FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

MEMORANDUM

November 28, 2012

To: **Committee on Energy and Commerce Democratic Members and Staff**

From: **Committee on Energy and Commerce Democratic Staff**

Re: **Hearing on "Examining Options to Combat Health Care Waste, Fraud, and Abuse"**

On Wednesday, November 28, 2012, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Health of the Committee on Energy and Commerce will hold a hearing entitled, "Examining Options to Combat Health Care Waste, Fraud, and Abuse."

I. WITNESS LIST

Mr. Neville Patterson
Senior Vice President Government Affairs, Standards and Business Development
Gemalto, Inc.
on behalf of the Secure ID Coalition

Mr. Dan Olson
Director of Fraud Prevention
Health Information Designs

Ms. Alanna Lavelle
Director Investigations, East Region/Special Investigations Unit
Wellpoint

Mr. Michael Tezrich
Senior Vice President, Global Sales and Marketing
Zebra Technologies

Mr. Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association

II. FRAUD IN MEDICARE

Health care fraud impacts private health care providers and government health care programs such as Medicare, costs enormous sums, and potentially affects the medical care received by millions of patients. While estimates of the total cost of health care fraud are difficult to obtain, the National Health Care Anti-Fraud Association has estimated that all health care fraud – affecting private health insurers, Medicare, Medicaid, and other government programs – costs patients, taxpayers, and health care providers tens of billions of dollars annually.[1] There are no precise measures of the cost of health care fraud to the Medicare program specifically, but Medicare is a frequent fraud target, in part because "consumers are more susceptible to fraud if they are older and/or poor."[2]

Fraud in Medicare is not synonymous with the "improper payments" or "payment errors" made by these programs. In 2009, the government paid approximately $65 billion in Medicare and Medicaid payments classified as "improper."[3] The vast majority of payments classified as improper stemmed from inadvertent errors, such as illegible doctors' signatures, incomplete paperwork, or provision of legitimate care in the wrong sort of facility, and do not represent overpayments or payments for unnecessary care.[4] Recent increases in the reported improper payment rate are not necessarily evidence of increased fraud; they appear to be artifacts of changes in reporting methodology rather than indicators of actual increases in fraud or improper payments.[5]

Health care fraud schemes can take a variety of different forms: billing for services that were never provided, misreporting costs in order to increase payments, stealing providers or beneficiaries' identities, or paying kickbacks to physicians or other health care providers. Perpetrators of fraud run the gamut from street corner criminals trafficking in illegally obtained

[1] National Health Care Anti-Fraud Association, *The Problem of Health Care Fraud* (2010) (online at http://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-problem-of-health-care-fraud.aspx) (accessed Nov. 20, 2012).

[2] S. Rosenbaum et al., *Health Care Fraud*, The George Washington University School of Public Health and Health Services (Oct. 27, 2009) (online at http://sphhs.gwu.edu/departments/healthpolicy/dhp_publications/pub_uploads/dhpPublication_924894E4-5056-9D20-3DA16EE2DF2E2336.pdf).

[3] Payment Accuracy, *High Error Programs* (2010) (online at http://paymentaccuracy.gov/content/high-priority-programs) (accessed Nov. 20, 2012).

[4] Centers for Medicare & Medicaid Services, *Improper Medicare Fee-For Service Payment Report* (November 2009) (online at https://www.cms.gov/apps/er_report/preview_er_report_print.asp?from=public&which=long&reportID=15) (accessed Nov. 20, 2012).

[5] S. Rosenbaum et al., *Health Care Fraud*, The George Washington University School of Public Health and Health Services (Oct. 27, 2009) (online at http://sphhs.gwu.edu/departments/healthpolicy/dhp_publications/pub_uploads/dhpPublication_924894E4-5056-9D20-3DA16EE2DF2E2336.pdf).

drugs to large health care providers and multinational drug manufacturers inflating costs or taking kickbacks. In recent years, CMS has identified durable medical equipment and home health care as areas "highly vulnerable to waste, fraud, and abuse."[6]

The variety in different types of fraud makes it likely that no one solution will be the cure-all for eliminating fraud. Different solutions will be needed to address the various aspects of fraudulent activities.

According to the Government Accountability Office (GAO), in 2010, 10,187 subjects were investigated for health care fraud (7,848 criminal cases and 2,339 civil cases). Approximately 49 percent of criminal fraud subjects were affiliated with medical facilities (medical practices, clinics, centers), durable medical equipment suppliers, or home health agencies. Hospitals and medical facilities were the most common subjects of civil cases. More than 2,000 providers were excluded from participation in federal health care programs in 2010, the majority (60%) were nurses or nurse aides, and the next largest block was pharmacies or individuals associated with pharmacies (7%).[7]

Every year, GAO issues a report identifying government operations that are particularly vulnerable to fraud, waste, abuse, and mismanagement or that need transformation to address deficiencies in efficiency or effectiveness. This "High-Risk Report" has included Medicare since 1990 and Medicaid since 2003. In its most recent testimony on the High-Risk Report, GAO noted Medicare's size, complexity, and susceptibility to improper payments as reasons for its placement on the list.[8]

III. ADMINISTRATION EFFORTS TO COMBAT HEALTH CARE FRAUD

The Health Care Fraud and Abuse Control Program (HCFAC), established under the Health Insurance Portability and Accountability Act of 1996, is the primary funding source and coordinating authority for federal and state efforts to fight health care fraud. Total HCFAC mandatory and discretionary funding has increased in recent years, from $1.13 billion in FY 2008, to $1.36 billion in FY 2009, then to $1.48 billion in FY 2010, and an estimated $1.7 billion in FY 2011. Under HCFAC, the Center for Program Integrity within CMS (which includes the Medicare and Medicaid Integrity Programs), the Department of Health and Human Services (HHS), the Office of the Inspector General (OIG) the Department of Justice (DOJ), and state Medicaid programs share responsibility for preventing and detecting fraud, investigating and trying civil and criminal cases, and taking other actions to enforce anti-fraud provisions.

[6] House Committee on Ways and Means, Subcommittee on Health and Subcommittee on Oversight, Testimony of CMS Director, Program Integrity Group, Kimberly L. Brandt, *Hearing on Reducing Fraud, Waste, and Abuse in Medicare* (June 15, 2010).

[7] Government Accountability Office, *Health Care Fraud, Types of Providers Involved in Medicare, Medicaid, and the Children's Health Insurance Program Cases* (September 2012) (GAO-12-820).

[8] House Committee on Oversight and Government Reform, Testimony of Comptroller General Gene L. Dodaro, *Hearing on GAO's 2011 High-Risk Series: An Update* (Feb. 17, 2011).

Enforcement tools available to these entities include civil monetary penalties, criminal penalties, and exclusion from participation in federal health care programs.

Spending to prevent health care fraud results in a significant positive return-on-investment. In conjunction with DOJ, HHS has taken aggressive steps to respond to and reduce Medicare and Medicaid fraud since President Obama took office. In May 2009, HHS and DOJ announced the creation of the Health Care Fraud Prevention and Enforcement Team (HEAT), designed to coordinate Cabinet-level agency activities to reduce fraud. In January 2010, HHS and DOJ held the first "National Summit on Health Care Fraud" to bring together public- and private-sector experts to identify and discuss ways to investigate and eliminate health care fraud. And in April 2010, CMS established the Center for Program Integrity, consolidating the agency's Medicare and Medicaid anti-fraud activities in an effort to improve coordination between the two programs and with other agencies at the state and local level.

Under the HEAT program, HHS and DOJ have expanded the use of dedicated strike force teams, placing law enforcement personnel in locations that are identified as health care fraud hotspots. Strike force teams are presently active in South Florida, Los Angeles, Houston, Brooklyn, Baton Rouge, Detroit, Chicago, Dallas, and Tampa. Most recently, in October 2012, Medicare Fraud Strike Force operations in seven cities led to charges against 91 individuals – including doctors, nurses and other licensed medical professionals – for their alleged participation in Medicare fraud schemes involving approximately $432 million in false billing. That total includes more than $230 million in home health care fraud; more than $100 million in community mental health care fraud and more than $49 million in ambulance transportation fraud.[9]

In addition to standard program integrity activities, CMS has taken targeted action in the Durable Medical Equipment (DME) market and undertaken education efforts with seniors, who are particularly susceptible to fraud. In 2009, CMS established new enrollment, accreditation, and surety bond requirements for DME providers and expanded the use of unscheduled site inspections at DME facilities. In the summer of 2010, CMS partnered with HHS's Administration on Aging in a national fraud prevention campaign that included radio, television, and print advertising and outreach efforts. As part of that initiative, all Medicare beneficiaries received a mailer advising them on how to protect themselves against identity theft and fraud.

In FY 2011, the Health Care Fraud and Abuse Control Program (HCFAC) recovered nearly $4.1 billion in taxpayer dollars. This is the highest annual amount ever recovered from individuals and companies who attempted to defraud seniors and taxpayers or who sought

[9] HealthCare.Gov, *New Tools to Fight Fraud, Strengthen Federal and Private Health Programs, and Protect Consumer and Taxpayer Dollars* (2011) (online at http://www.healthcare.gov/news/factsheets/2011/03/fraud03152011a.html) (accessed Nov. 20, 2012).

payments to which they were not entitled. The 3-year average Return on Investment (ROI) for the HCFAC program is $7.2 to $1.0, meaning that $7.2 is returned for every dollar spent.[10]

In FY 2012, the HCFAC program received $309.8 million in discretionary funding to expand program integrity activities at CMS, DOJ, and HHS. The Administration has requested an additional $610 million in FY 2013 to expand work on preventing fraud and improper payments before they occur as well as supporting Health Care Fraud Prevention and Enforcement Action Team activities.[11]

The FY 2013 House Labor, Health and Human Services, and Education appropriations bill provides $308.9 million in discretionary funding for the HCFAC program. The FY Senate 2013 Labor, Health and Human Services, and Education House appropriations bill provides $610 million in discretionary funding for the HCFAC program.[12]

IV. THE AFFORDABLE CARE ACT'S NEW TOOLS TO REDUCE MEDICARE AND MEDICAID FRAUD AND ABUSE

The *Affordable Care Act (ACA)*[13] contains over 30 provisions to help CMS, HHS OIG, and DOJ reduce Medicare and Medicaid fraud.[14] The most important provisions involve a shift from the traditional "pay and chase" approach to fraud reduction to a preventive approach, keeping fraudulent suppliers out of the program before they can commit fraud. The Congressional Budget Office (CBO) estimates that these provisions will save taxpayers over $7 billion dollars over the next decade.[15]

A. Key *Affordable Care Act* Anti-Fraud Provisions

- **New tools to prevent fraudulent providers from enrolling in or taking advantage of Medicare and Medicaid.** The *ACA* contains new enrollment requirements for all providers, allowing CMS to identify and eliminate fraudulent providers before they can receive payment from Medicare and Medicaid. The new enrollment process allows for enhanced background checks for providers, new disclosure requirements, and on-site visits to verify provider information. Providers must also create internal compliance programs. CMS may enact moratoria on enrolling new providers if the Secretary believes that such enrollments will increase fraud risks, may conduct enhanced oversight of new providers once they have enrolled in Medicare and Medicaid, and may suspend

[10] The Department of Health and Human Services and the Department of Justice, *Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2011* (February 2012).

[11] Office of Management and Budget, *Fiscal Year 2013 Budget of the U.S. Government* (online at http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/budget.pdf).

[12] S. 3295, H.R. 3070.

[13] *ACA* is comprised of two public laws, P.L. 111-148 and P.L. 111-152.

[14] *ACA* Sections 6401-6411.

[15] Letter from Congressional Budget Office Director Douglas W. Elmendorf to Speaker Nancy Pelosi (Mar. 20, 2010).

payments to providers in cases where there is a substantiated fraud allegation against the provider.

- **Fighting fraud in DME and home health care.** The *ACA* contains several additional provisions specifically designed to fight fraud in the high-risk DME and home health programs. After July 1, 2010, physicians who order Medicare DME and home health care services are required to be enrolled in the Medicare program. Physicians are also required to maintain access to and provide upon request documentation on orders for DME and home health care services, and are required to have a face-to-face encounter with the individual prior to issuing a certification or re-certification for DME or home health services.

- **New and enhanced penalties for fraudulent providers.** The *ACA* provisions add new civil monetary penalties for individuals who fail to grant timely access to information required for audits or investigation, individuals who have been excluded from Federal health care programs who order or prescribe services provided by that program, individuals who make false statements on enrollment applications or bids, and individuals who know of, but do not return overpayments from Medicare and Medicaid. New provisions also allow the Inspector General to exclude from Medicare and Medicaid any provider that makes false statements on an application to enroll or participate in these programs, and impose new sanctions on Medicare Advantage or Part D plans that falsify information or fail to comply with marketing requirements.

- **New data sharing and data-collection provisions.** The *ACA* requires the HHS Secretary to maintain a national health care fraud and abuse database to retain information on any adverse actions taken against health care providers, requires enhanced data sharing between CMS, States, and other federal health care programs, and provides additional access to new and existing databases for DOJ, the Inspector General, and States.

- **New funding to fight Medicare and Medicaid fraud.** The *ACA* significantly increases funding for the HCFAC Fund, indexing the program’s mandatory baseline and funding for the Medicare and Medicaid Integrity Programs to increase at the same rate as the CPI, and providing additional mandatory HCFAC funding of $105 million in FY 2011, $65 million in FY 2012, $40 million in FY 2013 and 2014, $20 million in FY 2015 and 2016, and $10 million in FY 2017-2020. Overall, the Affordable Care Act provides an estimated $500 million in increased mandatory funding to fight fraud.

The Administration has rapidly implemented these provisions. In May 2010, CMS issued interim final rules requiring ordering and referring physicians of certain medical supplies and services to be enrolled in Medicare, and establishing new documentation requirements for high-risk programs. On November 17, 2010, CMS issued final rules requiring face-to-face encounters for home health and hospice referrals. And on January 24, 2011, CMS issued final rules implementing the provider and supplier screening requirements, enrollment moratoria, and payment suspensions.

V. FRAUD PREVENTION SYSTEM AND AUTOMATED PROVIDER SCREENING

On June 30, 2011, the Administration implemented the Fraud Prevention System (FPS) which monitors all 4.5 million claims (Medicare Part A, Medicare Part B and DME) each day using a variety of analytic models. The FPS generates a system of alerts consolidated regarding potentially problematic providers and prioritizes the cases based on risk. The daily results are provided in real-time to CMS' Zone Program Integrity Contractor (ZPIC) analysts and investigators. The results are also available to CMS and law enforcement partners. This program integrates predictive modeling as part of an end-to-end solution that triggers effective, timely administrative actions, minimizes false positives and sets priorities based on risk to the program. In addition to the FPS claims-based analysis, CMS has strengthened provider screening and enrollment with deployment of a new Automated Provider Screening (APS) system. The new process integrates all providers into the same database, with reliable, up-to-date information, checking medical identities against the Compromised Numbers database, address against valid location databases, and other databases that cover issues such as revocations, exclusions, felony convictions. This database assesses risk scores on provider enrollment for follow-up activity.[16]

Since March 2011, CMS enrolled or revalidated enrollment information for nearly 410,000 Medicare providers and suppliers under the enhanced screening requirements of the *ACA*. As a result of revalidation and other proactive initiatives, CMS has deactivated 136,682 enrollments and revoked 12,447 enrollments. These efforts will ensure that only qualified and legitimate providers and suppliers can provide health care items and services to Medicare beneficiaries.[17]

VI. NEXT STEPS IN FRAUD FIGHTING

This hearing will focus on what more can be done to fight fraud in Medicare. The anti-fraud activities and technology adopted will need to consider the various types of fraud and solutions specific to address those.

- **Provider Screening**. CMS has already implemented an extensive new provider screening program called the Automated Provider Screening program. This program has to date yielded considerable results in weeding out bad actors. Robust provider screening is critical to help keep bad actors from enrolling to bill Medicare in the first place. Additional provider screening activities should be balanced against the prospect of creating barriers to enrollment or excessive bureaucracy for legitimate providers. Much

[16] Peter Budetti, *CMS' Innovative Approach to Program Integrity*, Centers for Medicare & Medicaid Services (Mar. 5, 2012) (online at http://www.allhealth.org/briefingmaterials/Budetti3-05-12(Alliance)SlidesforWebsite-2220.pdf).

[17] HealthCare.gov, *New Tools to Fight Fraud, Strengthen Federal and Private Health Programs, and Protect Consumer and Taxpayer Dollars* (2011) (online at http://www.healthcare.gov/news/factsheets/2011/03/fraud03152011a.html) (accessed Nov. 20, 2012).

of the new screening process CMS has implemented relies on checking databases that is invisible to the provider.

- **Compromised Number Checklist (CNC).** In January 2010, CMS released its first national database of compromised Medicare beneficiary and provider ID numbers called the Compromised Number Checklist (CNC). The purpose of the CNC is to share compromised ID numbers and any associated corrective actions that have been taken. CMS continues to leverage this national CNC database to enhance efforts detecting and preventing fraud and abuse in Medicare. In 2011, the CNC identified approximately 5,000 compromised providers and suppliers and approximately 280,000 beneficiaries whose Health Insurance Claim Number (HICN) is known or strongly suspected to have been compromised. The CNC also utilizes “geomapping” analyses to identify clustering of compromised numbers, which is valuable in the development of new investigations.

- **Claims Edits.** CMS has implemented approximately 30,000 claims edits to screen Medicare claims for potential fraud or inappropriate billing, for example a medically improbably event. These edits are automated and can eject a claim from the processing system for fraud or other error in billing.

- **Prior Authorization.** Under a current demonstration, CMS has implemented a prior authorization program for all power mobility devices, including wheelchairs, an item of durable medical equipment prone to fraud and errors. Other payers have implemented prior authorization programs for other select services that are high cost or prone to abuse, such as prescription drugs, radiology services, or physical therapy. Expansion of prior authorization must be balanced with maintaining timely beneficiary access to services and provider burden.

- **Prepayment Review.** CMS is currently conducting a demonstration that will allow Medicare Recovery Auditors (RACs) to review claims before they are paid to ensure that the hospital complied with all Medicare payment rules. The RACs will conduct prepayment reviews on certain types of claims that historically result in high rates of improper payments. These reviews will focus on seven states with high populations of fraud- and error-prone providers (Florida, California, Michigan, Texas, New York, Louisiana, and Illinois) and four states with high claims volumes of short inpatient hospital stays (Pennsylvania, Ohio, North Carolina, Missouri) for a total of 11 states. This demonstration will also help lower the error rate by preventing improper payments rather than the traditional "pay and chase" methods of looking for improper payments after they occur. This demonstration began on August 27, 2012.

- **Lock-In/Restrictive User Programs.** CMS currently does not use any beneficiary lock-in programs in Medicare, however such programs are employed by state Medicaid programs, particularly to address prescription drug abuse. Current CMS Medicare Part D guidance prohibits plans from locking beneficiaries into particular pharmacy providers or prescribers, however plans can use case management, drug utilization review, as well as claims data analysis to identify aberrant behavior on the part of prescribers and beneficiaries. A number of private sector insurers, however, currently use these lock-in programs to restrict access to controlled substances, prevent doctor or pharmacy shopping and attempt to reduce fraud and abuse.

- **Predictive Analytics.** Predictive analytics is the use of a variety of statistical techniques such as modeling and data mining to analyze current and historical information to identify risks and patterns and predict behavior. CMS implemented a predictive analytics claims review system starting in June 2011. FPS applies predictive analytic technology to claims prior to payment to identify aberrant and suspicious billing patterns. Leveraging leads from FPS, CMS and its contractors review claims before payment, and trigger administrative actions and law enforcement referrals. Early results from the Fraud Prevention System show significant promise and the system will mature over time. In its first year of implementation, the FPS generated leads for 538 new fraud investigations, provided new information for 511 existing investigations, and triggered 617 provider interviews and 1,642 beneficiary interviews.

- **Smart Cards.** Smart Cards are credit card-like cards that contain a computer chip with varying types of data. A number of companies that manufacture smart cards or smart card readers have proposed providing Medicare beneficiaries and providers with these credit card type devices to verify identity at the point of care.

Currently, there are no major private insurers in the United States that issue smart cards to all enrollees. A handful of Medicaid programs piloted smart cards, but to date, none have wound up adopting them widespread and most have ceased their pilots. According to a recent paper on state Smart Card initiatives, "Past experience has shown that verification programs in government benefits do not effectively reduce fraud or save state resources, but rather serve as a barrier to enrollment into these programs."[18]

While smart cards can help address the issue of an individual misrepresenting himself to receive services or to bill for services, this represents only a small universe of fraud. It is unclear (or potentially unlikely) that a smart card would address fraud issues of sham storefronts (only onsite visits can identify these), up-coding, billing for services that weren't actually provided, or fraud where the provider and the beneficiary are together complicit in the fraudulent activity.

The question of the cost to implement such a card is also an open question. While there are the obvious up front and ongoing costs of issuing cards to 46 million Medicare beneficiaries and more than one million Medicare providers (not including additional hospitals, clinics and other provider types and the fact that each provider would likely need more than one card reader), there are additional costs that have not been explored, for example the necessary systems changes to allow Medicare claims processors to receive transmissions from smart card reader

[18] National Health Law Program, *Fact Sheet: Biometric Smart Cards in Medicaid: Barrier to Coverage and Ineffective at Reducing Fraud* (2012) (Feb. 1, 2012) (online at http://files.www.enrollamerica.org/best-practices-institute/publications-and-resources/2012/biometric-smart-cards-in-medicaid-barrier-to-coverage-and-ineffective-at-reducing-fraud/Medicaid_Biometric_Smart_Cards.pdf)

terminals as well as how such a smart card "transaction" would interface with the CMS system (would it be filed on a claim, would it be something separate claims processors had to track down to integrate with the claim submission, etc).

While smart cards may address one aspect of the fraud landscape, employing smart cards creates additional opportunities for fraud schemes to simply migrate. Smart cards are generally recognized as quite secure, however they are not 100% foolproof. Viruses attacking smart card readers infiltrated the Department of Defense Common Access Card system this past year. Entrepreneurial criminals have developed counterfeit card readers or viruses that can be attached to the card reader to skim data. Hackers have already developed methods to take the computer chips out of the card to scan the data on the chip. Evidence from France and Taiwan indicate that fraud in those health systems, which rely on smart cards for beneficiaries has not been eliminated.

There are also questions of how such a smart card would integrate into the health care work flow. What happens if a beneficiary shows up without a card; is care withheld? Given that most providers do not personally submit claims to Medicare, how much of the provider's time would be taken up by now administering the billing process with their card? Would the provider have to carry the card reader from room to room or walk the patient down to the billing office to complete the transaction of inserting provider and patient cards into the card reader at the same time? If beneficiary pictures were placed on cards, how would CMS obtain pictures of all 46 million Medicare beneficiaries? How often would pictures have to be updated?

Finally, as technology is rapidly evolving, policy makers should explore what other technologies might accomplish the same or better results for equal or lesser costs. Given the rapid deployment of smart phones – even in the aged population – options for development of secure apps that could be integrated on smart phones might be another option worthy of exploration. The anti-fraud landscape is constantly changing and as new technologies emerge, new schemes emerge to thwart detection. Locking Medicare into one type of technology and hardware (smart cards and readers) would commit Medicare to the expense of continual updating of cards, card readers, and systems to accommodate on mode of technology might turn out to be a significant financial drain on the program – to date no independent analyses have been conducted on this matter and to date, no independent calculation of return on investment has been done.

VII. CONCLUSION

Waste, fraud, and abuse drain resources and undermine care throughout the health care system. The Administration has taken significant steps to combat fraud in Medicare and Medicaid, and is seeing results from these ramped up efforts. The *ACA* added new tools to the fight against fraud in Medicare and Medicaid, and repeal or defunding the law would prevent the government from using this significantly expanded anti-fraud authority. As Congress explores new options for adding to the CMS arsenal of fraud fighting techniques, a thorough exploration of all technologies, and the various kinds of fraud each can detect or prevent is essential – as well as a cost-benefit analysis to ensure Medicare dollars are being spent wisely.