIES

Investigative Cases

The Office of Personnel Management administers benefits from its trust funds, with approximately $1 trillion in assets for all Federal civilian employees and annuitants participating in the Civil Service Retirement System, the Federal Employees Retirement System, FEHBP, and FEGLI. These programs cover over nine million current and retired Federal civilian employees, including eligible family members, and disburse over $128 billion annually. The majority of our OIG criminal investigative efforts are spent examining potential fraud against these trust funds. However, we also investigate OPM employee and contractor misconduct and other wrongdoing, such as fraud within the personnel security and suitability program administered by OPM.

During the reporting period, our office opened 48 criminal investigations and closed 21, with 124 still in progress. Our criminal investigations led to 10 arrests, 16 indictments and informations, 17 convictions and $4,188,783 in monetary recoveries to OPM-administered trust funds. Our criminal investigations, many of which we worked jointly with other Federal law enforcement agencies, also resulted in $39,630,300 in criminal fines and penalties, which are returned to the General Fund of the Treasury, asset forfeitures, and court fees and/or assessments. For a complete statistical summary of our office's investigative activity, refer to the table on page 33.

HEALTH CARE FRAUD CASES

Health care fraud cases are often time-consuming and complex, and may involve several health care providers who are defrauding multiple health insurance plans. Our criminal and civil investigations are critical to protecting Federal employees, annuitants, and members of their families who are eligible to participate in the FEHBP. Of particular concern are cases that involve harm to the patients, the growth of medical identity theft and organized crime in health care fraud, all of which have affected the FEHBP.

We coordinate our health care fraud investigations with the Department of Justice (DOJ) and other Federal, state, and local law enforcement agencies. We are participating members of health care fraud task forces across the nation. We work directly with U.S. Attorney's Offices nationwide to focus investigative resources in areas where fraud is most prevalent.

Our special agents are in regular contact with FEHBP health insurance carriers to identify possible fraud by health care providers and enrollees. Additionally, special agents work closely with our auditors when fraud issues arise during carrier audits. They also coordinate with the OIG's debarring official when investigations of FEHBP health care providers reveal evidence of violations that may warrant administrative sanctions. The following investigative cases represent some of our activity during the reporting period.

HEALTH CARE FRAUD CASES

FEHBP Beneficiary Pled Guilty to Receiving Over $2 Million from False Claims

A Department of Defense (DOD) employee living in Germany received over $2 million after he submitted false claims to both the FEHBP and the Department of Veterans Affairs (VA). Since he was living overseas and seeking health care on the local economy, he submitted his own insurance claims and was reimbursed directly by the insurance company. His fraud was discovered when a German pharmacist accidentally received one of the reimbursement checks, and called the FEHBP insurance carrier (the Foreign Service Benefit Plan) to report that the claimed drugs were never dispensed. We worked closely with the Veterans Affairs OIG, the Defense Criminal Investigative Service (DCIS), Army Criminal Investigative Service (CID and the German Criminal Police on this investigation, which required us to send one of our investigators to Germany.

The DOD employee was arrested by the German Criminal Police in April 2012 on charges of false claims and fraud within Germany and his home was searched. During the search, it was discovered that he was using the stolen money to build a new house, buy a new car, and that he had a safe filled with silver bars in his home. German and U.S. authorities seized assets worth $1.2 million after the search.

The DOD employee was indicted in the District of Columbia in October 2013 on 15 counts of fraud. The DOJ worked with German authorities to arrange extradition, and in July 2014 he self-surrendered and was extradited to the United States.

In December 2014, he pled guilty and was sentenced to serve 40 months in jail, 36 months' probation, and pay $2.2 in restitution ($943,519 to the FEHBP and $1,261,512 to the VA). As part of the plea agreement, he agreed that the assets seized, as well as any interest accrued on those assets, would be used to satisfy a portion of his court ordered restitution.

OtisMed Corporation and CEO Pled Guilty to Distributing Adulterated Medical Devices and Agree to Pay Over $80 Million

In December 2014, OtisMed Corporation and its former chief executive officer (CEO), pled guilty to distributing cutting guides that the Food and Drug Administration (FDA) rejected for knee replacement surgeries. OtisMed and its former CEO admitted to intentionally distributing the knee replacement surgery cutting guides after its application for marketing clearance had been rejected by the FDA. The corporation agreed to pay more than $80 million to resolve its related criminal and civil liability.

OtisMed pled guilty to charges that it distributed adulterated medical devices into interstate commerce, with the intent to defraud and mislead, in violation of the Food, Drug, and Cosmetic Act (FDCA). For criminal liability, OtisMed was fined $34.4 million and ordered to pay restitution of $5.16 million. In a separate civil settlement, OtisMed agreed to pay $40 million, plus interest, to resolve its civil liability. The CEO pled guilty to three counts of introducing adulterated medical devices in interstate commerce.

The former CEO was among the founders of OtisMed and acted as OtisMed's president and served as chairman of its board of directors until OtisMed was acquired by Stryker in November 2009. The former CEO also created the OtisKnee orthopedic cutting guide in August 2005, which became its primary sales product.

The OtisKnee was used by surgeons during total knee arthroplasty (TKA), commonly known as knee replacement surgery. This surgical procedure requires a surgeon to remove the ends of the leg bones and to reshape the remaining bone to accommodate the implanted artificial knee prosthesis. The cuts to the bone must be made at precise angles because they are critical to the clinical result. Failure to achieve the correct angle in a TKA procedure can result in unsuccessful implantation.

OtisMed marketed the OtisKnee cutting guide as a tool to assist surgeons in making accurate bone cuts specific to individual patients' anatomy based on magnetic resonance imaging (MRI) performed prior to surgery. None of OtisMed's claims regarding the OtisKnee device were evaluated by the FDA before the company used them in advertisements and promotional materials. Between May 2006 and September 2009, OtisMed sold more than 18,000 OtisKnee devices, generating revenues of approximately $27.1 million.

The civil settlement alleged that in May 2006, OtisMed, through co-promotional activities with Stryker Corporation, began commercially distributing the OtisKnee without having received clearance or approval from the FDA. OtisMed continued to distribute the device while its application was pending. Distribution continued even after the FDA informed OtisMed that the product could not be lawfully distributed until FDA approval was granted. The settlement also alleged that OtisMed encouraged health care providers to submit claims for MRIs that were not reimbursable because they were not performed for diagnostic use, but rather solely to provide data for the creation of the OtisKnee. The civil settlement resolves allegations arising from the marketing and distribution of the OtisKnee without receiving approval or clearance from the FDA.

As a result of the settlement, the FEHBP will receive $257,807. This case was a joint investigation conducted by the Department of Health and Human Services (HHS) OIG, the FDA, and our office.

Owner of Hearing Aid Center Prosecuted for Submitting Fraudulent Health Care Claims

In February 2011, we received an allegation from an FEHBP carrier alleging that a hearing aid center, located in Alabama, was submitting medical claims for services that were not rendered and not medically necessary. The hearing aid center directly solicited FEHBP members by offering "free or no cost" hearing aids.

The center's practice was to have the hearing aid center's owner purchase the hearing aids at a cost of approximately $538. Then the center would bill the FEHBP $1,475 per hearing aid, and would receive a reimbursement of $1,000 per hearing aid. The owner's common law husband was responsible for preparing and designing television, newspaper and magazine advertisements which directly solicited FEHBP members by offering these free enticements. FEHBP members were never asked to pay any co-payments related to the amounts the center billed the FEHBP, so that the scheme resulted in FEHBP participants allegedly receiving "free" hearing aids. In addition, the hearing aid center billed for hearing aid tests that were never performed and for tests for which they lacked equipment.

In February 2013, both the owner and her husband were indicted on ten counts of Health Care Fraud and five counts of False Statements Relating to Health Care Matters. In August 2013, both parties were indicted on a superseding indictment for one count of Conspiracy to Commit Health Care Fraud, five counts of Health Care Fraud for Services Not Rendered, five counts of Health Care Fraud for Double Billing, and five counts of False Statements Relating to Health Care Matters.

In June 2014, the owner received Pre-Trial Diversion. In October 2014, the husband was sentenced to serve five years' probation. Both were jointly ordered to pay $325,000 in restitution to the FEHBP.

Medicare, TRICARE, and the FEHBP Recover Over $2.3 Million from Physician's Use of Non-Approved Foreign Cancer Drugs

In October 2012, our office received an allegation from the FDA related to a doctor and his medical practice in Utah that was purchasing multiple medications from a foreign distributor. The majority of these products, sold and distributed by this foreign supplier, were not approved by the FDA and included counterfeit versions of various cancer drugs.

The doctor knowingly purchased non-approved cancer drugs from various foreign suppliers to administer to his patients. These foreign-sourced non-approved drugs were purchased at a considerable discount as compared to their respective domestic approved versions (The estimated discount was approximately 28 percent). The physician then knowingly billed Government health programs for the approved versions of the drugs when the non-approved versions were administered. Additionally, neither the various Federal health programs nor patients were informed that non-approved foreign-sourced drugs were being substituted for the approved versions. Records obtained from the doctor's practice indicate that over $3.6 million in foreign-sourced cancer drugs were purchased. However, unknown quantities of the non-approved drugs were administered to members of various Federal health programs.

In December 2014, the physician agreed to pay Federal health programs $2,317,867 to resolve civil allegations under the False Claims Act arising from his medical practice's submission of false claims to Medicare, TRICARE, and the FEHBP. Of this agreed payment, $104,304 will be paid to OPM for losses incurred by FEHBP insurance carriers.

This case was investigated by special agents from HHS OIG; Railroad Retirement Board (RRB) OIG; FDA; DCIS; and our office.

Miami Clinic Owners Submit Over $5 Million in False Claims and Hire Patient Recruiters

We initiated this investigation based on information received during another investigation in which a health care clinic located in Miami, Florida, submitted over $5 million in false claims to the FEHBP and private insurance companies for member services that were never provided. The health care clinic opened under the auspices of providing physical therapy services when they were actually billing for vitamin injections, purportedly to alleviate pain.

Through our investigation, we discovered that not only were the vitamin injections not administered to the patients, but when they were performed, the invoiced amount the clinic submitted would have resulted in serious harm to the patient if such amounts actually had been administered. Furthermore, our investigation uncovered that the clinic never ordered the amount of vitamins or injection supplies for which claims were submitted.

We also learned that the health care clinic paid kickbacks to two individuals to assist in recruiting clinic patients and paid them a portion of the proceeds from the false claims reimbursements received from recruited patients. Additionally, we uncovered that one of the patient recruiters recruited two United States Postal Service (USPS) employees who were also paid to receive services at the clinic. These USPS employees also accepted kickbacks for agreeing to serve as patients and allowing FEHBP billing for medical services that were not medically necessary and not provided.

In a previous Semi-Annual Report to Congress, we reported that the clinic's two owners were indicted, convicted and ordered to pay $190,306 in restitution to the FEHBP. In September 2014, the two individuals employed as patient recruiters also pled guilty to health care fraud.

In December 2014, one defendant was sentenced to serve 46 months in prison, followed by three years of supervised release for the role he played as patient recruiter for the medical clinic. The other defendant was sentenced to 65 months in prison, followed by three years of supervised release.

On April 2015, the two USPS employees who accepted payment in exchange for allowing their FEHBP insurance policies to be used by the clinic both pled guilty to health care fraud. They will be sentenced later this year.

This case was investigated by the Federal Bureau of Investigation (FBI), and the OIGs of HHS, USPS, and OPM.

Chiropractor and Co-conspirators Guilty of Health Care Fraud and Ordered to Pay Restitution Ranging from $1.3 to $2.4 Million

A chiropractor and several co-conspirators submitted claims for services not rendered to the FEHBP and private insurers in the Dallas-Fort Worth area. The conspiracy involved the chiropractor and a union representative engaging in a scheme in which the union representative recruited patients who would allow their insurance policies to be billed for services not rendered. In exchange for this fraudulent billing, monthly kickbacks, work excuse notes, and a variety of other incentives were received by the patients.

The Government presented trial evidence that from 2009 to 2012, the chiropractor and union representative, along with four other co-conspirators submitted health insurance claims to BlueCross BlueShield of Texas (BCBS) and other insurers, for services not rendered. Other co-conspirators included an occupational therapist, the clinic owner, office manager, and the individual responsible for billing. The office manager was also a clinic patient whose insurance policy was billed in excess of $700,000 for services not rendered for her family members as patients, when they had no knowledge that the clinic was billing for services in their names.

In June 2014, in the Northern District of Texas, the chiropractor and union representative were convicted by jury and found guilty of Conspiracy to Commit Health Care Fraud; Health Care Fraud; and Aggravated Identity Theft.

In November 2014 all defendants were sentenced and the four co-conspirators were sentenced to between six and ten months confinement in the U.S. Bureau of Prisons. The union representative was also sentenced to 156 months confinement. In January 2015, the chiropractor was sentenced to 145 months confinement. The court ordered each defendant to make restitution, jointly and severally with codefendants in amounts ranging from $1.3 to $2.4 million. The FEHBP Trust Fund received $39,329.

This was a joint investigation conducted by the FBI and our criminal investigators.

Debarred Unlicensed Physician Imprisoned and Fined for Making False Health Care Statements

This investigation was opened based on a request from the HHS OIG regarding a medical provider in Kansas City, Missouri alleged to have hired an unlicensed physician who was debarred from providing medical care to patients enrolled in all Federal health care programs, who was providing health care to these patients.

The investigation revealed that in May 2008, the unlicensed physician was banned from participating in Federal health care programs for a period of five years. This ban was due to a felony conviction in which he conspired to manufacture and distribute a controlled substance. The unlicensed physician operated within the medical home visit service and submitted claims to FEHBP, Medicare, Medicaid, and Tricare Federal programs from June 2008 to December 2012. All of these medical claims were for health care services that were provided after this provider was formally excluded from participating in Federal health care programs.

The unlicensed and debarred physician made false and fraudulent statements, to include his failure to disclose his debarment and his interest and involvement in the medical practice.

In May 2014, the unlicensed physician pled guilty to making false statements relating to health care matters. In November 2014 the debarred unlicensed provider was sentenced to 32 months imprisonment, three years supervised release, and ordered to pay restitution in the amount of $974,762, of which the FEHBP received $18,411.

This joint investigation was performed by the investigators from HHS OIG and our office.

Virginia Dentist Convicted of Health Care Fraud

A Virginia dentist was convicted of health care fraud because the provider was billing for services that were not performed.

The investigative team's evidence revealed that the fraudulent billing included such procedures as: incision and drainage, emergency palliative treatment, excision of hyperplastic tissue, and other restorative services. These services were not performed. The dentist was sentenced to serve 46 months in prison followed by twelve months of supervised release. He was also ordered to pay a fine of $250,000 and make restitution of $2,021,141, of which $168,819 was returned to OPM for FEHBP and the Federal Employees Dental and Vision Insurance Program.

In addition, the dentist entered into a civil settlement agreement with DOJ and agreed to pay $26,634 in lost investment income to OPM.

This case was investigated by the FBI and our investigative staff.

FEHBP Enrollee Convicted of Prescription Fraud

CVS Caremark, the pharmacy benefits manager for BCBS, received a tip from a pharmacist regarding forged prescriptions, and referred the allegations to our office. Investigation confirmed that an FEHBP enrollee, the spouse of a Federal employee, was forging prescriptions in order to obtain Schedule II Narcotics. Our investigators partnered with the vice/narcotics squad of the Police Department of Alexandria, Virginia and successfully executed search and arrest warrants. The case was presented to the Commonwealth's Attorney in Virginia for prosecution.

In January 2015, the defendant pled guilty to one felony count of prescription fraud and a misdemeanor count of possession of marijuana. He was sentenced to twelve months incarceration, suspended for two years, conditioned upon supervised probation with substance abuse treatment and fined $1,000.

This case was investigated by the Police Department from Alexandria, Virginia and our criminal investigators.

RETIREMENT FRAUD

Under the law, entitlement to annuity payments ceases upon the death of an annuitant or survivor annuitant (spouse). The most common type of retirement fraud involves the intentional receipt and use of Civil Service Retirement System (CSRS) or Federal Employees Retirement System (FERS) annuity benefit payments by an unentitled recipient. However, retirement fraud can also include incidents of elder abuse.

Our Office of Investigations uses a variety of approaches to identify potential retirement fraud cases for investigation. We coordinate closely with OPM's Retirement Services office to identify and address program vulnerabilities. We also coordinate with the Department of the Treasury's Financial Management Service to obtain payment information. Other referrals come from Federal, state, and local agencies, as well as private citizens. The OIG also works proactively to identify retirement fraud.

The following retirement fraud investigations represent some of our activities during the reporting period.

RETIREMENT FRAUD CASES

Daughter Fraudulently Receives Deceased Survivor Annuitant's Benefit Payments

We initiated this investigation in December 2013 after receiving an allegation that a Federal survivor annuitant died in 1977 and her daughter continued to receive her mother's benefit payments for 35 years.

Our investigation confirmed that the survivor annuitant's daughter maintained a joint bank account with her deceased mother where the

annuity benefit payments were electronically deposited. In addition, we learned that the daughter was fraudulently receiving her mother's Social Security benefits.

In July 2014, the daughter pled guilty to one count of theft of public money. The daughter paid full restitution at the time of her sentencing to OPM and Social Security Administration (SSA). SSA will receive $206,680 and OPM will receive $124,951. She was also ordered to perform ten hours of community service per week during the term of her supervised released and the court imposed a criminal fine of $40,000.

This was a joint OIG investigation conducted by criminal investigators from SSA and our office.

OIG Resolves Return of Annuitant's Benefit Payments

A suspected survivor annuitant fraud case was referred to our Office of Investigations by OPM's Reclamation Unit after unsuccessful attempts were made to recover the funds deposited into a joint checking account after the annuitant's death.

In December 2014, our investigators interviewed the daughter of the deceased annuitant. We determined that the she had made efforts to notify OPM of her mother's death, followed up with her mother's banking institution, and sought assistance from her tax accountant without resolution. In light of the evidence found, our investigative agents coordinated directly with OPM's Office of Retirement Services and the daughter to resolve repayment efforts in the amount of $43,266 to be paid to the OPM Trust Fund.

OPM Implements Identity Procedural Recommendations Following Theft of Annuity Benefit Payments

In December 2014, our Office of Investigations issued procedural recommendations to OPM's Retirement Services, based on our findings in a complaint involving a survivor annuitant suffering from advanced dementia. The survivor annuitant's son, who had been living with her, moved out, leaving her alone to fend for herself. He also changed the bank account where her annuity was deposited to an account he shared with his girlfriend, and thereby stole from his mother benefits totaling $11,015. In October 2012, the state of Alabama authorities discovered the survivor annuitant in unacceptable living conditions, moved her to a nursing home, and also arranged for a court-ordered conservator effective October 2013. Effective May 2014, OPM began issuing the survivor annuitant's benefits to the court-ordered conservator, as a representative payee. However, in June 2014, OPM changed the payment back to the account controlled by the son, based on a phone call from the son and his girlfriend.

We worked with local law enforcement on this case and subsequently the son and his girlfriend were arrested for theft of these funds. The case is currently pending final court disposition.

Procedural recommendations were presented to OPM concerning these internal control weaknesses including the lack of records documenting who requested the changes in bank accounts; the failure to record the telephone call OPM received from the survivor annuitant's son and his girlfriend; and the procedures used by OPM to verify caller identities. OPM concurred with our recommendations, and OPM's efforts to implement the recommendations are being tracked in the same manner as our audit resolution process.

REVOLVING FUND PROGRAM INVESTIGATIONS

Our office investigates OPM employee and contractor misconduct and other wrongdoing, including allegations of fraud within OPM's Revolving Fund programs, such as the background investigations program and human resources products and services.

OPM's Federal Investigative Services (FIS) conducts background investigations on Federal job applicants, employees, military members, and contractor personnel for suitability and security purposes. FIS conducts over 95 percent of all personnel background investigations

for the Federal Government. With a staff of over 9,600 Federal and contract employees, FIS processed over 2.3 million background investigations in FY 2013. Federal agencies use the reports of investigations conducted by OPM to determine individuals' suitability for employment and eligibility for access to national security classified information.

The violations investigated by our criminal investigators include fabrications by OPM background investigators (i.e., the submission of work products that purport to represent investigative work which was not in fact performed). We consider such cases to be a serious national security and public trust concern. If a background investigation contains incorrect, incomplete, or fraudulent information, a qualified candidate may be wrongfully denied employment or an unsuitable person may be cleared and allowed access to Federal facilities or classified information.

OPM's Human Resources Solutions (HRS) provides other Federal agencies, on a reimbursable basis, with human resource products and services to help agencies develop leaders, attract and build a high quality workforce, and transform into high performing organizations. For example, HRS operates the Federal Executive Institute, a residential training facility dedicated to developing career leaders for the Federal Government. Cases related to HRS investigated by our criminal investigators include employee misconduct, regulatory violations, and contract irregularities.

The following Revolving Fund investigations represent some of our activities during the reporting period.

Former OPM Background Investigator Convicted of Falsifying Numerous Background Investigations

In May 2014, our office received an allegation from the FIS Integrity Assurance Group regarding misconduct and false statements made by an OPM background investigator.

From the summer of 2013 through April 2014, in ten Reports of Investigation, the background investigator indicated that she had interviewed a source or reviewed a record relating to the subject of the background investigation, when in fact, she had not conducted the interview or obtained the record of interest. These reports were utilized and relied upon by Federal agencies requesting the background investigations to determine whether these subjects were suitable for positions having access to classified information, for positions impacting national security and public trust, or for receiving or retaining security clearances. These false representations required FIS to reopen and reinvestigate numerous background investigations assigned to the background investigator.

Our criminal investigators interviewed the background investigator who admitted she randomly falsified reports, to include, multiple source contacts and personal testimony which she falsely reported that she had interviewed. Furthermore, she also admitted that on numerous occasions she falsified documentary evidence, such as employment and residential record reports, to verify and corroborate information provided by the subject of the background investigation.

The former background investigator pled guilty to making a false statement and was sentenced in December 2014 to serve 48 months of supervised probation, perform 100 hours of community service, and ordered to pay restitution of $10,000 to OPM.

OIG HOTLINE AND COMPLAINT ACTIVITY

The OIG's Fraud Hotline also contributes to identifying fraud and abuse. The Hotline telephone number, email address, and mailing address are listed on our OIG Web site at *www.opm.gov/oig*, along with an online anonymous complaint form. Contact information for the Hotline is also published in the brochures for all of the FEHBP health insurance plans. Those who report information to our Hotline can do so openly, anonymously, and confidentially without fear of reprisal.

The information we receive on our OIG Hotline generally concerns customer service issues, FEHBP health care fraud, retirement fraud, and other complaints that may warrant investigation. Our office receives inquiries from the general public, OPM employees, contractors and others interested in reporting waste, fraud, and abuse within OPM and the programs it administers.

We received 740 hotline inquires during the reporting period, with 227 pertaining to health care and insurance issues, and 513 concerning retirement or special investigation. The table on page 33 reports the summary of hotline activities including telephone calls, emails, and letters.

OIG and External Initiated Complaints

Based on our knowledge of OPM program vulnerabilities, information shared by OPM program offices and contractors, and our liaison with other law enforcement agencies, we initiate our own inquiries into possible cases involving fraud, abuse, integrity issues, and occasionally malfeasance.

During this reporting period, we initiated 65 preliminary inquiry complaints related to retirement fraud and special investigations. We also initiated 676 health care fraud preliminary inquiry complaints. These efforts may potentially evolve into formal investigations.

We believe that these OIG and external initiated complaints complement our hotline to ensure that our office continues to be effective in its role to guard against and identify instances of fraud, waste, and abuse.

Debarment Initiative Update

As discussed in previous reporting periods, the agency implemented a new Suspension and Debarment program, which became effective March 2013. During this reporting period, the OIG referred 18 cases to the agency for debarment action, for a total of 59 referrals since the inception of the program. OPM issued Debarment letters to 17 individuals between October 2014 and March 2015. The majority of cases we refer for debarment action have been former Federal Investigative Services (FIS) employees and contractors. Most of these former FIS employees and contractors are referred to us through FIS' internal controls and programs. Although these individuals were removed from Government employment or from the relevant OPM contract, we feel that Government-wide contract debarment action for these individuals is necessary to protect the integrity of Federal programs.

Our office will continue to develop and refer cases where we believe a Government-wide debarment is necessary in order to protect the integrity of OPM, as well as other Federal agencies and programs.

Administrative Sanctions of FEHBP Health Care Providers

Under the FEHBP administrative sanctions statute, we issue debarments and suspensions of health care providers whose actions demonstrate that they are not responsible to participate in the program. At the end of the reporting period, there were 33,397 active suspensions and debarments from the FEHBP.

During the reporting period, our office issued 366 administrative sanctions – including both suspensions and debarments – of health care providers who have committed violations that impact the FEHBP and its enrollees. In addition, we responded to 2,904 sanctions-related inquiries.

We develop our sanctions caseload from a variety of sources, including:

- Administrative actions issued against health care providers by other Federal agencies;
- Cases referred by the OIG's Office of Investigations;
- Cases identified by our office through systematic research and analysis of electronically-available information about health care providers, referred to as e-debarment; and,
- Referrals from other sources, including health insurance carriers and state Government regulatory and law enforcement agencies.

Sanctions serve a protective function for the FEHBP and the Federal employees who obtain, through it, their health insurance coverage. The following articles, highlighting a few of the administrative sanctions handled by our office during the reporting period, illustrate their value against health care providers who have placed the safety of enrollees at risk, or have obtained fraudulent payment of FEHBP funds.

Debarment *disqualifies a health care provider from receiving payment of FEHBP funds for a stated period of time. The FEHBP administrative sanctions program establishes 18 bases for debarment. The ones we cite most frequently are for criminal convictions or professional licensure restrictions or revocations. Before debarring a provider, our office gives prior notice and the opportunity to contest the sanction in an administrative proceeding.*

Suspension *has the same effect as a debarment, but becomes effective upon issuance, without prior notice or process. FEHBP sanctions law authorizes suspension only in cases where adequate evidence indicates that a provider represents an immediate risk to the health and safety of FEHBP enrollees.*

The following is a summary of one of our debarment actions.

Michigan Physician Debarred for Participating in Health Care Fraud Scheme

In January 2015, our office debarred a Lansing, Michigan Internist. The Internist was part of a group of 44 physicians, pharmacists, pharmacy owners, home health care operators, and others who engaged in a conspiracy to defraud private insurance companies and Government insurance programs, including the FEHBP. According to the U. S. Attorney's Office for the Eastern District of Michigan, the 44 individuals participated in a scheme to defraud health care programs of over $21.5 million.

Various individuals in the group were charged with:

- Unlawful distribution and dispensing of various controlled substances, including OxyContin, Oxycodone, Vicodin, Opana, Codeine, Xanax, and Lortab, without conducting an appropriate medical examination supporting the prescription's necessity;
- Receiving kickbacks, bribes, money laundering, health care fraud, and other illegal benefits from the sale of drugs obtained by writing illegal prescriptions; and,
- Submitting fraudulent home health claims.

To support the claims, medical practices and medical clinics were organized in multiple locations throughout Michigan and Ohio to engage in various aspects of the scheme. The group employed patient recruiters or "marketers" to obtain patients or patient's personal information and directed them to one of the six doctors involved in the conspiracy. The doctors would sometimes perform a cursory examination; in most cases the patient did not receive an examination nor had any physical contact with the physician. After the limited examination or exposure to the patient's information, prescriptions for controlled substances were written, and the physician would direct the patients to have them filled at one of the pharmacies in their network.

The United States District Court, Eastern District of Michigan sentenced the Internist to eighteen months in prison; three years supervised release, and ordered him to pay $582,912 in restitution for health care fraud.

In September 2013, we suspended the physician from participating in the FEHBP based on his indictment in the health care fraud scheme. Subsequent to our suspension, the physician was excluded from participating as a health care provider in Medicaid and Medicare by the Department of Health and Human Services (DHHS). Under Federal law and regulations, our office must debar any health care provider who has been excluded by another Federal agency. Therefore, our final action to debar the provider was based on his exclusion by DHHS. The terms of our debarment will run concurrent with the term of the physician's DHHS exclusion.

STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES

Judicial Actions:

Indictments and Informations 16
Arrests. 10
Convictions 17

Judicial Recoveries:

Restitutions and Settlements $4,188,783
Fines, Penalties, Assessments, and Forfeitures . . . . . $39,630,300[1]

Retirement and Special Investigations Hotline and Preliminary Inquiry Activity:

HOTLINE

Referred to:

- OPM Program Offices 159
- Other Federal Agencies. 168
- Informational Only 139
- Inquiries Initiated 4
- Retained for Further Inquiry. 43

Total Received: 513

(Continued on next page)

[1]*This figure represents criminal fines and criminal penalties returned not to OPM, but to the general fund of the Treasury. It also includes asset forfeitures and court assessments and/or fees resulting from criminal investigations conducted by our office. Many of these criminal investigations were conducted jointly with other Federal agencies, who share the credit for the fines, penalties, assessments, and forfeitures.*

PRELIMINARY INQUIRY COMPLAINTS

Total Received: 65

Total Closed: 56

Health Care Fraud Hotline and Preliminary Inquiry Complaint Activity:

HOTLINE

Referred to:

- OPM Program Offices 65
- FEHBP Insurance Carriers or Providers 59
- Other Federal Agencies. 13
- Informational Only 65
- Inquiries Initiated 2
- Retained for Further Inquiry. 23

Total Received: 227

PRELIMINARY INQUIRY COMPLAINTS

Total Received: 676

Total Closed: 812

Hotline Contacts and Preliminary Inquiry Complaints:

Total Hotline Contacts and Preliminary Inquiries Received:. 1,481

Total Hotline Contacts and Preliminary Inquiries Closed:. 1,542

Administrative Sanctions Activity:

FIS Cases Referred for Debarment and Suspension 18

Health Care Debarments and Suspensions Issued 366

Health Care Provider Debarment and Suspension Inquiries 2,904

Health Care Debarments and Suspensions in Effect at End of Reporting Period. 33,397

APPENDICES

APPENDIX I-A
Final Reports Issued With Questioned Costs for Insurance Programs
OCTOBER 1, 2014 TO MARCH 31, 2015

Subject	Number of Reports	Dollar Value
A. Reports for which no management decision had been made by the beginning of the reporting period	1	$ (4,613)[2]
B. Reports issued during the reporting period with findings	10	9,799,095
Subtotals (A+B)	11	9,794,482
C. Reports for which a management decision was made during the reporting period:	11	9,794,482
1. Disallowed costs	N/A	9,876,685
2. Costs not disallowed	N/A	(82,203)[2]
D. Reports for which no management decision has been made by the end of the reporting period	0	0
E. Reports for which no management decision has been made within 6 months of issuance	0	0

[2]Represents the net costs, which includes overpayments and underpayments, to insurance carriers. Underpayments are held (no management decision officially made) until overpayments are recovered.

APPENDIX I-B
Final Reports Issued With Questioned Costs for All Other Audit Entities
OCTOBER 1, 2014 TO MARCH 31, 2015

Subject	Number of Reports	Dollar Value
A. Reports for which no management decision had been made by the beginning of the reporting period	2	$2,044,484
B. Reports issued during the reporting period with findings	4	22,730
Subtotals (A+B)	6	2,067,214
C. Reports for which a management decision was made during the reporting period:	1	32,955
1. Disallowed costs	N/A	32,955
2. Costs not disallowed	N/A	0
D. Reports for which no management decision has been made by the end of the reporting period	5	2,034,259
E. Reports for which no management decision has been made within 6 months of issuance	1	2,011,529

APPENDIX II
Final Reports Issued with Recommendations for Better Use of Funds
OCTOBER 1, 2014 TO MARCH 31, 2015

Subject	Number of Reports	Dollar Value
No activity during this reporting period	0	$0

APPENDIX III
Insurance Audit Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued	Questioned Costs
1H-01-00-14-008	Limited Scope Audit of BlueCross and BlueShield's Pricing of Pharmacy Claims as Administered by Caremark PCS Health LLC for Contract Year 2012 in Scottsdale, Arizona	October 6, 2014	$ 0
1C-ML-00-14-022	AvMed Health Plans in Gainesville, Florida	October 9, 2014	0
1C-WD-00-14-033	Dean Health Plan, Inc. in Madison, Wisconsin	October 9, 2014	0
1C-LP-00-14-044	Health Net of California, Inc. - Southern Region in Woodland Hills, California	October 9, 2014	0
1C-JC-00-14-047	Aetna Open Access - New York in Blue Bell, Pennsylvania	October 15, 2014	0
1C-ZJ-00-14-019	Humana Health Plans of Puerto Rico, Inc. in San Juan, Puerto Rico	October 23, 2014	0
1A-10-55-14-027	Independence BlueCross in Philadelphia, Pennsylvania	December 2, 2014	86,594
1C-RL-00-14-042	Grand Valley Health Plan, Inc. in Grand Rapids, Michigan	December 3, 2014	0
1C-9U-00-14-034	Physicians Health Plan in Lansing, Michigan	December 23, 2014	90,226
1G-LT-00-14-025	Federal Long Term Care Insurance Program as Administered by Long Term Care Partners, LLC for Contract Years 2010 through 2012 in Portsmouth, New Hampshire	December 23, 2014	(43,066)
1G-LT-00-14-031	BENEFEDS as Administered by Long Term Care Partners, LLC for Contract Years 2010 through 2013 in Portsmouth, New Hampshire	December 23, 2014	77,852
1A-10-15-14-030	BlueCross BlueShield of Tennessee in Chattanooga, Tennessee	December 24, 2014	5,824,432
1C-BJ-00-14-052	Coventry Health Care of Louisiana, Inc. in Downers Grove, Illinois	January 14, 2015	0
1C-NM-00-14-056	Health Plan of Nevada, Inc. in Las Vegas, Nevada	January 14, 2015	0
1A-10-69-14-012	Regence in Portland, Oregon	January 20, 2015	1,066,072
1C-SF-00-14-060	SelectHealth Plan in Murray, Utah	January 29, 2015	0

APPENDIX III
Insurance Audit Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

(Continued)

Report Number	Subject	Date Issued	Questioned Costs
1C-JK-00-14-032	TakeCare Insurance Company in Tamuning, Guam	January 29, 2015	$ 163,557
1C-2U-00-14-059	Aetna Open Access – Athens and Atlanta, Georgia in Blue Bell, Pennsylvania	February 20, 2015	0
1C-U4-00-14-038	Health Plan of the Upper Ohio Valley, Inc. in St. Clairsville, Ohio	February 20, 2015	2,144,107
1C-ML-00-14-026	AvMed Health Plans in Gainesville, Florida	February 27, 2015	182,000
1C-JR-00-14-058	Aetna Open Access - Northern New Jersey in Blue Bell, Pennsylvania	March 23, 2015	0
1C-M9-00-15-003	MVP Health Plan, Inc. - Central Region in Schenectady, New York	March 23, 2015	0
1C-MX-00-15-004	MVP Health Plan, Inc. – Mid-Hudson Region in Schenectady, New York	March 23, 2015	0
1C-LB-00-14-043	Health Net of California - Northern Region in Woodland Hills, California	March 23, 2015	207,321
TOTALS			**$9,799,095**

APPENDIX IV
Internal Audit Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued
4A-CF-00-14-039	OPM's Fiscal Year 2014 Consolidated Financial Statements in Washington, D.C.	November 10, 2014
4A-CF-00-14-040	OPM's Fiscal Year 2014 Closing Package Financial Statements in Washington, D.C.	November 17, 2014

APPENDIX V
Combined Federal Campaign Audit Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued
3A-CF-00-14-050	The 2011 and 2012 Chesapeake Bay Area Combined Federal Campaigns of Central Maryland in Baltimore, Maryland	December 23, 2014
3A-CF-00-14-049	The 2011 and 2012 Long Island Combined Federal Campaigns in Deer Park, New York	February 11, 2015
3A-CF-00-14-048	The 2011 and 2012 Northern Lights Combined Federal Campaigns in St. Paul, Minnesota	March 23, 2015
3A-CF-00-14-041	The 2011 and 2012 Tennessee Valley Combined Federal Campaigns in Huntsville, Alabama	March 23, 2015

APPENDIX VI
Information Systems Audit Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued
4A-CI-00-14-016	Federal Information Security Management Act for Fiscal Year 2014 in Washington, D.C.	November 12, 2014
1A-10-70-14-007	Information Systems General and Application Controls at Premera BlueCross in Mountlake Terrace, Washington	November 28, 2014
4A-CI-00-14-064	Information Technology Security Controls of OPM's Dashboard Management Reporting System in Washington, D.C.	January 14, 2015
1A-10-49-14-021	Information Systems General and Application Controls at Horizon BlueCross BlueShield in Newark, New Jersey	February 11, 2015

APPENDIX VII
Evaluation Reports Issued
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued
4K-RS-00-14-076	Review of OPM's Compliance with the Freedom of Information Act in Washington, D.C.	March 23, 2015

APPENDIX VIII
Summary of Reports More Than Six Months Old Pending Corrective Action
OCTOBER 1, 2014 TO MARCH 31, 2015

Report Number	Subject	Date Issued
4A-CF-00-05-028	Administration of the Prompt Payment Act at OPM in Washington, D.C.; 12 total recommendations; 1 open recommendation	April 16, 2007
4A-CI-00-08-022	Federal Information Security Management Act for Fiscal Year 2008 in Washington, D.C.; 19 total recommendations; 2 open recommendations	September 23, 2008
4A-CF-00-08-025	OPM's Fiscal Year 2008 Consolidated Financial Statement in Washington, D.C.; 6 total recommendations; 1 open recommendation	November 14, 2008
4A-CI-00-09-031	Federal Information Security Management Act for Fiscal Year 2009 in Washington, D.C.; 30 total recommendations; 2 open recommendations	November 5, 2009
4A-CF-00-09-037	OPM's Fiscal Year 2009 Consolidated Financial Statement in Washington, D.C.; 5 total recommendations; 1 open recommendation	November 13, 2009
4A-IS-00-09-060	Quality Assurance Process Over Background Investigations in Washington, D.C.; 18 total recommendations; 1 open recommendation	June 22, 2010
4A-CF-00-10-015	OPM's Fiscal Year 2010 Consolidated Financial Statement in Washington, D.C.; 7 total recommendations; 3 open recommendations	November 10, 2010
4A-CI-00-10-019	Federal Information Security Management Act for FY 2010 in Washington, D.C.; 41 total recommendations; 3 open recommendations	November 10, 2010
1K-RS-00-11-068	Stopping Improper Payments to Deceased Annuitants in Washington, D.C.; 14 total recommendations; 3 open recommendations	September 14, 2011
4A-CI-00-11-009	Federal Information Security Management Act for Fiscal Year 2011 in Washington, D.C.; 29 total recommendations; 6 open recommendations	November 9, 2011
4A-CF-00-11-050	OPM's Fiscal Year 2011 Consolidated Financial Statement in Washington, D.C.; 7 total recommendations; 1 open recommendation	November 14, 2011
4A-RI-00-12-034	Insecure Password Reset Process on Agency-owned Information Systems in Washington, D.C.; 3 total recommendations; 1 open recommendation	February 7, 2012
4A-CF-00-09-014	OPM's Interagency Agreement Process in Washington, D.C.; 8 total recommendations; 2 open recommendations	March 28, 2012
4A-OP-00-12-013	Information Technology Security Controls of OPM's Audit Report and Receivables Tracking System in Washington, D.C.; 24 total recommendations; 14 open recommendations	July 16, 2012
4A-CF-00-11-067	Administration of the Prompt Payment Act at OPM in Washington, D.C.; 12 total recommendations; 6 open recommendations	September 13, 2012
4A-CI-00-12-016	Federal Information Security Management Act for FY 2012 in Washington, D.C.; 18 total recommendations; 8 open recommendations	November 5, 2012

APPENDIX VIII
Summary of Reports More Than Six Months Old Pending Corrective Action
OCTOBER 1, 2014 TO MARCH 31, 2015
(Continued)

Report Number	Subject	Date Issued
4A-CF-00-12-039	OPM's Fiscal Year 2012 Consolidated Financial Statement in Washington, D.C.; 3 total recommendations; 1 open recommendation	November 15, 2012
1K-RS-00-12-031	OPM's Voice over the Internet Protocol Phone System Interagency Agreement with the District of Columbia in Washington, D.C.; 2 total recommendations; 1 open recommendation	December 12, 2012
1A-10-67-12-004	BlueShield of California in San Francisco, California; 13 total recommendations; 2 open recommendations	January 10, 2013
1A-99-00-12-055	Global Assistant Surgeon Claim Overpayments for BlueCross and BlueShield Plans in Washington, D.C.; 3 total recommendations; 1 open recommendation	February 21, 2013
1A-99-00-12-029	Global Coordination of Benefits for BlueCross and BlueShield Plans in Washington, D.C.; 7 total recommendations; 4 open recommendations	March 20, 2013
4A-CF-00-12-066	Assessing the Relevance and Reliability of OPM's Performance Information in Washington, D.C.; 5 total recommendations; 1 open recommendation	April 1, 2013
1A-10-32-12-062	BlueCross BlueShield of Michigan in Detroit, Michigan; 11 total recommendations; 3 open recommendations	July 19, 2013
1A-99-00-13-004	Global Continuous Stay Claims for BlueCross and BlueShield Plans in Washington, D.C.; 6 total recommendations; 1 open recommendation	August 20, 2013
1A-10-41-12-050	Florida Blue in Jacksonville, Florida; 13 total recommendations; 6 open recommendations	September 10, 2013
4A-CI-00-13-036	OPM's Common Security Control Collection in Washington, D.C.; 4 total recommendations; 1 open recommendation	October 10, 2013
1H-01-00-12-072	BlueCross and BlueShield's Retail Pharmacy Member Eligibility in 2006, 2007, and 2011 in Washington, D.C.; 11 total recommendations; 11 open recommendations	November 8, 2013
4A-CI-00-13-021	Federal Information Security Management Act for FY 2013 in Washington, D.C.; 16 total recommendations; 9 open recommendations	November 21, 2013
1A-99-00-13-032	Global Coordination of Benefits for BlueCross and BlueShield Plans in Washington, D.C.; 7 total recommendations; 5 open recommendations	November 22, 2013
4A-CF-00-13-034	OPM's Fiscal Year 2013 Consolidated Financial Statement in Washington, D.C.; 1 total recommendation; 1 open recommendation	December 13, 2013
1B-32-00-13-017	National Association of Letter Carriers Health Benefit Plan in Ashburn, Virginia; 12 total recommendations; 7 open recommendations	December 23, 2013
1A-10-17-13-026	Information Systems General and Application Controls at Health Care Service Corporation in Chicago, Illinois; 12 total recommendations; 6 open recommendations	January 28, 2014
4A-IS-00-14-017	Information Technology Security Controls of OPM's Investigations, Tracking, Assigning and Expediting System Fiscal Year 2014 in Washington, D.C.; 4 total recommendations; 1 open recommendation	April 3, 2014

APPENDIX VIII
Summary of Reports More Than Six Months Old Pending Corrective Action
OCTOBER 1, 2014 TO MARCH 31, 2015
(Continued)

Report Number	Subject	Date Issued
4A-CF-00-14-009	OPM's Fiscal Year 2013 Improper Payments Reporting for Compliance with the Improper Payments Elimination and Recovery Act of 2010 in Washington, D.C.; 1 total recommendation; 1 open recommendation	April 10, 2014
1A-99-00-13-046	Global Non-Covered Ambulance Claims for BlueCross and BlueShield Plans in Washington, D.C.; 4 total recommendations; 1 open recommendation	April 17, 2014
1B-32-00-13-037	Information Systems General and Application Controls at the National Association of Letter Carriers Health Benefit Plan in Ashburn, Virginia; 41 total recommendations; 20 open recommendations	May 6, 2014
4A-IS-00-13-062	The Federal Investigative Services' Case Review Process over Background Investigations in Washington, D.C.; 6 total recommendations; 6 open recommendations	June 4, 2014
1A-10-15-13-058	BlueCross BlueShield of Tennessee in Chattanooga, Tennessee; 16 total recommendations; 14 open recommendations	June 6, 2014
4A-CI-00-14-015	Information Technology Security Controls of OPM's Development Test Production General Support System Fiscal Year 2014 in Washington, D.C.; 6 total recommendations; 6 open recommendations	June 6, 2014
1C-2C-00-13-056	Piedmont Community HealthCare in Lynchburg, Virginia; 2 total recommendations; 2 open recommendations	July 9, 2014
1A-10-67-14-006	Information Systems General and Application Controls at Blue Shield of California in San Francisco, California; 16 total recommendations; 7 open recommendations	July 9, 2014
4A-CI-00-14-028	Status of Cloud Computing Environments within OPM in Washington, D.C.; 3 total recommendations; 3 open recommendations	July 9, 2014
3A-CF-00-13-051	The 2005 through 2012 Combined Federal Campaigns as Administered by the Metropolitan Arts Partnership in Sacramento, California; 10 total recommendations; 5 open recommendations	July 10, 2014
Not Applicable	Review of FIS Background Investigation Process; 3 total recommendations; 3 open recommendations	August 15, 2014
1A-99-00-13-061	Global Duplicate Claim Payments for BlueCross and BlueShield Plans in Washington, D.C.; 6 total recommendations; 6 open recommendations	August 19, 2014
4A-RI-00-14-036	Information Technology Security Controls of OPM's BENEFEDS and Federal Long Term Care Insurance Program Information Systems Fiscal Year 2014 in Washington, D.C.; 10 total recommendations; 9 open recommendations	August 19, 2014
1A-10-13-14-003	Highmark Inc.in Camp Hill, Pennsylvania; 7 total recommendations; 1 open recommendation	August 22, 2014

APPENDIX IX
Most Recent Peer Review Results
OCTOBER 1, 2014 TO MARCH 31, 2015

We do not have any open recommendations to report from our peer reviews.

Subject	Date of Report	Result
System Review Report for the U.S. Office of Personnel Management's Office of the Inspector General Audit Organization *(Issued by the Office of Inspector General, Board of Governors of the Federal Reserve System)*	September 26, 2012	Pass[3]
Quality Control System Review of the U.S. Department of Commerce's Office of Inspector General Audit Organization *(Issued by the Office of the Inspector General, U.S. Office of Personnel Management)*	July 13, 2012	Pass[3]
Quality Assessment Review of the Investigative Operations of the Office of the Inspector General for the Railroad Retirement Board *(Issued by the Office of the Inspector General, U.S. Office of Personnel Management)*	August 13, 2014	Compliant[4]
Quality Assessment Review of the Investigative Operations of the Office of the Inspector General for the U.S. Office of Personnel Management *(Issued by the Office of Inspector General, U.S. Department of State)*	June 21, 2013	Compliant[4]

*[3]A peer review rating of **Pass** is issued when the reviewing Office of Inspector General concludes that the system of quality control for the reviewed Office of Inspector General has been suitably designed and complied with to provide it with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The Peer Review does not contain any deficiencies or significant deficiencies.*

*[4]A rating of **Compliant** conveys that the reviewed Office of Inspector General has adequate internal safeguards and management procedures to ensure that the Council of the Inspectors General on Integrity and Efficiency standards are followed and that law enforcement powers conferred by the 2002 amendments to the Inspector General Act are properly exercised.*

APPENDIX X
Investigative Recoveries
OCTOBER 1, 2014 TO MARCH 31, 2015

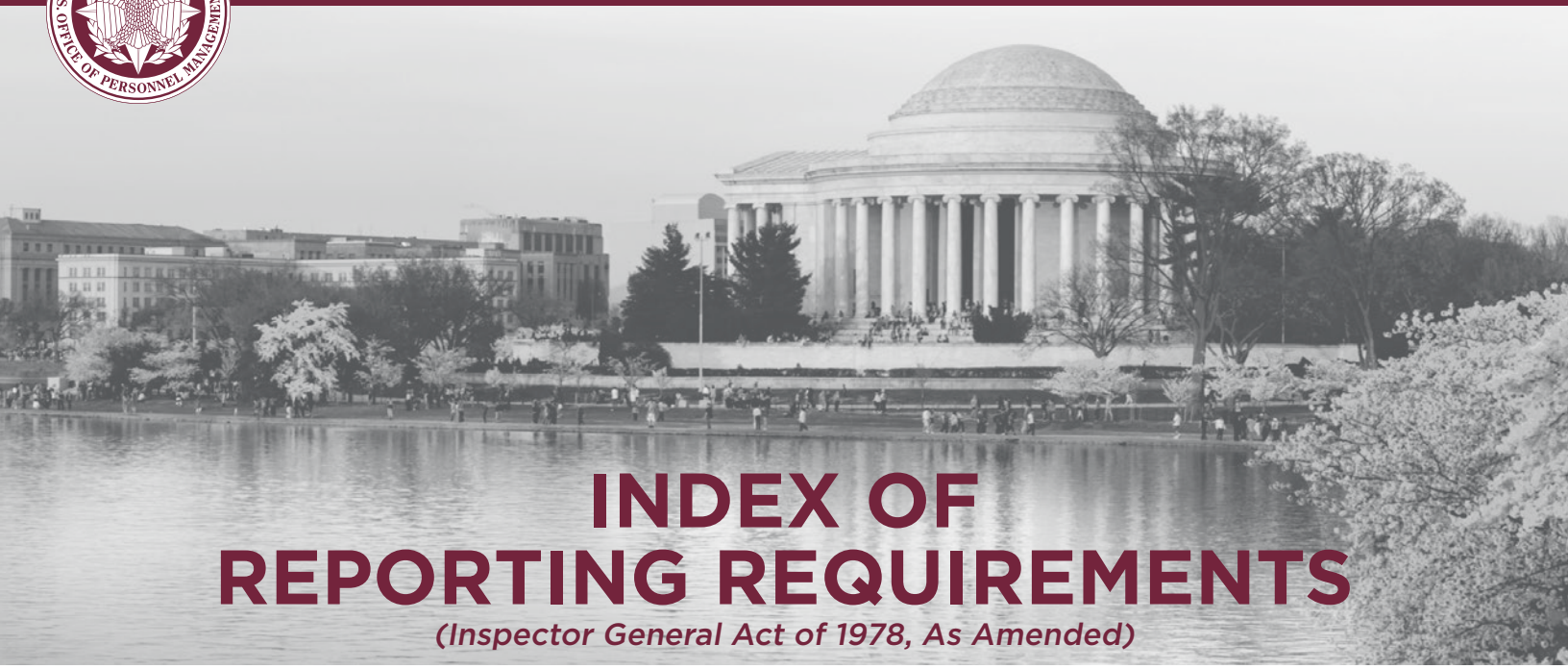
OIG Case Number[5]	Case Category	Action[5]	OPM Recovery (Net)	Total Recovery (All Programs/ Victims)	Fines, Penalties, Assessments, and Forfeitures
I 2011 00004	Federal Investigative Services Fraud	Administrative	$ 107,124	$ 107,124	$ 0
I-12-00006	Federal Investigative Services Fraud	Administrative	162,301	162,301	0
I-12-00442	Federal Investigative Services Fraud	Administrative	80,835	80,835	0
I-12-00637	Federal Investigative Services Fraud	Administrative	95,114	95,114	0
I-13-00144	Federal Investigative Services Fraud	Administrative	248,119	248,119	0
I-14-00829	Federal Investigative Services Fraud	Criminal	10,000	10,000	100
TOTAL	**Federal Investigative Services Fraud**		**$ 703,493**	**$ 703,493**	**$ 100**
I 2010 00461	Healthcare Fraud	Civil	1,578,607	22,280,000	0
I 2011 00194	Healthcare Fraud	Civil	257,807	41,158,232	0
I 2011 00423	Healthcare Fraud	Civil	9,700	662,000	0
I-12-00037	Healthcare Fraud	Civil	26,634	27,458	0
I-12-00415	Healthcare Fraud	Civil	137,124	6,400,000	0
I-13-00018	Healthcare Fraud	Civil	5,035	92,503	0
I-13-00286	Healthcare Fraud	Civil	101,175	2,317,867	0
I-13-00560	Healthcare Fraud	Civil	9,426	28,800	0
I 2007 00109[5]	Healthcare Fraud	Criminal	0	2,482,902	100
I 2011 00023	Healthcare Fraud	Criminal	0	0	200
I 2011 00051	Healthcare Fraud	Criminal	0	0	100
I 2011 00148	Healthcare Fraud	Criminal	0	0	1,025
I 2011 00148	Healthcare Fraud	Criminal	0	0	1,025
I 2011 00148	Healthcare Fraud	Criminal	0	0	1,025
I 2011 00148	Healthcare Fraud	Criminal	0	0	1,100
I 2011 00148	Healthcare Fraud	Criminal	0	0	1,025
I 2011 00148	Healthcare Fraud	Criminal	0	0	2,600

APPENDIX X
Investigative Recoveries
OCTOBER 1, 2014 TO MARCH 31, 2015
(Continued)

OIG Case Number[5]	Case Category	Action[5]	OPM Recovery (Net)	Total Recovery (All Programs/ Victims)	Fines, Penalties, Assessments, and Forfeitures
I 2011 00148	Healthcare Fraud	Criminal	$ 0	$ 0	$ 2,700
I 2011 00148	Healthcare Fraud	Criminal	0	0	3,700
I 2011 00148	Healthcare Fraud	Criminal	0	0	5,100
I 2011 00148	Healthcare Fraud	Criminal	0	0	5,100
I 2011 00148	Healthcare Fraud	Criminal	0	0	100
I 2011 00148	Healthcare Fraud	Criminal	0	0	100
I 2011 00194	Healthcare Fraud	Criminal	0	0	39,560,400
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,895	1,000
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,895	100
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,895	100
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,896	100
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,896	1,000
I 2011 00359	Healthcare Fraud	Criminal	6,555	404,896	100
I-12-00314	Healthcare Fraud	Criminal	943,519	2,205,032	100
I-12-00378	Healthcare Fraud	Criminal	18,411	974,762	900
I-14-00298	Healthcare Fraud	Criminal	190,306	1,473,504	100
I-14-00299	Healthcare Fraud	Criminal	0	0	100
I-14-00699	Healthcare Fraud	Criminal	0	0	1,000
TOTAL	Healthcare Fraud		$3,317,074	$82,532,433	$39,590,000
I-14-01227	Retirement Fraud	Administrative	43,266	43,266	0
I-14-00201	Retirement Fraud	Criminal	124,950	331,630	40,200
TOTAL	**Retirement Fraud**		**$ 168,216**	**$ 374,896**	**$ 40,200**
GRAND TOTAL			**$4,188,783**	**$83,610,822**	**$39,630,300**

[5] *The amount of OPM's recovery has not been calculated yet. The conviction and judgment have been appealed.*

Note: Cases that are listed multiple times indicate there were multiple subjects.



INDEX OF REPORTING REQUIREMENTS

(Inspector General Act of 1978, As Amended)

		Page
Section 4 (a) (2):	Review of legislation and regulations	No Activity
Section 5 (a) (1):	Significant problems, abuses, and deficiencies	1-31
Section 5 (a) (2):	Recommendations regarding significant problems, abuses, and deficiencies	1-19
Section 5 (a) (3):	Recommendations described in previous semiannual reports on which corrective action has not been completed	No Activity
Section 5 (a) (4):	Matters referred to prosecutive authorities	21-31
Section 5 (a) (5):	Summary of instances where information was refused during this reporting period	No Activity
Section 5 (a) (6):	Listing of audit reports issued during this reporting period	37-39
Section 5 (a) (7):	Summary of particularly significant reports	1-31
Section 5 (a) (8):	Audit reports containing questioned costs	35-36
Section 5 (a) (9):	Audit reports containing recommendations for better use of funds	36
Section 5 (a) (10):	Summary of unresolved audit reports issued prior to the beginning of this reporting period	40-42
Section 5 (a) (11):	Significant revised management decisions during this reporting period	No Activity
Section 5 (a) (12):	Significant management decisions with which the OIG disagreed during this reporting period	No Activity
Section 5 (a) (14) (A):	Peer reviews conducted by another OIG	43
Section 5 (a) (16):	Peer reviews conducted by the OPM OIG	43

OIG HOTLINE

Report Fraud, Waste or Abuse to the Inspector General

PLEASE CALL THE HOTLINE:

202-606-2423

TOLL-FREE HOTLINE:

877-499-7295

Caller can remain anonymous • Information is confidential

http://www.opm.gov/oig/html/hotline.asp

MAILING ADDRESS:

Office of the Inspector General

U.S. OFFICE OF PERSONNEL MANAGEMENT

Theodore Roosevelt Building
1900 E Street, N.W.
Room 6400
Washington, DC 20415-1100

VISIT US ON THE WEB AT: **www.opm.gov/oig**

For additional information
or copies of this publication, please contact:

OFFICE OF THE INSPECTOR GENERAL
United States Office of Personnel Management

Theodore Roosevelt Building
1900 E Street, N.W., Room 6400
Washington, DC 20415-1100

Telephone: (202) 606-1200
Fax: (202) 606-2153

SEPTEMBER 2015 **OIG-SAR-52**