RPTS MCCONNELL

DCMN HOFSTAD

This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.

EXAMINING OPTIONS TO COMBAT HEALTHCARE

WASTE, FRAUD, AND ABUSE

WEDNESDAY, NOVEMBER 28, 2012

House of Representatives,

Subcommittee on Health,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 2123, Rayburn House Office Building, Hon. Joseph R. Pitts [chairman of the subcommittee] presiding.

Present: Representatives Pitts, Burgess, Shimkus, Blackburn, Gingrey, Latta, Lance, Cassidy, Barton, Pallone, Engel, Schakowsky, and Waxman (ex officio).

Also Present: Representatives McKinley and Christensen.

Staff Present: Matt Bravo, Professional Staff Member; Paul Edattel, Professional Staff Member, Health; Julie Goon, Health Policy

Advisor; Sean Hayes, Counsel, O&I; Robert Horne, Professional Staff Member, Health; Ryan Long, Chief Counsel, Health; Carly McWilliams, Legislative Clerk; John O'Shea, Policy Advisor, Health; Monica Popp, Professional Staff Member, Health; Chris Sarley, Policy Coordinator, Environment and Economy; Heidi Stirrup, Health Policy Coordinator; Alli Corr, Minority Policy Analyst; Amy Hall, Minority Senior Professional Staff Member; Elizabeth Letter, Minority Assistant Press Secretary; and Karen Nelson, Minority Deputy Committee Staff Director for Health.

Mr. Pitts. The subcommittee will come to order.

The chair recognizes himself for 5 minutes for an opening statement.

In May of this year, the Department of Justice brought charges against 107 individuals who bilked Medicare for over $452 million. Just seven individuals in Louisiana were responsible for over $225 million of this fraud.

In a separate case in February, a single Dallas doctor was arrested for making $350 million in false claims. In February of 2011, 114 individuals who had bilked over $240 million were arrested in another crackdown.

All told, that billion dollars in improper payments represents less than 2 percent of the estimated $60 billion annually lost to waste, fraud, and abuse.

As bad as that number is on its own, I want to put it into context. The Medicare program is running out of money. The CMS actuary predicts the program could be insolvent in just 5 years. As the Congressional Research Service wrote in a June 2011 report, quote, "As long as the Medicare trust fund has a balance, the Treasury Department is authorized to make payments on behalf of seniors."

However, the report continues, quote, "There are no provisions in the Social Security Act that govern what would happen if insolvency were to occur," end quote. The report contends that when insolvency of the Medicare program happens, quote, "There would be insufficient funds to pay for all Part A reimbursements to providers," end quote.

If Congress and the President support the idea that seniors should depend on the Medicare program to pay their provider bills, reform of the program through legislative action will be needed. The Medicare trustees in their 2011 report to Congress have already stated as much. One area of reform that I hope we can tackle in a bipartisan way is the area of fraud and abuse in the Medicare program.

The Federal Government has made strides recently to improve catching fraudulent providers and beneficiaries, and I commend them for their efforts. However, at the same time, they have largely failed to implement mechanisms that would prevent fraudulent payments from being made in the first place. Prosecuting offenders does not get all the money that they stole.

One such area is predictive analytics. CMS implemented the fraud prevention system in July of 2011 to analyze Medicare claims data using models of fraudulent behavior after such a system was shown to work well in the private industry. However, while the current system can draw on a host of data sources in support of its efforts, the system has not yet been integrated with the agency's payment processing system to allow for the prevention of payments until suspicious claims can be determined to be fraudulent.

Further, a recent GAO report stated that CMS has failed to define an approach for even measuring whether the current system is helping to prevent fraudulent billing. It is my firm belief that greater transparency from CMS with regard to current fraud programs is needed if we hope to build upon what is currently being done to make the program

more secure.

Our Nation's seniors are counting on us to ensure that Medicare fulfills its promises. We can do that in part by making sure their premium dollars are managed wisely and not lost to con artists.

Our hearing today will discuss the efforts Medicare has undertaken currently to prevent fraud in government programs. In addition, the panel has generously offered us their time and expertise to explore emerging technologies and mechanisms that might help improve those efforts.

I want to thank all of our witnesses for sharing their thoughts with us today. And I am confident that these ideas can help generate a bipartisan effort to improve the solvency of the Medicare program in the coming Congress.

The chair now recognize the ranking member of the Subcommittee on Health, Mr. Pallone, for 5 minutes.

[The prepared statement of Mr. Pitts follows:]

******** COMMITTEE INSERT ********

Mr. Pallone. Thank you, Mr. Chairman.

And good morning to everyone. It is good to be back after the election and seeing that our subcommittee is having hearings and moving forward in the lame duck as well as for next year.

While the total cost of healthcare fraud is difficult to obtain, estimates range anywhere from $65 billion to $98 billion annually. For every dollar put into the pockets of criminals, a dollar is taken out of the system to provide much-needed care to millions of seniors.

Fraud schemes come in all shapes and sizes and affect all kinds of insurance, public and private alike. Whether it is a sham storefront posing as a legitimate provider or legitimate businesses billing for services that were never provided, it is all the same result: undermining the integrity of our public health system and driving up healthcare costs.

I think we can all agree that healthcare fraud is a serious longstanding problem that will take aggressive long-term solutions to reverse. And we made a strong commitment to combat these issues within the Affordable Care Act. The law contains over 30 antifraud provisions to assist CMS, the OIG, and the Justice Department in identifying abusive suppliers and fraudulent billing practices. These include enhanced background checks, new disclosure requirements, onsite visits to verify provider information, and a requirement that healthcare providers create their own internal compliance programs.

The most important provisions in the Affordable Care Act change the way we fight fraud by heading up the bad actors before they strike

and thwarting their enrollment into these Federal programs in the first place. And this way, we aren't just left chasing a payment once the money is already out the door.

And I am encouraged by the work that has been done of late. Over the past 3 years, the government has recovered a record-breaking $10.7 billion of healthcare fraud. So I am confident that we will begin to see even more savings as the implementation of these programs continues.

But our efforts must not stop there. Fraud is ever-changing; criminals will always find loopholes. And it is our job to keep one step ahead of them. Today we are going to hear from an array of witnesses about the state of antifraud measures currently being used, as well as discussing new approaches.

One example of a new approach is the secure ID program, which would create identification cards with encrypted chips. Each Medicare provider and beneficiary would be required to swipe these cards at the point of service.

And while there may be some benefits to this technology, such as preventing identity theft, I do have questions about how this would affect the overall system. Most important to me is how such a program would affect patients' access to care. For example, what happens if a senior simply forgets his ID card? Will he be sent away? I am also interested in how this technology can prevent the sheer criminals colluding with beneficiaries and handing out kickbacks.

And as we discuss any potential pilot programs, we must ensure

that we can evaluate different technologies that allow us to determine what provides the best value for our tax dollars.

So, Mr. Chairman, as Congress discusses the expiring tax policies and impending sequestration during the lame duck, I do not believe we need to decrease benefits to seniors or raise the eligibility age to further fortify the program. Instead, we should focus on building upon the reforms of the ACA and creating better efficiencies within the system, including innovative ways to combat fraud and waste.

Standing up to protect Medicare includes supporting the constant work that must be done to cut waste, fraud, and abuse. And I am committed to working with my colleagues now and in the future to help address this ongoing threat. So I do appreciate your having this committee hearing today because I think it addresses a very important issue, both now and in the future, in the next Congress as well.

I did want, Mr. Chairman, if I could, to ask unanimous consent to insert two pieces of testimony in the record. The first is from the American Medical Association, which I believe raises some very important questions about smart cards. At a minimum, further discussion with a more robust representation of interested parties would seem to be warranted on that issue.

And the second is a statement from the national Health Law Program, which discusses smart cards in the Medicaid context and raises concerns about whether these cards could serve as a barrier to timely patient care.

So I would ask unanimous consent. I think you have both of them.

Mr. Pitts. Yes. Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Pallone. Thank you. And I yield back.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. The chair thanks the gentleman and now recognizes the vice chairman of the subcommittee, Dr. Burgess, for 5 minutes.

Dr. Burgess. And I thank the chairman for the recognition and the time.

We all know that the Centers for Medicare and Medicaid Services has not done enough to address the issue of inappropriate payments even though our government-administered health system does appear to waste billions of dollars every year. Eliminating inappropriate payments, payments that, in fact, embarrassingly hemorrhage from the programs, is, as Mr. Pallone pointed out, a bipartisan issue.

Unfortunately, there is no simple answer. Fraud analysts are estimating up to 10 cents out of every dollar that is spent in health care is lost yearly to fraud. That is 10 cents out of every dollar we are spending. One-fifth of all healthcare expenditures in this country are spent on the Medicare system. So that is a big figure, a big dollar figure, that demands our attention. We could pay for everything we need to pay for, the doc fix, in this decade and the next decade if we simply fixed that problem.

We do pay providers in practically an automatic fashion. This May I asked for and received a briefing from one of the deputy administrators at CMS, who is the Director for Center Program Integrity, and talked about their efforts to move from a pay-and-chase mindset into one that builds on a system of predictive modeling.

Now, the good news is that things do seem to be moving forward in that arena. They started with 9 algorithms and quickly grew to over

30. And that was last May, so I don't know what that figure stands at today. But it is clearly an area that is crying to be taken care of.

They are some first steps, but they are not going nearly far enough. Had we addressed these technologies years ago, just think about the amount of money that could have been saved and how many generations of algorithms and new generations of algorithms that could now be in place.

As a physician, I support prompt pay, and I realize the size, scope, and complexity of the Medicare program makes it highly susceptible to inappropriate payments. We have to accelerate the use of these analytics to aid in our detection efforts. But, you know, it is not new concepts. The Visa folks do this every hour of every day of every week and will call you when there is untoward activity occurring on your credit or debit card and are pretty quick to do so. Unfortunately, in our Federal agencies, anything we do cannot be defined as "quick."

We have learned from watching some of the predictive modeling activities in the crop insurance program that, simply recognizing that there is a cop on the beat, people are less likely to misbehave. Right now we have whole industries -- illicit industries, crooked industries -- that are being built around the fact that we just simply make so much money available to them, they can hardly resist the temptation to cheat.

Back-end investigations will remain a part of what CMS is required

to do. We need to be sure that we have the prosecutorial force to be able to go -- when these individuals are uncovered, to make certain that we can go after them with the full force of the law.

The Government Accountability Office has made recommendations, some of which date back to a decade when I first started in Congress, and many of those have yet to be implemented. And we need to pay attention to what they tell us this morning.

Developing new and innovative approaches to fight fraud has become increasingly important. I certainly look forward -- we have a very -- a panel in front of us today that has vast experience, and I expect that they can give us a great deal of enlightenment.

And with that, I do want to yield to my colleague from Georgia, Dr. Gingrey.

[The prepared statement of Dr. Burgess follows:]

******** COMMITTEE INSERT ********

Dr. Gingrey. I thank Dr. Burgess for yielding to me.

Mr. Chairman, it is appropriate that we as a committee look at the various tools for fixing the Medicare program. Strategically, identifying fraud, waste, and abuse is essential to trying to solve and to save this program that so heavily benefits our seniors.

Let's face it, Medicare will go bankrupt, depending on who you talk to, between 2017 and 2024. At this point, we must seek to identify waste and eliminate it -- an estimated, what is it, anywhere from $60 billion to $90 billion a year. And this money should be used to preserve Medicare and not pad the wallets of criminals.

We need to ensure that the agencies are all using all of the powers they already have at their disposal to save wasted money. I would hope that we can eventually take a proactive approach in identifying criminals, one where we eliminate the payment before it is made rather than chase them afterwards. This is a huge problem. And I think that every one of us are appalled, especially those of us who are healthcare providers, who have worked in that field, as Dr. Burgess and myself, for years, trying to do the right thing, and knowing that people are stealing money from those who really, really need it.

So I am glad, Mr. Chairman -- thank you for having the hearing. And I look forward to hearing from the witnesses.

And I yield back. Thank you, Dr. Burgess.

[The prepared statement of Dr. Gingrey follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. The chair thanks the gentleman and now recognizes the ranking member of the full committee, Mr. Waxman, for 5 minutes for an opening statement.

Mr. Waxman. Thank you, Mr. Chairman, for recognizing me and for holding this hearing today and focusing on the important topic of Medicare and Medicaid fraud.

Healthcare fraud robs taxpayers of funds, affects the quality of care provided to program enrollees, and saps the public confidence in the program. And that is why I see fighting fraud as a critical need and an issue where we should be able to achieve bipartisan consensus.

The vast majority of Medicare and Medicaid providers are compassionate and honest. The vast majority of beneficiaries of these programs desperately need the care they provide. So we need to be tough on fraud and tough on criminals who take advantage of these programs and their beneficiaries, but we can and should not blame the victim.

One of the reasons I am so proud of the Affordable Care Act is that it contains dozens of antifraud provisions. The legislation has the most important reforms to prevent Medicare and Medicaid fraud in a generation, and already they are yielding results.

As a result of the strengthened enrollment and re-enrollment process, CMS has deactivated 136,682 provider enrollments and revoked another 12,477. The new fraud prevention system of analytics has generated numerous new leads for new and existing investigations and providers and beneficiary interviews.

The healthcare reform law shifted the prevailing

fraud-prevention philosophy from pay and chase, where law enforcement authorities only identify fraud after it happens, to inspect and prevent. But even so, the need for boots-on-the-ground investigation work will always remain.

I am proud of these efforts to reduce fraud. We are going to hear today from a number of witnesses describing additional steps and technologies CMS could take in terms of fighting fraud. I know some of today's witnesses support legislation to mandate CMS undertake a pilot project testing specific technology. If Congress is considering giving CMS additional funding to test new fraud-fighting activities, first we should give them the flexibility to test different interventions and compare the results, not mandate one very prescriptive activity.

Second, we must ensure that whatever CMS decides to test is evaluated carefully to determine which technologies provide the best value for our tax dollars. Smart cards may help address the problem of identity theft; however, reducing identity theft will not eliminate fraud, and smart cards may not be the only way to address issues of identity verification. In fact, both the American Medical Association, representing our Nation's physicians, and the national Health Law Program, representing low-income beneficiary advocates, raise some important issues for policymakers to consider with respect to these cards.

I am glad the committee is continuing the dialogue on reducing fraud in the Medicare program. If we truly care about protecting the

taxpayer, we should build upon the administration's initiatives to reduce Medicare fraud. I hope that we can work across the aisle to do just that.

Thank you, Mr. Chairman. I yield back my time.

Mr. Pitts. The chair thanks the gentleman.

[The prepared statement of Mr. Waxman follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. That concludes our opening statements from Members.

Dr. Burgess. Mr. Chairman?

Mr. Pitts. Yes?

Dr. Burgess. If I could ask unanimous consent, I have a letter here from Mr. Roskam describing a bill that he and Mr. Carney have introduced on provider identity protection, and I would like to submit that for the record.

Mr. Pitts. Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. Any other Members having opening statements, if you will provide them in writing, they will be made a part of record.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. Today we have one panel with seven witnesses.

Our first witness is Ms. Kathleen King, director of the Health Care team at the U.S. Government Accountability Office. Our second witness is Mr. Dan Olson, director of fraud prevention at Health Information Designs. Third, Ms. Alanna Lavelle is the director of the East Region/Special Investigations Unit at WellPoint. Our fourth witness is Louis Saccoccio, chief executive officer of the national Health Care Anti-Fraud Association; fifth, Mr. Neville Pattinson, testifying on behalf of the Secure ID Coalition; sixth, Mr. Michael Terzich, senior vice president of global sales and marketing at Zebra Technologies. And, finally, we have Dr. Kevin Fu, associate professor of computer science and engineering at the University of Massachusetts, Amherst.

We are happy to have all of you here with us today. Your written testimony will be made a part of the record. We will ask that you summarize in 5 minutes verbally your testimony before beginning questions and answers from the committee.

Ms. King, you are recognized for 5 minutes.

STATEMENTS OF KATHLEEN M. KING, DIRECTOR, HEALTH CARE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; DAN OLSON, DIRECTOR OF FRAUD PREVENTION, HEALTH INFORMATION DESIGNS; ALANNA M. LAVELLE, DIRECTOR, SPECIAL INVESTIGATIONS, WELLPOINT, INC.; LOUIS SACCOCCIO, CHIEF EXECUTIVE OFFICER, NATIONAL HEALTH CARE ANTI-FRAUD ASSOCIATION; NEVILLE PATTINSON, SENIOR VICE PRESIDENT, GEMALTO, INC., TESTIFYING ON BEHALF OF THE SECURE ID COALITION; MICHAEL H. TERZICH, SENIOR VICE PRESIDENT OF GLOBAL SALES AND MARKETING, ZEBRA TECHNOLOGIES; AND KEVIN FU, PH.D., ASSOCIATE PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MASSACHUSETTS, AMHERST

STATEMENT OF KATHLEEN M. KING

Ms. King. Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, I am pleased to be here today to discuss our work regarding Medicare fraud, including the types of providers involved in fraud and strategies we have identified that could help prevent or detect fraud.

Since 1990, we have designated Medicare as a high-risk program because its size and complexity make it vulnerable to fraud. Recently, for the first time, we were able to identify the types of providers investigated for and convicted of fraud, which should help CMS and other agencies target their efforts to prevent and reduce fraud.

In our work, we defined the subject of fraud cases as either

institutions or individuals. We found that many different types of providers were investigated for fraud. In 2010, medical facilities, such as medical centers, clinics, and practices, were the most frequent subjects of criminal fraud investigations, accounting for about a quarter of all investigations, followed by durable medical equipment suppliers, which accounted for 16 percent. Beneficiaries accounted for 3 percent of investigations.

Of these, the HHS Office of Inspector General referred about 15 percent of the subjects investigated for criminal fraud to the Department of Justice for prosecution. And in 2010, nearly 1,100 subjects were charged in criminal fraud cases. Of those charged, approximately 85 percent were found guilty, pled guilty, or pled no contest. Medical facilities and DME suppliers accounted for about 40 percent of these subjects.

With respect to civil fraud cases, about 2,300 subjects were investigated in 2010. Hospitals and other medical facilities accounted for nearly 40 percent of the subjects in the civil cases that were pursued. According to the OIG, about 40 percent of the -- I am sorry, about 50 percent of the cases were pursued, and the remaining cases were not pursued for a variety of reasons, including lack of resources and insufficient evidence.

Of the subjects pursued, about 60 percent resulted in judgments or settlements. And, again, hospitals and other medical facilities accounted for about 40 percent of the judgments. None of the subjects were beneficiaries.

Turning to strategies to reduce fraud, we have identified three, including strengthening provider enrollment processes and standards; improving pre- and post-payment review of claims; and developing processes to address identified vulnerabilities.

CMS has made progress in each of these areas through implementing provisions of the Affordable Care Act and the Small Business Jobs Act. For example, CMS now has a process in place to better screen providers before enrolling them in Medicare. And it has implemented the fraud prevention system, which detects suspicious claims before they are paid.

Still, further action is needed. We have made a number of recommendations to CMS that have not been implemented, and we continue to urge CMS to adopt them.

In addition, we have significant ongoing work designed to assist CMS in its fraud-prevention efforts. We are currently assessing the effectiveness of the prepayment edits CMS and its contractors use to ensure that Medicare claims are paid correctly the first time. We also have a study under way examining how Federal agencies are allocating funds from the Health Care Fraud and Abuse Control Program, as well as evaluating the effectiveness of those efforts. And we are also examining the effectiveness of CMS's fraud contractors, the Zone Program integrity contractors.

Preventing and reducing fraud requires constant vigilance, as a wide variety of providers are involved in fraud and those intent on committing fraud will always seek new opportunities to circumvent

program safeguards. We urge CMS to continues its efforts.

And this concludes my prepared statement. Thank you.

Mr. Pitts. The chair thanks the gentlelady.

[The prepared statement of Ms. King follows:]

******** INSERT 1-1 ********

Mr. Pitts. Mr. Olson, you are recognized for 5 minutes for an opening statement.

STATEMENT OF DAN OLSON

Mr. Olson. Thank you. Good morning, Chairman Pitts, Ranking Member Pallone, and congressional leaders. Thank you so much for the opportunity to testify on the issue of examining options to combat healthcare fraud, waste, and abuse within the Medicare and Medicaid programs.

I am Dan Olson. I am the director of fraud prevention for Health Information Designs, which is a national healthcare analytics company. I oversee our product offering for fraud called SURVEIL, and I have worked in the program integrity field for over 17 years.

Thank you for entering my full comments, as I will summarize today my testimony.

Today we recognize that healthcare fraud is indeed a criminal problem. It is multidimensional and has many facets to it. But I suggest to you today and recommend that we need a multidimensional toolset to address healthcare fraud, waste, and abuse. Within this toolset we need to have something that is dynamic in nature, nimble to change, and responsive to emerging trends.

Several items that I would suggest this morning are: the traditional business rules, which has been in place for a long time, which evaluates medical guidelines and Federal and State policy. But

to enhance this, we must have predictive models, which are using past claims and billing behaviors to forecast future actions. We must also include predictive analytics, which is developing statistical models to identify unknown data relationships. We must include link analysis, which identify relationships between providers, billing entities, and recipients, often where we can find kickbacks so they don't become so prevalent. We must also incorporate clinical decision support systems so that we no longer look at just volume-based metrics but we look at clinical guidelines to identify areas where patients are at risk for developing major medical issues.

I must caution, though, against the belief that the toolkit can stand alone because simply it cannot. The toolkit must be managed by a broad-based partnership that includes medical professionals, includes legal entities, analytical professionals, investigative entities, coding experts, statisticians, et cetera. By so doing that, we will have a toolkit that can address the multi facets of fraud, waste, and abuse.

As has been mentioned, significant progress has already been made in the healthcare world, but significant progress needs to continue to be made. Healthcare fraud is dynamic; it is not static. If we sit and do nothing or rely on what we have done in the past, we will be behind the curve. We must implement the following recommendations that I present this morning.

First, we should continue to expand the Medicare Fraud strike force at the Federal level, but not only that, we must implement it

at the State level. By implementing it at the State level -- and I would recommend that each of the regional CMS offices oversee this -- then we can improve upon and recover greater than 1 percent of the overall Medicare and Medicaid spend.

We must continue and I recommend to expand and fund the Integrated Data Repository. The singular importance of this alone can simply not be overstated. I recommend that CMS adopt a regionalized approach to this implementation that will allow for a more rapid development and will reduce the testing and training time that is needed for deployment. It is estimated that over $250 million can be accomplished in recoveries during the initial year and over $100 million in successive years.

We must also continue to expand the do-not-pay list that was originally implemented by including retired and sanctioned Drug Enforcement Agency numbers. Estimated savings: $200 million.

Finally, we must also publish national and statewide healthcare statistics. We have read time and again about something called a national healthcare fraud hotspot, where we see billings in excess of 3,000 percent or 2,000 percent. These are absurd. We need to know this. This needs to be in front of us so that we can act upon it.

In order to do this, I recommend that we establish baseline thresholds at the provider level for Medicare and Medicaid; that these threshold lists be updated regularly; and that they be published on the CMS Web site so that fraud analysts can further act on them and know what emerging trends and patterns will be.

I would be happy to expand on any of these issues that I presented

this morning. I have also included these in much more detail in the two white papers that are attached as appendices to my testimony.

I would like to thank you, Congressman Pitts, Ranking Member Pallone, and congressional leaders, for this opportunity to present. And I look forward to the question-and-answer time that will follow. Thank you.

Mr. Pitts. The chair thanks the gentleman.

[The prepared statement of Mr. Olson follows:]

******** INSERT 1-2 ********

Mr. Pitts. Ms. Lavelle, you are recognized for 5 minutes for an opening statement.

STATEMENT OF ALANNA M. LAVELLE

Ms. Lavelle. Thank you.

Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, I am Alanna Lavelle, director of special investigations for WellPoint. Thank you for the opportunity to provide our input and recommendations on detecting and deterring fraud and abuse in the healthcare system.

Healthcare fraud is not a victimless crime. We all pay, and we pay dearly. Costs extend beyond financial loss. People are harmed by wasteful, inappropriate testing and treatment.

One of the significant strengths that we and other health plans provide is the data available from our integrated healthcare benefits. This allows us the ability to see the entire healthcare spectrum and to spot trends and outliers.

We also have a dedicated fraud and abuse prevention team, known as the Special Investigations Unit, SIU. I am one of the lead investigators, and we are staffed by former Federal and State law enforcement agents and medical professionals. We also have a data analysis team.

Our goal at WellPoint is to prevent healthcare fraud and abuse for the benefit of our members' health. And in order to meet this goal,

we have developed a number of different types of programs to identify and prevent healthcare fraud and abuse, three of which I will briefly describe.

First, we have our Controlled Substance Utilization Monitoring Program and our Medicaid Restricted Recipient Program. Prescription narcotic drug abuse is a national epidemic today. Through these programs, we are helping identify those who are engaged in or contributing to prescription drug abuse and/or drug diversion.

For example, for our Medicaid plans, we have implemented a restricted recipient program in which a member who within a 3-month period visits 3 or more prescribers, 3 or more pharmacies, and fills 10 or more controlled substance prescriptions without a confirmed underlying medically necessary condition, and we lock them into using only 1 primary care physician as prescriber, 1 retail pharmacy of their choice, and 1 hospital. Our case managers work directly with providers and members. And to date, the program has saved lives and many millions of dollars in emergency department visits alone for drug-seeking behavior.

Second, we have recently contracted with a vendor to do predictive modeling at WellPoint. The program uses advanced neural network technology from FICO to identify previously unknown and emerging fraud and abuse provider and member schemes. Suspect providers and claims are reviewed to identify potential fraud, waste, or abuse and investigated thoroughly. Since we began using this tool just 6 months ago, we have opened 90 investigations and have achieved $27 million

in projected savings. The return on the investment at this time is well over 15 to 1.

And, finally, we take a multifaceted approach to identify bogus providers who do not actually perform services for real patients. Our provider database team alerts our investigators as to the presence of new claims coming in for new labs, new pharmacies, and new durable medical equipment suppliers, or DMEs. And we provide a full background check as well as a drive-by of the provider's purported office space. To date, in the State of California alone, we at WellPoint have stopped over 239 bogus DME providers before they were able to defraud us.

So based on our experience in combating healthcare fraud and abuse, we offer the following recommendations to enhance future efforts throughout all sectors of health care.

First, we are supportive of giving CMS the authority to establish a restricted recipient program in Medicare Part D for those beneficiaries displaying a pattern of misutilization.

Second, we recommend that dually eligible beneficiaries with evidence of drug-seeking behavior should be locked into one managed care plan, rather than continue to be allowed to switch plans on a monthly basis to evade detection.

Third, we support better coordination and cooperation among CMS, DOJ, and all stakeholders.

And, finally, all expenses for health insurers' antifraud and -abuse programs should be included as activities that improve healthcare quality in the medical loss ratio calculation since they

reduce waste, which reduces the cost of health care, and enhance patient safety by helping identify and remove providers engaging in unsafe and fraudulent practices from the healthcare system.

In conclusion, I would like to thank the committee for the opportunity to testify today on behalf of WellPoint on this critical issue and pledge our support in any efforts to make the healthcare system financially viable and safe for our members.

[The prepared statement of Ms. Lavelle follows:]

******** INSERT 1-3 ********

Mr. Pitts. The chair thanks the gentlelady and recognizes Mr. Saccoccio for 5 minutes for an opening statement.

Mr. Saccoccio. Thank you. And good morning, Chairman Pitts, Ranking Member Pallone, and other distinguished members of the subcommittee. I am grateful for the opportunity this morning to discuss with you the various methods we believe can be effective in combating healthcare fraud. In my testimony today, I draw upon our organization's 27 years of experience examining, understanding, and fighting healthcare fraud.

There is no silver bullet for defeating healthcare fraud. A winning antifraud strategy for Medicare must be multifaceted and include, as outlined in my written testimony, effective information-sharing among private and public payers of health care; the application of data analytics to healthcare claims; rigorous screening of providers attempting to enter or continue in the program; and a well-trained, adequate, and multidisciplinary workforce. Also, as with prescription drug fraud and diversion, solutions specially designed to address different types of fraud must be developed.

I would like to focus on the first of these points in my oral testimony, effective antifraud information-sharing among public and private payers of health care.

Healthcare fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare and Medicaid migrate to private insurance, and schemes perpetrated against private insurers make their way into government programs. Additionally, many

private insurers and Medicare Part C and D contractors provide Medicare coverage in the States, making clear the intrinsic connection between private and public interests on this issue.

The United States spends $2.8 trillion on health care annually and generates billions of claims from well over a million healthcare service and product providers. The vast majority of these providers of services and products bill multiple payers, both private and public. For example, a healthcare provider may be billing Medicare, Medicaid, and several private health plans in which it is a network provider, and may also be billing other health plans as an out-of-network provider.

However, when analyzing this provider's claims for potential fraud and abuse, each payer is limited to the claims it receives and adjudicates and is not privy to the claims information collected by other payers. In this type of environment, those intent on committing fraud bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme.

And it is precisely this reason why the sharing of preventive and investigative information among payers is crucial for effectively identifying and stopping healthcare fraud. Payers, whether private or public, who limit the scope of their antifraud information to data from their own organization or agency are taking an uncoordinated and a piecemeal approach to the problem.

NHCAA was formed in 1985 precisely for the purpose of serving as a catalyst for antifraud information-sharing. My written statement

provides examples of the types of information-sharing activities conducted by NHCAA.

The Department of Justice also has recognized the benefit of private-public information-sharing. For example, many U.S. attorneys offices sponsor healthcare fraud task forces that hold routine information-sharing meetings. And when invited to do so, private insurers often participate in these meetings to gather and offer investigative insight.

Despite the Justice Department's general recognition of information-sharing as an antifraud tool, many, including NHCAA, saw the need to improve and expand the cooperation and antifraud information-sharing between the private and public sectors. After more than 2 years of discussions and meetings involving several interested parties, including NHCAA, the new Health Care Fraud Prevention Partnership was formally announced on July 26th at the White House.

The Health Care Fraud Prevention Partnership represents a joint HHS and DOJ initiative, bringing together antifraud associations, private insurers, and government and law enforcement agencies. The partnership's purpose will be to exchange facts and information between the public and private sectors in order to reduce the prevalence of healthcare fraud. The partnership will also enable members to individually share successful antifraud practices and effective methodologies and strategies for detecting and preventing fraud.

NHCAA has forged collaborative relationships between the private

and public sectors for nearly 3 decades, and it is from this perspective that we believe the Health Care Fraud Prevention Partnership holds great promise. Just getting under way, the partnership needs time to develop and to demonstrate it can be successful. It needs consistent high-level support if it is to realize the sorts of tangible results we believe it is capable of.

Whether undertaken through NHCAA, regional task forces and workgroups, or through the new Health Care Fraud Prevention Partnership, antifraud information-sharing and cooperation between the private and public sectors is essential to being able to detect emerging scenes and trends at the earliest time possible.

Thank you for the opportunity to testify this morning. I would be happy to answer any questions that you might have.

[The prepared statement of Mr. Saccoccio follows:]

******** INSERT 1-4 ********

Mr. Pitts. The chair thanks the gentleman and now recognizes Mr. Pattinson for 5 minutes for an opening statement.

STATEMENT OF NEVILLE PATTINSON

Mr. Pattinson. Thank you, Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, for inviting me to testify on the solution to the problems for Medicare waste, fraud, and abuse. My name is Neville Pattinson, and I am the senior vice president of Gemalto. And I am here today representing the Secure ID Coalition.

Gemalto is the world's leader in digital security, with over a billion people using our products every day. We develop secure operating systems and run them on secure devices that include smart cards, banking cards, U.S. passports, electronic ID cards, and tokens.

Founded in 2005, the Secure ID Coalition is composed of companies which make smart cards and attendant technologies. We work with industry experts, public policy officials, and government agencies to promote identity solutions that both enable security and privacy protections. We are offering our industry expertise in the area of contact smart cards, which are used extensively throughout the Federal Government and around the world to protect access to both physical and logical assets as well as to protect personal information.

Our Nation's Medicare system is under attack. Medicare abuse and fraud needlessly costs American taxpayers billions of dollars every year. The Centers for Medicare and Medicaid Services estimated in 2010

over $65 billion in improper Federal payments were made through both the Medicare and Medicaid programs. An April 2012 study published in the Journal of the American Medical Association estimated that fraud and abuse cost Medicare and Medicaid as much as $98 billion in 2011. Despite these good-faith estimates, the true cost of fraud and abuse in health care remains unknown.

If we are ever to curb the fraud within the Medicare system, we need to start verifying those who are authorized to provide services, verify those who are authorized to receive benefits, and prevent those who are unauthorized from ever entering the system. Unfortunately, our current inability to address this fundamental identity and verification problem leaves the Medicare system perpetually open to ongoing exploitation. Programs to curb Medicare fraud without first resolving the identity verification problem will ultimately fail if we don't know who is a legitimate beneficiary and who is not.

In order to get to the right track, we must structure the Medicare system to prevent fraud before it happens. This will not only save taxpayers billions of dollars every year, but ensure that Medicare survives to serve Americans well into the future. The Medicare Common Access Card Act, or the Medicare CAC, H.R. 2925, introduced by Congressman Gerlach and Congressman Blumenauer and Congressman Shimkus, is an important bipartisan piece of legislation that looks to solve this problem.

In short, it calls for a pilot program to modernize the current Medicare card in order to verify both providers and beneficiaries as

legitimate participants in the program. In it, five regional pilots would test upgrading the current paper Medicare card to a secure smart card, similar to those used by the DOD and all Federal employees.

The pilots would do three things. First, it would reduce the number of fraudulent transactions by eliminating ways criminals can scam Medicare. Secondly, it would create significant efficiencies within the Medicare program, providing enormous benefit to the legitimate providers and their patients. And, lastly, and some would say most importantly, it would remove the Social Security number from the front of the Medicare card, immediately protecting seniors from identity theft and fraud.

Here is how it would work. When checking out at the doctor's office, the beneficiary inserts their upgraded Medicare card into a reader and inputs their PIN code. The provider simultaneously inserts their upgraded provider card and scans perhaps their finger. This guarantees the transaction is agreed to, authenticated, and is legitimate. It has been electronically signed and encrypted and sent directly to CMS.

What enables the transaction of the high-level assurance is a secure smart card embedded into the card. Smart cards are based on established, nonproprietary, open standards widely used by the Federal Government. Additionally, government healthcare systems globally utilize smart cards. The French, German, Taiwanese healthcare systems all use similar twin card systems to eliminate fraud and increase efficiencies.

Smart cards are also widely used throughout the private sector. Financial services companies worldwide issue debit cards and credit cards to their consumers to prevent fraud and abuse. American banks will be introducing these Chip and PIN cards starting next year. But based on the savings reported by the U.K. financial services industry, the use of smart cards in that sector led to a reduction in overall fraud losses upwards of 70 percent.

Mr. Chairman, I realize I am running out of time, and I beg to continue for another minute.

Mr. Pitts. You may proceed.

Mr. Pattinson. Thank you, sir.

While industry experts believe that Medicare CAC will be able to deliver similar results, it is entirely reasonable to assume a cost savings of at least 50 percent. At the current rate of fraud, that represents well over $30 billion a year.

We are not claiming this will eliminate fraud as we know it, nor is it a panacea. You may hear of vulnerabilities of otherwise resilient and stalwart systems. For that, our security innovations are constantly improving to solve current exploits and prevent future ones. The point is not to create an invulnerable system. That is impossible. The point is to save the Medicare system for the next generation.

Existing fraud-mitigation technologies currently used by CMS cannot do it alone. We must prevent bad actors from getting into the system to begin with. Contact smart cards are the strongest, surest,

proven, and most mature technology to do that.

In conclusion, we are confident that a program such as Medicare CAC will bring value to beneficiaries, providers, and taxpayers alike. For beneficiaries, Medicare CAC ensures that their sensitive personal information, including their Social Security number, is protected by strong encryption that can only be read by an authorized Medicare CAC card reader. Providers will benefit from quicker processing of payments, increased billing accuracy, and the protection of their Medicare provider ID numbers. And taxpayers will ultimately gain the most significant benefit: the reduction in fraud, waste, and abuse within the Medicare system that can prevent the loss of tens of billions of dollars every year.

Everone in Congress wants to preserve Medicare for the next generation of beneficiaries. Medicare CAC does this without having to raise taxes, eliminate benefits, or cut reimbursements. In our opinion, it is the best outcome for all possible solutions.

Mr. Chairman, Ranking Member, and members of the subcommittee, I will be happy to answer questions that you may have. Thank you.

[The prepared statement of Mr. Pattinson follows:]

******** INSERT 1-5 ********

Mr. Pitts. The chair thanks the gentleman and now recognizes Mr. Terzich for 5 minutes for an opening statement.

STATEMENT OF MICHAEL H. TERZICH

Mr. Terzich. Thank you, Mr. Chairman, Ranking Member Pallone, and members of the subcommittee. My name is Michael Terzich, and I am the senior vice president of global sales and marketing for Zebra Technologies Corporation, which is headquartered outside of Chicago in Lincolnshire, Illinois.

I greatly appreciate the opportunity to testify today and share my company's perspective on how secure ID card technology can help address the problem of fraud, waste, and abuse in the healthcare system and, more specifically, the Medicare program.

My company commends you, Mr. Chairman, along with Ranking Member Pallone, for your leadership on this issue. We likewise wish to express our appreciation to your colleague from our home State of Illinois, Congressman John Shimkus, who has worked diligently --

Mr. Pitts. Could you pull your microphone a little closer to you? Thank you.

Mr. Terzich. -- who has worked diligently on this issue and has been a key leader in efforts to eliminate healthcare and Medicare fraud.

As a global leader in the secure ID digital printer industry, Zebra designs and manufactures a variety of products that use sophisticated technology to safeguard identity and streamline business

processes. As a result, I will focus my remarks on H.R. 2925, the Medicare Common Access Card Act, which, as you know, would establish a pilot program to test the potential security benefits associated with modernizing Medicare through the use of secure ID card technology.

Zebra believes that this kind of technology will help protect the continued integrity of the Medicare program. Our confidence reflects the fact that technology enjoys a strong record of performance in both the Federal Government and the private sector. From the Department of Defense's use of secure identity credentials for logical and physical access to vital defense facilities and data networks, to the work of global credit card companies in advancing combined Chip and PIN systems which protect the integrity of both personal identity and financial transactions, secure ID technology provides a tested platform that Medicare can leverage in advancing efforts to combat fraud, waste, and abuse.

Moreover, our experience in the private sector is that the digitization of business processes within Medicare will also help reduce the overall cost of operating the Medicare system. On this point, we associate ourselves with the testimony from our colleagues in the Secure ID Coalition, who address this point in greater detail in their statement.

Let me briefly turn to three key technical elements of secure identification that the subcommittee may wish to consider as it advances H.R. 2925.

The first is the value of leveraging the experience the Federal

Government has gained over the past decade in improving identity security. In particular, we believe that the Federal Information Processing Standard Publication 201, better known by its acronym FIPS 201, and its subsidiary standards known as Personal Identity Verification 1, Personal Identity Verification 2, and Personal Identity Verification Interoperable, also known by their acronyms, PIV-1, PIV-2, and PIV-I, provide a proven framework for providing secure identity management technology into the fight against Medicare fraud.

Since 2005, the Federal Government has issued millions of FIPS 201 and standard PIV cards to Federal employees and contractors covering a wide range of trusted identity applications. Given the Federal Government's significant and positive experience in using PIV-based secure ID technology elsewhere, we believe it makes sense to employ the FIPS 201 standard in the pilot program that is created by H.R. 2925.

Second is the recognition of the value that secure ID card technology brings to the fight against counterfeiting and identity theft. Counterfeiting secure ID cards is exponentially more difficult than counterfeiting paper-based cards, even for the most sophisticated, well-financed criminal enterprises. This enhanced security comes from a combination of media features, printer capabilities, and coding of encrypted data on the smart chip database verification, and secure methods and processes. H.R. 2925's pilot program will provide an opportunity to test these features and

determine the best combination for the Medicare system.

Third, Mr. Chairman, both security and efficiency are substantially enhanced through the use of a decentralized print model, which provides a realtime tie between the creation of a secure ID card and the immediate verification of the cardholder's information. Delays or gaps in time between these two steps, which inevitably occur when cards are manufactured in a remote centralized manner, increase opportunities that can be otherwise reduced through the use of a decentralized print model.

In sum, Mr. Chairman, secure ID card technology enables the use of tested security features which enhance privacy and identity protection. PIV-compliant secure ID cards provide secure, multifactor authentication at a high level of assurance by combining cryptographic private authentication with a personal identification number in a durable, tamper-resistant card format. Once a secure ID card is programmed and associated with a user, it provides a trusted, authentical identity usable for a wide range of cyber-based and physical transactions.

Thank you again, Mr. Chairman, for the opportunity to testify today. We stand ready to assist the subcommittee in developing legislative language related to the technical issues I have mentioned and urge the subcommittee to report out H.R. 2925 with modifications early next year. I look forward to any questions you or your colleagues may have.

[The prepared statement of Mr. Terzich follows:]

******** INSERT 1-6 ********

Mr. Pitts. The chair thanks the gentleman and now recognizes Dr. Fu for 5 minutes for an opening statement.

Mr. Fu. Good morning, Chairman Pitts, Ranking Member Pallone, and distinguished members of the subcommittee. Thank you for the invitation to testify on the expectations of smart cards to combat waste, fraud, and abuse in the Medicare program.

My name is Kevin Fu. I teach courses on smart cards and how to build secure computer systems in health care. While studying at MIT 17 years ago, I helped a hospital deploy a smart-card precursor to authenticate healthcare providers. My responsibility included issuing replacement authentication cards to nurses and physicians who would lose their cards. I am speaking today as an individual.

While smart cards may reduce fraud in other sectors, there do remain challenges that may make deployment more costly and less effective than anticipated. One, smart cards authenticate smart cards, not people. The cards can still be borrowed or stolen. Two, there are several hacks against smart cards that have led to fraud and cloned credentials. And three, interrupting the clinical workflow can lead to unanticipated consequences on patient care that need to be investigated.

So let me highlight the types of fraud remaining in healthcare programs in other countries who have already deployed smart cards for their national health programs. Further details do appear in my written testimony.

In France, it was routine for people to share smart cards. Many

healthcare professionals still do not have the smart-card readers after nearly 15 years. In such cases, a patient in France uses an ancient paper-based system for reimbursement. Thus, loopholes remain for fraud, and the French maintain two separate payment processing systems.

In Taiwan, fraud persists because multiple patients collude with one or more doctors to report higher examination and medication fees such that they can split the extra money among themselves. Even a secure smart card cannot stop that kind of fraud.

In Germany this past summer, the smart-card deployment proved difficult when the manufacturer accidentally distributed cards without PINs to 2 million patients. All the smart cards required replacement.

In Britain, a survey found that general practitioners and staff share their National Health Service smart cards despite warnings of disciplinary action.

And in Australia, they recently terminated its $25 million contract last month for their national eHealth program using a smart-card authentication service.

RPTS JANSEN

DCMN CRYSTAL

[11:05 a.m.]

Mr. Fu. Let me also highlight a few security shortcomings in smart cards just to give you an idea of what could be expected.

In 2011, the DOD Common Access Card was suggested as a model approach for the Medicare Common Access Card. This was a valid approach. But 2 months later, a Chinese computer virus hacked into the computers connected to smart-cards readers to steal PINs from the military cards.

Security, I teach my students, is very difficult to measure or predict and a common property of the hacked smart-card system is that the smart-card system was previously believed to be secure.

In 2006, I culled out a study that analyzed the security of credit cards containing contact-less smart-card technology. The New York Times reported that card companies imply through their marketing that the data was encrypted to make sure that a digital eavesdropper could not get any intelligible information. But instead we found that we could wirelessly scan the credit cards through clothing with a tiny device built with $150 in spare parts.

The Chip and PIN system deployed overseas has also experienced several security flaws that led to fraud. The BBC reported that cards were found to be open to a form of cloning despite past assurances from banks that Chip and PIN could not be compromised. Hundreds of Chip

and PIN machines in stores and supermarkets across Europe have been tampered with to relay credit card data to overseas fraudsters to make cash withdrawals.

With implications to public health, my understanding is that a significant source of fraud comes from home healthcare services. A home healthcare patient who cannot remember to eat breakfast on his own is not going to be able to remember a PIN or password. A stroke victim who must relearn how to swallow may not be able to talk or feed herself without assistance. The home healthcare patient depends greatly on the kindness of others and can be particularly vulnerable to overly trusting a provider.

In short, a vulnerable home healthcare patient would likely comply with an unscrupulous provider who asked to hold onto the card and PIN so as not to inconvenience the patient.

I have four recommendations.

A pilot study should include a security analysis and penetration testing of the system by a neutral third party as well as tests designed with clinical engineers and health IT specialists to measure the impact on patient care.

Two, a pilot study should measure fraud in comparison with alternatives.

And three, a smart-card pilot should measure the impact on fraud while controlling for fraud reductions due to other fraud detection systems.

And four, there should be a period of public feedback coordinated

by a neutral third party who has no financial interest in the outcome of the selected technology. NIST may be a logical choice, given that the proposed legislation refers to NIST standards.

So thank you. Let me conclude. And I am happy to answer any questions you may have.

Mr. Pitts. The chair thanks the gentleman.

[The prepared statement of Mr. Fu follows:]

******** INSERT 2-1 ********

Mr. Pitts. That concludes the opening testimony. We will now begin questioning, and I will recognize myself 5 minutes for that purpose.

Ms. King, in 2010, the Obama administration announced that CMS would cut the Medicare improper payment rate in half by 2012, an error rate that led them to conclude $60 billion in improper payments that were made.

It is almost December of 2012. And knowing that GAO has just released a report on this demonstration project, can you tell us why the administration failed to release its mandated October report?

Ms. King. Sir, you are referring to the Predictive Analytics Report?

Mr. Pitts. I am sorry?

Ms. King. You are referring to the Predictive Analytics Report --

Mr. Pitts. Yes.

Ms. King. -- that was due to Congress?

I can't speak for them. I do know that it has not been submitted yet.

Mr. Pitts. Has the administration met their goal of improper payment rates being reduced by half by 2012?

Ms. King. No, they have not.

Mr. Pitts. What did your report reveal?

Ms. King. Well, the improper payments rate is produced by HHS. And that is not -- the 2012 number was just released. And I do know

that they did not meet their rate, that the rate for 2012 was 8.5 percent or $29 billion, which was slightly lower in percentage terms but higher in dollar amounts than the 2011.

Mr. Pitts. Now, Mr. Olson, in 2010, then-acting Deputy Attorney General Gary Grindler stated that, quote, "It is not enough just to prosecute and punish healthcare fraud after it occurs, we must target it before it happens through aggressive prescreening, auditing, and prevention techniques," end quote.

An all-of-the-above strategy, if you will, and while much public attention has been given to post-payment recovery efforts under this administration, do you believe that we are doing enough in aggressive prescreening and prevention techniques, and what priorities do you recommend?

Mr. Olson. I believe that we have made a good start. But I believe that there is significant progress that needs to be made.

The prescreening methods that have been put in place are good to identify the low, medium, and high providers that are at risk. I still believe this is a beginning point and there needs to be much progress that would be made there. As well with the predictive analytics, I believe it is a starting point. I believe it is a good step that is being taken, but yet much more needs to be done, and I believe we are seeing that with the fraud prevention system that is in place. But it will continue to grow, and as the years roll on, that we will continue to see more activity in that area.

Mr. Pitts. Ms. Lavelle, you mentioned in your testimony that

data sharing between public and private entities is very important for fraud prevention. Medicare Advantage seems like a good example of where public and private payers meet.

What sorts of data sharing occur between Medicare and Medicare Advantage plan companies? And do you believe that data sharing could be improved between the two to improve fraud prevention? If so, how?

Ms. Lavelle. Mr. Chairman, I do believe there is a need to improve some of the sharing. We work through the NHCAA to share amongst all payers. And we do, as private payers, share with the government. However, oftentimes it is just a one-way street and we do not get the information back that we need. For example, if they suspend or revoke a provider, we continue to pay because we do not know who they have suspended or who they have revoked.

Oftentimes, the Department of Justice will have an ongoing criminal case and we will not be allowed to intervene with that payer during this long criminal investigation and we continue to pay bad claims.

And thirdly, there are a number of whistleblower lawsuits that involve patient harm. And until that qui tam lawsuit is unsealed, we cannot do any intervention with our providers that may be causing harm to our members.

Mr. Pitts. Okay. Now, you mentioned in your testimony the Controlled Substance Utilization Monitoring Program and limiting documented prescription drug abusers to one pharmacy and one prescriber as a mechanism to prescription drug abuse and to stop the costs

associated with doctor shopping.

Does Medicare Advantage or Part D plans allow insurers to implement a similar type of program? If not, do you know why?

Ms. Lavelle. Not at this time. We have sought to get authority to do that. But at this time, they have not authorized that type of lock-in program.

And, generally speaking, our biggest problems are with the dual eligibles between the age of 20 and 40. They not necessarily are seniors. But these are the folks that have the addiction problem and are overdosing, basically.

Mr. Pitts. Thank you. My time has expired.

Chair recognize Ranking Member Mr. Pallone for 5 minutes for questions.

Mr. Pallone. Thank you, Mr. Chairman.

I wanted to ask Ms. King initially, one of the witnesses today, I guess it was Mr. Pattinson, noted that by requiring identity verification of providers and beneficiaries, Medicare would easily eliminate more than 50 percent of the fraud within the current system.

Do you believe, you know, that that is fairly accurate or would a verification process eliminate that much of current fraud?

Ms. King. First, I do not think we really -- there is no reliable estimate of how much fraud there is in the healthcare system. So half of a total that we do not know, it is hard to say what that would be.

Secondly, I think that we just identified for the first time the types of providers that were involved in healthcare fraud. And no one,

to my knowledge, has done an in-depth analysis of what the causes of fraud might be.

So I think it would be premature to say that you could eliminate 50 percent of the fraud based just on identity theft, because we do not know the extent to which identity theft contributes to healthcare fraud.

Mr. Pallone. Let me ask Ms. Lavelle about WellPoint's anti-fraud initiatives. Does WellPoint use a smart card for beneficiaries like the one envisioned by the Medicare Common Access Card legislation?

Ms. Lavelle. Mr. Pallone, we are on shifting sands right now with emerging technologies in the healthcare arena. We decided in the past year to pick up a predictive analytic modeling tool. And, to date, we haven't explored the smart card. We are exploring other sophisticated methods in the future, including an app that might go on a smart phone or an iPad. But we are still analyzing all the tools out there.

Mr. Pallone. Are you aware of any of the Blues' plans that require beneficiary and provider smart cards? Do they use them?

Ms. Lavelle. I am not aware of any that do, no.

Mr. Pallone. As opposed to spending money on cards and card readers, where has WellPoint invested its anti-fraud dollars? If you had to pick one activity that you believe gives you the best bang for the buck, what would that be? And do you have any sense of your return on investment for these anti-fraud activities?

Ms. Lavelle. Our most valuable tool at this time is our predictive analytic modeling tool. We are finding anomalies in systems, we are finding aberrant providers that are basically committing fraud. We are finding weaknesses in our own systems, in our own contracts, and in our own medical policies, things that we can urgently change to save dollars on an enterprise-wide basis.

Mr. Pallone. Do you have any idea of the return on the investment, though, in terms of that?

Ms. Lavelle. It is well over 15 to 1 at this point.

Mr. Pallone. Okay.

And then I wanted to ask Dr. Fu, I noticed in your testimony how a number of instances of fraud were committed when card readers were tampered with. Seems to me that placing multiple card readers in every physician's office just invites the opportunity for more fraud. Even an unsuspecting physician could be victimized by a faulty card reader. While that may not be happening today, isn't it conceivable that that is a danger in the future?

Mr. Fu. That is a potential risk because of the software that is associated with the card readers and the connections that different components make into the clinical computing systems.

Mr. Pallone. I am also concerned about the costs of implementing a smart-card system for all of Medicare. There is the cost of issuing the cards, the fingerprinting a million-plus physicians and new physicians, possibly the costs of getting photos of beneficiaries for the cards, and the card readers, not to mention the system changes that

Medicare would need to make to accept information from this new technology.

From your experience in working in a medical setting, do you think it is reasonable to assume that each provider office would only need one card reader or do you think estimates of one card reader per office are a bit understated?

Mr. Fu. I would suspect that providers would need more card readers than they originally anticipated. I say that because 17 years ago, when we rolled out a similar system in a community hospital, that was one of the areas where it was underestimated how many card readers we needed, as well as how many cards we needed to purchase, too, because the physicians and nurses would inevitably misplace the cards.

Mr. Pallone. Let me just go back to Ms. King.

One of the things that I believe is important to keep in mind as we design our anti-fraud arsenal is that fraud is multifaceted.

Could you just take a moment to describe the different kinds of fraud that is perpetrated against the Medicare program? I know I am almost out of time, but as briefly as you can.

Ms. King. According to the Inspector General, there are lots of different kinds of fraud, but they include billing for services that aren't needed or not provided. There are kickback schemes where people sell their numbers, sell their beneficiary numbers.

But, you know, there is a broad spectrum of fraud that is committed. But I don't think there has been a comprehensive analysis done that really drills down on all the types of fraud that have been

identified. And there is, of course, a lot of fraud that goes unidentified because it is under the radar. People are committing acts that would be fraud that are not detected.

Mr. Pallone. All right. Thanks a lot.

Thank you, Mr. Chairman.

Mr. Pitts. The chair thanks the gentleman and recognizes Dr. Burgess for 5 minutes for questions.

Dr. Burgess. I thank the chairman for the recognition.

Ms. King, thank very much for being here. Thank you for your testimony today.

Now, you gave us an impression in your spoken testimony that you have provided CMS a list of items that they might consider doing in order to implement the programs that they said that they are already implementing. Did I understand that correctly?

Ms. King. Yes. We have a number of recommendations that we made to them.

Dr. Burgess. Would it be appropriate for GAO to provide this committee with an itemized list of those things they have sent to the Centers for Medicare and Medicaid Services in order to get to the bottom of some of these inappropriate payments?

Ms. King. We would be happy to.

Dr. Burgess. Now, to date, has CMS replied to your provision? You have provided this information to CMS. Is it a two-way street? Are they coming back to you with the information?

Ms. King. If we issue a report that has recommendations, the

agency always has a chance to comment on them. And usually they either agree or disagree. And then we have an annual process where we follow up with them once a year to see whether they have implemented recommendations.

Dr. Burgess. Well, that is really my question, that opportunity to agree or disagree.

In your bibliography, you referenced another report you did last month about Medicare fraud prevention, CMS has implemented a predictive analytic system.

In your recommendations part, you said HHS agreed to described action CMS was taking to address the recommendations. But my problem is, we have been talking about this for the 10 years that I have been here and we are not getting anywhere.

So how do they provide you with definitive actions that they are going -- do they provide you with definitive actions that they are going to take that are associated with metrics where we could all know that they are doing what they said they were going to do?

Ms. King. When we do our annual follow-up on recommendations, we engage in a rigorous process with them to determine whether, in fact, they have adopted recommendations.

Dr. Burgess. When was this last annual report generated by CMS?

Ms. King. We do our recommendation --

Dr. Burgess. I am sorry, your --

Ms. King. We do our recommendation follow-up each year in the fall.

Dr. Burgess. Okay. So is there a recent one that has been provided?

Ms. King. That is an internal document to GAO. But we track that and we would be happy to provide you with a list of recommendations and the status of the follow-up.

Dr. Burgess. That is what I was getting at. Thank you.

And, Mr. Chairman, I would like for those to be provided and made part of the record and made available to every member of the committee, because I do think that it is important.

We are all talking about the fact that we are just a few months away from Elysian Fields of the Affordable Care Act, and everyone is going to have everything that they ever wanted. But I don't know quite the number of States that have agreed to do their own exchanges, but there is a big number of States -- I know my State is not going to do a State exchange -- so there are a number that will fall into whatever this Federal fallback position is, which looks a lot like the public option.

And one of the concerns I had about the public option when we talked about in this committee during a markup on H.R. 3200, which was the healthcare bill that didn't become law, one of the big concerns I had with the public option was we got a lot of problem right now with inappropriate payment in Medicare. Why in the world would we expand another public program before we get our hands around this problem?

So I know the GAO does not speculate and they don't engage in conjecture. But do you have a feeling about what the future holds just

a short year from now as those large public options come online?

Ms. King. Sir, I would have to say not yet.

Dr. Burgess. Well, I was afraid of that answer. Okay.

Ms. Lavelle, let me ask you, because you are WellPoint. You are private sector. Is your company going to be developing a product that will be available in the State exchanges?

Ms. Lavelle. I am not certain at this point. But I can find out and have someone get back with you on that.

Dr. Burgess. Then, of course, along the same line of reasoning, you know, would you participate in a Federal exchange if there were this large Federal fallback that were provided to States that weren't going to set up their exchanges?

My understanding is this will be set up through the Office of Personnel Management, not through HHS. This is a pretty little-known and little-understood Federal agency right now that administers the Federal Employee Health Benefits Plan. But it is fixing to become an enormous Federal agency that will administer a problem -- a problem -- -- sorry, Freudian slip -- a program that is every bit as big as what CMS administers today in the Medicare system.

So I would assume a company like yours would look at that and say, this is market share, we have got to be a participant in this.

But at the same time, you have got this other problem with the medical loss ratio rules that are there in the Affordable Care Act. And I assume your company has looked at those medical loss ratios rules because they probably do affect you, do they not?

Ms. Lavelle. Yes. Absolutely.

Dr. Burgess. So if you spend money on fraud prevention, is that money scored as an administrative expense or a healthcare expense?

Ms. Lavelle. We can only count the dollars up to the amount of recovery we bring in each year. So if we bring in, you know, $2 million, that is all we can count outside of the administrative costs.

Dr. Burgess. I think you gave us a figure of ROI, of return on investment, of 15 to 1. So, presumably, that would be something you would pursue even in light of the MLR rules. Is that correct? Or is the MLR going to be an inhibitory factor for you?

Ms. Lavelle. It continues to be inhibiting, based on our growth. We do a lot of quality of care investigations. We have found diluted chemo drugs. We have cases on cardiologists doing unnecessary stents, unnecessary bilateral cardiac caths. Maybe half of our work deals with quality of care and patient harm. And that is why we feel we should get some credit for some of the work and the prevention that we do.

Dr. Burgess. I couldn't agree with you more.

Mr. Chairman, I would just submit, at some point, we perhaps need to have a much wider evaluation of these medical loss ratio rules and how they affect. I mean, you are talking about patients -- you are not just talking about fraud, you are talking about patient safety.

Ms. Lavelle. Exactly.

Dr. Burgess. We just had a big hearing in Oversight Investigations on patient safety because of some altered steroids in the compounding pharmacy. Patients depend upon us to be their

watchdogs on this. And the fact that you feel that this is something that is being inhibited by the Affordable Care Act, we need to get on top of that.

Now I will yield back my time.

Mr. Pitts. The chair thanks the gentleman and now recognizes the gentlelady from Illinois, Ms. Schakowsky, for 5 minutes for questions.

Ms. Schakowsky. Thank you, Mr. Chairman.

Ms. King, I wanted to ask you a question. I think the chairman was getting at whether or not the administration has met its goals. And so the issue of how does one measure the effectiveness of fraud reduction measures. And I wanted to ask you about this.

Those that prevent fraud from happening, how would we measure that? For example, since March of 2011, CMS has deactivated 136,682 provider enrollments and revoked 12,447 enrollments, taking away their billing privileges because of, I guess, identifying them as fraudsters. And they no longer have the privilege of billing Medicare.

So how would we calculate, or can we calculate, what kind of savings are realized by this revocation of billing privileges or any other kind of prevention measure that we might take?

Ms. King. I think there are a number of steps that CMS has taken that are in the prevention category. And one thing is strengthening provider enrollments and standards so that you are keeping out people from the get-go who shouldn't be providing services to the program.

So it is hard, you are right, it is hard to measure, well, you know, what might they have billed had they been allowed.

And I think on the other side another example is the Fraud Prevention System, the Predictive Analytic System. If you are preventing things from happening, then how do you measure the magnitude of that? And I think that is something that CMS is working on and struggling with, but it is a difficult issue.

Ms. Schakowsky. I think it is really, really important that we do that. And I think everyone on both sides of the aisle agree we need to do better. But I think it is also important that we get the metrics right so that we properly evaluate the measures that we are taking.

Let me ask you a question, Dr. Fu. As you know, the smart-card industry has legislation that would mandate CMS undertake a specific demonstration project to pilot their technology in five States.

I am not a researcher, but it would seem to me that the bill could be made better in this fashion. It seems that testing one particular intervention against doing nothing likely will yield results. But it seems to me that the better question that Medicare and Congress should be exploring is testing one technology against another technology.

So wouldn't it make more sense to test different interventions against each other to see which one is best?

Mr. Fu. So in my written testimony, I have some further comments on that. I can highlight that.

I agree, it would be more telling if the experiment were comparative as opposed to absolute.

In particular, commingling the fraud reduction from the predictive analytics may make it more difficult to understand where

is the reduction coming from, from the analytics or from the smart card. So it should not be conflated with the benefits from other anti-fraud mechanisms.

There are some other technologies one could try. I would say none of them are surefire. But it is a valid question to ask.

I believe one comment that was raised today was the issue of using a mobile app. And I have heard of suggestions of using an inexpensive photo ID. They all have problems. They all have benefits. But it is good to know the comparative.

Mr. Pattinson. I would just like to add to Dr. Fu's comments that the smart-card technology is well proven around the world. Everybody in this room probably has at least one of them on your person in the form of a SIM card in your phone. It is in the U.S. passport. The Federal Government is using them to protect all of their infrastructure.

So this is not testing a technology on the basis of does it work or not. Smart cards work in this situation for authentication and for identification. We are certainly not saying they should be done alone, and we agree that they should be done in conjunction with other technologies as they emerge. They can be included.

But at the moment, this is an easy thing to help save the Medicare system a great deal of money very quickly with proven technology, even though under H.R. 2925, we are only asking for a pilot because we want everybody to be confident that we can build the best system to save the most money to preserve the longevity of Medicare.

Ms. Schakowsky. Thank you, Mr. Chairman.

Mr. Pitts. Chair thanks the gentlelady.

Now recognizes Dr. Cassidy for 5 minutes for questions.

Dr. Cassidy. Thank you all for being here.

Ms. Lavelle, WellPoint has MA plans. And do you have the same level of fraud, waste, and abuse in your MA plans that you administer for CMS as is reported to occur in direct fee-for-service Medicare?

Ms. Lavelle. That is difficult to answer, Congressman.

We are very vigilant with our MA plan. We have a lot of rigorous applications, data mining programs we run against it.

One of the common denominators and one of our biggest issues is the "any willing provider" clause that allows any willing provider to bill.

Dr. Cassidy. Are you allowed to do precertificaiton, preauthorization even if you have an "any willing provider"?

Ms. Lavelle. On certain procedures, yes.

Dr. Cassidy. Okay. Okay. So you are not sure, possibly, but just not sure.

Ms. Lavelle. Well, I am not certain if our level of fraud in MA is the same as CMS.

Dr. Cassidy. Got you.

Ms. Lavelle. It is just hard to determine.

Dr. Cassidy. Okay. Now, everybody is familiar with McAllen, Texas, immortalized in the New Yorker as a place with a lot of CMS fraud, waste, or abuse. But there is a health affairs article, first author

is Franzini, looking at the Blue Cross population. And in this actually McAllen, Texas, had a 7 percent lower utilization rate than El Paso.

Now, it seems like if Blue Cross is 7 percent lower in a place where -- I forget the exact number -- but where McAllen is like 180 percent higher than El Paso, that the problem is CMS, frankly. And the authors of the paper at the end postulate what could be the problem. Some of them are reflected in your GAO report.

Would you like to render an opinion on that?

Ms. Lavelle. I am not familiar with the article, so I'd rather not.

Dr. Cassidy. What would be your estimate of why Blue Cross Texas has 7 percent lower expenditures in McAllen, whereas CMS has, again, I wish I had looked at -- 80 percent or 180 percent higher than the cohort city, if you will, the comparison city?

Ms. Lavelle. I think we do have some sophisticated tools in place that stop the dollars before they go out the door.

Dr. Cassidy. So that suggests that CMS does not.

Ms. Lavelle. No. I am not suggesting they do not. But we are very competitive in the Blues. And we are very collaborative between States in warning each other, giving early warning signals. But we do have very rigorous special investigation --

Dr. Cassidy. Got you. The only reason I am cutting you off is time is limited. And it does seem as if the Blues have something that CMS does not, which is a little daunting when we figure we are turning

over our healthcare system to them.

You mention in your testimony, I think it was you, about the duel eligibles being able to change Part D plans month to month. And so those seeking drugs will try and stay one step ahead.

Ms. Lavelle. Yes.

Dr. Cassidy. Do you have an estimate of how much money we would save? Because prescription drug abuse is a huge problem.

Ms. Lavelle. It is.

Dr. Cassidy. Do you have an estimate of how much we would save were we to limit that activity?

Ms. Lavelle. I don't have an estimate. But I can tell you that a single provider that we lock into place with a single ER for nonemergency use, we could save at least 300,000 to 400,000 a year based on --

Dr. Cassidy. Three hundred four thousand what?

Ms. Lavelle. Dollars a year, per member.

Dr. Cassidy. Per member.

Ms. Lavelle. For locking them in. They evade the lock-ins by jumping from WellPoint to Humana to Aetna.

Dr. Cassidy. You would save $300,000 per member, per year?

Ms. Lavelle. For every dollar we spend on drugs, we have determined that we spend approximately $41 on facility fees.

Dr. Cassidy. And any clue the size of this population that you would save $300,000 per year on? I mean, is it a thousand people? Is it a million people?

Ms. Lavelle. It is hard to say. But it is --

Dr. Cassidy. Ballpark.

Ms. Lavelle. We probably have a thousand right now that we are monitoring. And we just don't have the manpower to monitor --

Dr. Cassidy. So a thousand times 300. We are talking about real change here --

Ms. Lavelle. Yes.

Dr. Cassidy. -- for one company. Granted, a big one.

Ms. Lavelle. Right.

Dr. Cassidy. Dr. Fu, I really liked your testimony, man. I will tell you, the TWIC card was supposedly going to be the answer for all security problems, and I get regular complaints from people fighting about the TWIC card. And I like the way you kind of, if you will, puncture a couple holes in its foolproofness.

Is there anything short of a retinal scan that could actually make a secure ID card? Because you mentioned, if somebody gives their card to somebody else and they can take that number, et cetera, et cetera.

Mr. Fu. Thank you, sir.

Identity is very difficult to establish. In computer security, there are three basic ways to do it. You can use something you have, like a smart card; something you know, like a password; or something you are, like a fingerprint. Whereas we also like to call it something you lost, something you can't remember, and something you were.

But I would say that the difficulty is in how the smart-card system is used in the greater system. So it doesn't matter if you have the

most secure technology or even if there is a flaw, if that system is put as a component in a larger system that it itself has flaws. For instance, a paper-based --

Dr. Cassidy. Got you.

Mr. Fu. -- alternative system would leave that door open to fraud.

Dr. Cassidy. But still within that, there has to be -- and you point that out -- there has to be things about the card itself even in a perfect system that can make that system vulnerable.

So I go back to again is anything besides the fingerprint or a retinal scan going to give you the assurance that somebody sitting at a computer terminal is just not filing claims for things not done?

Mr. Fu. Unfortunately, despite decades of research in computer security, there is no silver bullet. There is no surefire way to establish identity. I think one of the reasons that certain identity cards work well in buildings is that you may have police nearby or people watching or people who would catch you.

So I don't have a good answer for you on what would work better. I do think it is a good idea to try different alternatives because different contexts you will see different technologies having different advantages.

Dr. Cassidy. Thank you, Mr. Chairman. I apologize for going over.

Mr. Pitts. Thank you. The chair thanks the gentleman.

The chair recognizes the gentleman from New York, Mr. Engel, for 5 minutes for questions.

Mr. Engel. Thank you very much, Mr. Chairman.

Mr. Saccoccio, in your testimony, one of your recommendations is that we ensure a skilled and sufficient workforce of anti-fraud professionals. My sense is that no matter how much we invest in front-end screening or technology solutions, we will still have a need for those boots on the ground.

There are providers who look legitimate on paper and it is only until an unannounced visit that we discover something is wrong. Sometimes it is not until a beneficiary is interviewed or calls to report something suspicious that investigators get a hint of problems.

So my question is, can you talk about what kind of anti-fraud workforce CMS should maintain? Do you believe additional investments in anti-fraud funding, including for personnel, would be valuable to help fight Medicare fraud?

Mr. Saccoccio. Yes. Thank you for the question.

I definitely agree that technology is not the silver bullet. It is a tool that has to be used. Predictive analytics is important. It is going to give you a lot of leads. But once you get those leads from the technology, you need the people to examine those leads.

I don't know of any system right now where you could just flip a switch and based on the information you get back from a computer be able to automatically deny a claim or suspend a claim until there is some sort of investigation done.

So you definitely need folks that are very savvy with technology, experts in technology. You need folks able to analyze data that is

generated, statisticians, those types of folks. You need folks that have clinical backgrounds, because as a few of the witnesses talked about, a lot of the issues involve quality of care, necessary care. So you need folks that have clinical backgrounds.

And then you need investigators, folks that know how to do investigations, folks that can go out into the field and ask questions and visit sites where potentially you have phantom providers or fraudulent providers.

So you need a mix of workforce. So definitely any resources that are put into this, some have to be focused on technology. But you also have to ensure that you have the right type of workforce to go out there and conduct the investigations and validate the information that the technology is feeding you.

Mr. Engel. Thank you.

Let me ask you again, Mr. Saccoccio, and also Ms. King, the Affordable Care Act contains a number of provisions designed to promote data sharing between agencies, the Federal Government, and the States, and also various Federal healthcare programs. And it also, as you know, provides new tools and strengthens penalties against fraudulent providers.

The CBO, the Congressional Budget Office, estimates that these anti-fraud provisions when fully implemented will save American taxpayers $7 billion over the next 10 years.

So let me ask you again, Mr. Saccoccio, and also Ms. King, what specific aspects of fraud detection do you think are being most

positively impacted by the provisions in the Affordable Care Act and what additional steps do you believe Congress should take to enable better fraud detection and prevention?

Ms. King, why don't we start with you.

Ms. King. Yes. Well, one of the key provisions of the Affordable Care Act was a set of provisions strengthening the ability of CMS to screen providers before they are enrolled in the program. So you are ensured that you are only getting legitimate providers in the program.

And as part of that process, CMS also contracted with a couple of contractors to do onsite inspections to go up, you know, for high-risk providers to make sure that they are, in fact, legitimate businesses and to automate the enrollment process more quickly so that you can see before you enroll someone whether they are on the do-not-pay or the excluded list.

So those kinds of things I think have a good bit of potential.

Mr. Engel. Thank you.

Mr. Saccoccio?

Mr. Saccoccio. Yes. I think the biggest thing in the Affordable Care Act, as Ms. King mentioned, is the ability, giving CMS greater ability to screen providers coming into the program.

And I think some of that is going to require, depending on how you establish -- when you look at different providers, you have to establish potential risks from those different types of providers. So the greater risks that you anticipate, the more screening you will have

to do, which may require some onsite visits for things like DME companies, to ensure that these are actually valid companies that are actually in business.

But I think one of the steps looking to the future is that a lot of this information that is coming out of their automated screening process that CMS is doing has to also be incorporated into their Fraud Prevention System.

In other words, connecting the dots, not -- as you screen providers, to make the network connections between different types of providers. Because what you have is are often put up as fronts for different companies. And as you establish who these folks are, you'll see that there are connections with other folks that are actually committing fraud.

So I think a big piece of that is doing the screening, but then incorporating what you are finding out from that screening and what you are also doing with respect to claims analysis and predictive analytics.

Mr. Engel. Thank you.

Thank you, Mr. Chairman.

Mr. Pitts. The chair thanks the gentleman and now recognizes the gentleman from Georgia, Dr. Gingrey, 5 minutes for questions.

Dr. Gingrey. Mr. Chairman, thank you.

And I want to thank all of the panelists, all of the witnesses. I am going to direct my questions primarily to the member from the Government Accountability Office, Kathy King. So, Ms. King, it will

be primarily directed toward you.

I will kind of follow up on what my colleague from New York, Mr. Engel, was just referencing regarding the provisions in the Patient Protection Affordable Care Act, Obamacare, toward combating waste, fraud, and abuse. And I think he gave the figure of an estimated savings of $7 billion over 10 years if these provisions of Obamacare were implemented.

Ms. Lavelle testified that WellPoint's anti-fraud activities rely in part on a system of identifying high-risk practices, providers, and beneficiaries, and then creating solutions such as prior review to deal with these problems.

The Patient Protection and Affordable Care Act created a number of -- in fact, I think at least eight anti-fraud provisions, such as granting the Secretary the authority to conduct criminal background checks for providers and suppliers considered high risk.

Ms. King, you referenced that.

Can you tell me whether this administration has, to date, implemented all of these provisions that are in the law in Obamacare?

Ms. King. I cannot, because our process of checking on them is not complete. But, you know, in the spring when we also testified about this issue, there were a few provisions, including the criminal background check and surety bond provisions, that were not yet implemented.

Dr. Gingrey. Let me help you a little bit. You say you cannot answer the question on what has been implemented.

Section 6407 of Obamacare created a requirement that CMS implement face-to-face encounters between patients and providers before a physician can certify eligibility for durable medical equipment.

While the State of Georgia has many good and hopefully honest and mostly honest DME providers, we all know that durable medical equipment is one of the most fraudulent areas in Medicare and has garnered nationwide scrutiny on programs even like "60 Minutes."

Can you tell me, has the administration implemented face-to-face provider meetings for DME to date? Have we done that?

Ms. King. Not to my knowledge, they have not. Ordinarily, if I were appearing before a committee, I would check on all of those things, but I did not have the opportunity to fully check all those things before coming today.

Dr. Gingrey. Well, look, I am going to help you again. And I said there were eight things I think you -- maybe CMS has implemented one of the eight. But let me list, just read to you a number that have it, including this face-to-face encounter in regard to prescribing durable medical equipment.

Implement checks to make sure that a physician actually referred a Medicare beneficiary for medical service -- for example, clinical laboratory -- before paying the claim.

No, they have not done that.

Implement a surety bond on home health agencies and certain other providers of services and supplies.

No, they have not done that.

Establish a compliance program for fee-for-service providers and suppliers.

Once again, no, that has not been done.

Implement a temporary moratorium for new Medicare providers from enrolling and billing the Medicare program even though there are more than enough suppliers to furnish healthcare services in certain areas of the country.

No, they have not done that.

Mr. Chairman, I believe this committee should find out what powers CMS has. Many of them, as Ms. King indicated, and others, that were granted in the law which is now over 2 years old to help implement waste, fraud, and abuse that it currently does not employ. So how are we going to save that $7 billion over the next 10 years.

My opposition to Obamacare in this committee certainly is well known. I do believe that protecting taxpayer dollars and Medicare dollars from fraud and abuse is one of the main charges of this government and that we as committee members have.

And it is very much a bipartisan issue. Medicare is set to go bankrupt as early as 2017, as late as 2024. If this administration has the authority to implement changes within the Medicare program that could prevent billions in lost funds annually and it is not using them, I believe, Mr. Chairman, that the administration owes us an accounting of the reasons why to date, 2 years, seven out of eight provisions have not been implemented.

And I yield back.

Mr. Pattinson. Mr. Chairman, Congressman, I would like to make a comment.

Mr. Pitts. Go ahead. You may.

Mr. Pattinson. I think you are describing a very significant problem about the DME issue of being able to deliver equipment and have it prescribed without physical contact.

Looking at the pilot that we once proposed under this Medicare CAC Act, I would suggest that that is exactly a very good reason why we could use the twin card approach; a provider and a patient must both combine their cards in a reader to perform the transaction to show that they have authorized this particular DME equipment for this provider, by this provider for this individual. Then subsequently on delivery. Then we know who was responsible for issuing that request.

So no nefarious claims or no nefarious deliveries of DME equipment can now take part on the basis that you have to have two keys to make that request work. So I would strongly recommend that we include that as part of the pilot.

Mr. Pitts. All right. Thank you.

The chair now recognize the gentleman from Illinois, Mr. Shimkus, for 5 minutes for questions.

Mr. Shimkus. Thank you, Mr. Chairman.

Apologize for not being here for all the opening statements. Thanks for your testimony. In this era of budget crises and entitlement reform, to think that we wouldn't do some simple steps to

get a handle on waste, fraud, and abuse is unbelievable. Frustrating from those of us.

Mr. Pattison, just for a second, and you mentioned it earlier in one of the questions, H.R. 2925, which I am a co-sponsor of, bipartisan support, is what type of a program?

What is the intent of 2925?

Mr. Pattinson. It is to operate a pilot --

Mr. Shimkus. A pilot program.

Mr. Pattinson. Pilot program of five regions.

Mr. Shimkus. How are the region to be chosen?

Mr. Pattinson. The regions would be defined the by agency implementing the --

Mr. Shimkus. And it is my understanding under the highly abused areas of --

Mr. Pattinson. If that's what they so choose, that would be where they would have the best effect.

Mr. Shimkus. That is the intent.

Mr. Pattinson. Indeed.

Mr. Shimkus. I think that is our intent.

Mr. Pattinson. The pilot would be to upgrade the Medicare cards for the beneficiaries by taking the number off the card and providing the card, such as the one I have in my hand here. It would also be providing a similar smart card, but with more capability to the provider. Then by using the terminals at the various locations, which, by the way, with a Chip and PIN implementation coming out, these

terminals are going to become prevalent all over the place, anyway. So we are just adding basically functionality to existing terminals that will exist by the time we get around to a pilot.

But by putting the two cards in the same unit, performing the PIN actions of the beneficiary and the fingerprint of the provider, we conceal those transactions and prevent people from creating transactions without any of these technologies.

So think of it like a safety deposit box in the bank; you need to have two keys to make this drawer open. You need to have these two keys to make these transactions work.

So the pilot is to test this. And to date Dr. Fu's testimony, it is to make sure we design the very best and most robust system for a potential rollout.

Mr. Shimkus. And, Mr. Terzich, do you want to add to this discussion on the use of the card?

Mr. Terzich. Mr. Congressman, I would add the following. Essentially, when you look at, both from the government and from the private sector perspective, the pervasive deployment expansion of smart cards and smart chips, you know, today there are literally billions of smart chips in circulation, millions of smart cards in circulation. And despite some random rogue instances of security breach, the underlying technology has demonstrated time and time again that it is a very productive, useful technology.

And when you apply that to the challenge at hand here where there is a very optimal opportunity to engage in the low-hanging fruit by

simply deploying some technology, that I think would in many respects take a big slice out of the abuse and the fraud that exist today.

Mr. Shimkus. I have no understanding why we would not move immediately to do this as a start. Not the entire solution of waste, fraud, and abuse in the system. But this is really a no-brainer. Twenty million Department of Defense individuals use this system. This is not -- this is not new technology or new activity that no one has used before.

So the other thing I would like to add on is, Mr. Pattinson, how about international -- well, let me start by this too, because my frustration is pretty high on our challenges that we face in this country.

If anyone uses their credit card overseas today, theft comes by someone stealing your slip, not through the technology.

If anyone uses a passport, these new passports that we have that swipe through the system, they are using this with biometric facial identification. I mean, folks, we are using this now. All we are asking is that let's try it to highlight waste, fraud, and abuse.

I want to move to Ms. Lavelle real quick.

Your testimony is also illustrative of an issue with the healthcare law, fee for service, and Medicare Advantage. And I would hope that when you go back, you would ask to do an analysis of the waste, fraud, and abuse under fee for service versus waste fraud and abuse in dollars. You have to get some statistician that would make it equal sizes or whatever they have to do to make sure.

But I would wager money that fee for service is multiple times more abusive in waste, fraud, and abuse. And the argument I would postulate is that you have an organization established and folks making sure that there is not waste, fraud, and abuse going out the door, and that is that whole medical loss ratio debate and what is going to be able to be paid for.

So if we don't allow companies to do their due diligence because we don't let them qualify in the medical loss ratio, guess what, we are going to have more waste, fraud, and abuse. It is the most ludicrous thing that I have seen. We need market, we need competition. The private sector does that because they don't want to lose the money.

With that, Mr. Chairman, I think we need to have many more hearings on this issue.

Thank you all.

Mr. Pitts. The chair thanks the gentleman and now recognizes the gentlelady from Tennessee, Ms. Blackburn, for 5 minutes for questions.

Ms. Blackburn. Thank you, Mr. Chairman.

And I want to thank each of you for your patience, sitting through this hearing, being here with us today.

Ms. King, thank you for your report. I appreciate that you got that in to us in a timely manner, and I appreciate the way that you broke it out, looking at medical facilities, durable goods, and where the problem exists.

I think for those of us that have been focusing on this waste, fraud, abuse issue in the Medicare/Medicaid systems, and this is not

a new problem, what we have come to realize is that HHS as a whole doesn't put enough attention on this issue, and that we still have a broken system, and that the pay and chase model does not yield the results that we need.

And I can tell by looking at your nodding heads you all agree with that.

I will say this. I am disappointed that we did not get the Medicare report that was due to be made public on October 1 looking at these issues. And my hope is that we are going to see this soon.

I do want to ask you, Ms. King, did you all look at the contract that was given to Northrop Grumman in 2011 to develop a system? We had the bureaucrats there at Centers for Medicare and Medicaid at CMS that gave a $77 million contract to have Northrop Grumman in 2011 to come up with a fraud prevention system. Did you all look at this contract and the miserly little yield that has come from that with its first eight months of implementation?

Ms. King. We evaluated the implementation of the program. But we did not look specifically at the contract.

Ms. Blackburn. Okay. But I think you can say if we spent $77 million in 8 months into the implementation, we have seen a $7,591 return from that investment, that it is pretty poor, pretty poor investment.

I want to turn to Mr. Saccoccio, Mr. Terzich, and ask you all, if you were given a $77 million contract, how would you go about -- what would your advice to Medicare, to CMS be on solving this problem? Would

you have a ready answer? Would you have a way to move forward to help CMS, to help companies like WellPoint in identifying this fraud before it is committed?

Mr. Saccoccio. You know, the CMS contract and their implementation of this Fraud Prevention System, from our viewpoint, it is definitely a road they have to go down. Now, whether or not, you know, the cost of that contract and who they decided to go with, with respect to that contract, I have no particular information on that. But definitely predictive analytics and predictive modeling, those are the things that they have to be doing going down the road.

Now, sometimes I think what happens with these systems is that, with respect to suspension of payments, I know they haven't started where they are actually suspending payments based on the --

Ms. Blackburn. Well, in the interest of time, let me interrupt you now.

Do you know private sector companies that could probably solve this and solve this problem quickly?

Mr. Saccoccio. It is hard to say. I know some of the health plans are using predictive modeling of some sort. About 40 percent of our members do. And as Ms. Lavelle mentioned, they are having success with that.

So I think, you know, obviously, the implementation, there are more efficient ways of doing things. But not being part of that process, it is very hard for me to say.

Mr. Terzich. Congresswoman, can I add a comment here?

Ms. Blackburn. Yes, you may.

Mr. Terzich. You know, when you have look at the challenge that we face, I think it is the sum of a variety of technology-based solutions that can make a big impact.

And beyond predictive analytics, you know, you have the opportunity in H.R. 2925 to add the electronic handshake that occurs. And that information that gets processed in real time, in combination with predictive analytics, is going to increase visibility throughout the process.

And from our private commercial experience in business, what you see is the more visibility you apply to the process through the use of technology, the more opportunity you have to refine those processes over time. And so it is much more of a journey than an event. But it creates a tremendous opportunity.

Ms. Blackburn. So what you are saying basically is, with the existing technologies and with the existing platforms that you all have created in the private sector, we could create a pathway that would place the necessary firewalls and the necessary handshakes and the necessary screenings and prequalifications that would eliminate much of the fraud, which has now become big business in Medicare/Medicaid, so big that we have even had the Secretary of HHS before us say they don't know exactly how big it is, if it is a $4 billion a year or $10 billion or $100 billion.

The issue is, we have to find a way to track it and eliminate it and prevent it from occurring because pay and chase doesn't work. So

what you are saying is you all have the items that are necessary.

I yield back, Mr. Chairman.

RPTS MCCONNELL

DCMN HOFSTAD

[12:05 p.m.]

Mr. Pitts. The chair thanks the gentlelady.

I ask unanimous consent that Congresswoman Christensen and Congressman McKinley be allowed to address our witnesses for 5 minutes.

Without objection, so ordered.

Dr. Christensen, you are recognized for 5 minutes for questions.

Dr. Christensen. Thank you, Mr. Chairman. And, again, thank you and thank the ranking member for allowing me to sit in on this hearing.

And thank the panelists for being here.

Mr. Saccoccio, one of the points you raised in your testimony is that information-sharing -- and others did, too -- and cooperation among all players of health care is critical. And you spoke about collaboration between HHS, I guess, and DOJ.

But could you talk a little about the current information-sharing that might be taking place between private and public sector and what more could be done? And any specific examples you might have of how that public-private partnership and sharing of information has led to some success in cracking down on fraud?

Mr. Saccoccio. Yeah, as I mentioned in my testimony, information-sharing is critical between the public and private sides. You have a healthcare system where you have multiple, multiple payers.

None of them get a complete view of everything that is happening out there. Therefore, it is incredibly important that they share information.

Some of the things that are happening right now, my organization, NHCAA, our members consist of health plans, about 90 health insurers, but we also partner with the public side, as well. So the CMS, the IG's office at HHS, the FBI, they all participate with us. And the things that we do, we actually have meetings where everyone sits around a table and talks about what they are seeing, what the emerging schemes are, what the emerging trends are, so that you could take that information back and look at your own data and your own plan. So that is happening.

We have a database of investigations so that if a private insurer, say, WellPoint, opens an investigation and puts that information into the database, that information is available not only to other health plans but also to law enforcement, FBI. So that kind of information is being shared.

We also have a process by which if there is an open investigation that, say, the FBI is conducting and they want to know whether there was any private exposure on the private side for private health plans, they can query us, and we go out to the private side members to see what kind of exposure there may be.

So those types of things are happening.

What I see with this Health Care Fraud Prevention Partnership, I think that allows us to potentially take it to the next level, where

you could actually have data exchanges, data analysis done, where private health plans could take a look at their data, the government could take a look at their data, say, in Medicare fee for service and Medicaid, and on particular topics come together and share that data to see what each payer is seeing so that you can anticipate that.

A good example of this was, back in 2010, we had an information-sharing meeting at NHCAA that we hosted in Florida, where we had the FBI, the inspector general's office at HHS, local law enforcement, private payers, all came together to discussion the infusion therapy fraud in south Florida. And based on that, the private insurers found out that they had about a half a billion dollars of exposure from infusion therapy fraud just based on the information that they were able to obtain from CMS and vice versa.

So it is incredibly important in the environment that we have that, as information comes out from the various data analytics that different companies use and that CMS may be using, that as they see different things, that they share those with the other payers so that they can go back and see what kind of exposure they may have.

Dr. Christensen. Thank you.

Dr. Fu, we had at least two testimonies about smart cards, and we can see that they would provide protection. But one of the problems that was noticed in a National Health Law Program fact sheet was that they can also be a barrier to access and perhaps, this article suggested, that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining the cards and,

therefore, the benefits, rather than from preventing fraud.

So my question to you is, do you think in these pilot programs this is another factor that should be included in assessing --

Mr. Fu. I do think a pilot program should look at both -- or not only the benefits, but also the risks, including the clinical care and potential patients who may not receive the care they would have otherwise had.

Dr. Christensen. Thank you. And --

Mr. Pattinson. If I could comment, the fact that they have the card or not today, in terms of their care, it shouldn't detract in any way or make it any different to what we would have if we did a smart card implementation. The patient should always be getting their care and not have any negative effect.

So I don't see any difference between what we do today as well as what we could do with a smart card. You are not going to get denied service. We are just trying here to stop the fraud.

Dr. Christensen. It is just the hurdles that they have to go through to get the card. And for a person that might be disabled, poor, poorly educated, there are barriers there for them to really access the card and, therefore, the benefits.

Mr. Pattinson. I am sure you have a good point, Congresswoman. The fact that the ATM cards and everything, they are using bank cards today, debit cards, credit cards -- this is nothing more than a card and a PIN. And, yes, there will be instances where PINs are hard for those to manage, and in that case we need to have the right policy and

the right part of the pilot to work out how to correct those situations.

Dr. Christensen. That was the point of my question, that it should be a part of the pilot so that we could make sure that, while they provide the security, they don't increase the barriers. Thank you.

Thank you, Mr. Chairman.

Mr. Pitts. The chair thanks the gentlelady.

That concludes round one. We will go to one follow-up per side.

Dr. Burgess, you are recognized for 5 minutes for a follow-up.

Dr. Burgess. I thank the chairman for the recognition.

Ms. King, let me just ask you. You guys have done some extensive study on the fraud prevention system at CMS, and you have prepared a report. Can you give us an idea of what is the number of fraudulent claims that have been stopped dead in their tracks by this fraud-prevention system?

Ms. King. Not exactly. I can't, sir. But, you know --

Dr. Burgess. Well, let me ask you this: Has there been one instance where a claimed dollar didn't go out the door because of this fraud-prevention system?

Ms. King. I don't believe that they are stopping payments yet before.

And I think the way the system was designed, it was not intended to be an automatic stopping of payments in most cases. The way it is designed is that it flags problematic claims and problematic payments so that then those things are investigated to determine whether they

appear to be fraudulent.

Dr. Burgess. Your answer is not giving me -- I mean, I talked about the Elysian Fields and the problems that are ahead. You are not giving me a great deal of confidence that the dollars aren't going to fly out the door at an even faster rate and end up in places where they shouldn't be.

Now, one of the things I have talked about before and I mentioned in my opening statement, do you think there are a sufficient number of Federal prosecutors to be able to bring the prosecutorial case for fraud when it is discovered?

Ms. King. We are currently in the process of evaluating the use of the healthcare control account which provides funds to DOJ, the FBI, and the OIG. So we will be in a better position to evaluate that later this year.

Dr. Burgess. And once again, you are not giving me a great deal of confidence here.

You know, when I send one of my staff members with my personal credit card down to Chick-fil-A to buy lunch for the office, I get a call back that says, Hey, your card is being used to charge $100 worth of Chick-fil-A here; is that okay with you? Why can't it work that way in the CMS world?

Ms. King. You mean that there is an automatic response?

Dr. Burgess. Yeah. When something appears out of the ordinary. "This isn't something that we normally see in the conduct of your business day, Doctor. Here is some evidence that may be of interest

to you." And I say, "No, no, it is fine. You let them go ahead and have the Chick-fil-A." But why is it so hard in your world, or CMS's world I should say, for that to happen?

Ms. King. I don't know the exact magnitude of the cost, but I think implementing something like that -- and I have gotten phone calls, too, from the grocery store, you know, before I have gotten home, "Did you charge this?" I think, you know, that technology is expensive.

Dr. Burgess. Apparently it is worthwhile for Visa. Because what is their fraud rate? .03 percent? And CMS's fraud rate is anybody's guess, but 10 percent or whatever it is?

Ms. King. You know, we have not been able to determine what the fraud rate is in --

Dr. Burgess. I get you.

Ms. King. -- government or private health plans.

Dr. Burgess. But I would suspect that WellPoint is not in the business of letting all of their dollars go out the door inappropriately.

Is that correct, Ms. Lavelle?

Ms. Lavelle. Yeah, that is correct.

We have two prepayment review programs going, one in New York, one out of Chicago. Just last year alone, in placing some of these providers on prepay review where we turn off their ability to file electronically, they send in medical records, we have saved $18 million, just in the New York market. So that is one of our most

aggressive and useful tools right now.

Dr. Burgess. Yeah. As a provider, I would hate that. But at the same time, when you are dealing with the problem, the magnitude that we are seeing, and you are fixing to expand it -- you know, let's be honest. The Affordable Care Act, the States that aren't going to do a State exchange, that are going to do the Federal fallback, I mean, this creates an entire new dimension for fraud, which brings up the other point.

How at WellPoint are you staying ahead -- you know, some of the stuff we heard on Homeland Security, you have to learn to think like a terrorist. How are you learning to think like a criminal who wants to defraud the healthcare system?

Ms. Lavelle. Well, we try to stay ahead with the emerging technologies. We are looking at devices, pharmaceuticals, procedures. Every week there is something new that comes out.

The providers have consultants which tell them how to bill for these things. Even though they are investigational and not covered, they get counsel on how to bill for them under conventional coding. So we are constantly looking at those devices and trying to stop a lot of them on the dime.

The providers actually advertise the new devices on their Web site and tout that they are covered by most insurers. And we have shut several of them down in the last few years.

Dr. Burgess. But to reemphasize the point, those dollars spent on that activity would be scored as administrative dollars --

Ms. Lavelle. Exactly.

Dr. Burgess. -- under the medical loss ratio. In fact, you are not going to be rewarded for doing that in the new system under the Affordable Care Act. You will be penalized to some degree for your fraud-prevention activities.

So in an odd way the Affordable Care Act is creating new opportunities for fraud and penalizing you if you decide that you are not going to pay these dollars out inappropriately. It is a recipe for fiscal disaster.

Thank you, Mr. Chairman. I will yield back my time.

Mr. Pitts. The chair thanks the gentleman and now recognizes the ranking member, Mr. Pallone, for 5 minutes for follow-up questions.

Mr. Pallone. Thank you, Mr. Chairman.

I had one question, but I wanted to clarify the record. When Dr. Gingrey mentioned that CMS had not implemented the face-to-face requirement from the Affordable Care Act, that is not correct. The face-to-face requirement for durable medical equipment was implemented in this year's physician fee schedule rule, and home health face-to-face requirements were implemented in 2011.

The other thing, I wanted to respond to Ms. Lavelle's testimony and Mr. Shimkus's stating that the medical loss ratio formula undermines fraud-fighting activities by insurers. In fact, the medical loss ratio requirement in the ACA is a critical consumer protection that has already saved consumers over a billion dollars. HHS followed the NAIC position on how to characterize the

fraud-fighting activities and provided some room for insurers in the formula.

And fraud-fighting is an administrative activity, and I don't think it should become an open-ended loophole to undermine the medical loss ratio. The formula fairly allows some moneys to be deducted from the administrative side of the formula but balances that against undermining this important consumer protection, in my opinion.

I wanted to ask Dr. Fu, I have this article that discusses students at Cambridge University in England, and it finds -- basically what they did is they crashed the chip and PIN system. Have you seen this before?

Mr. Fu. I am not familiar with that particular article, but I am familiar with the work.

Mr. Pallone. Yeah. So, I mean, if this is happening with the secure card now, isn't there a danger of that in Medicare? I mean, how do we -- you know, I know it is Cambridge and they are smart, but isn't there the same risk?

Mr. Fu. Well, I think these -- you cannot underplay the risks. There will inevitably be problems in any technology. But one thing for sure, it is not a silver bullet. And, in particular, there can be some vulnerabilities in the software associated with interfacing with readers.

Mr. Pallone. And, Mr. Pattinson, since I brought this up, I should give you an opportunity to comment on that, too, if you want. I noticed the British accent, so maybe you are familiar with Cambridge and what is going on there.

Mr. Pattinson. Well, I am an American citizen, Congressman, but, yes, that is my roots.

I would say that in all these instances that you find it is not the card technology that has been compromised, it is the system that it has been involved in. And with the good offices of good security professionals like Dr. Fu, we often engage these people at Cambridge ourselves and hire them to actually try and attack our systems. And on that basis we can make better improvements for the future rollouts.

So for any Medicare pilot and potential rollout, we would ensure that we have all of the lessons learned from these other situations where the systems have become and are identified as vulnerable and make sure that we implement the technology which is the best for this Medicare program and, therefore, the best for sustaining the longevity of this benefit program.

Mr. Pallone. All right. Thank you very much.

Thank you, Mr. Chairman. I yield back.

Mr. Pitts. The chair thanks the gentleman.

That concludes the testimony. If Members have questions for the witnesses, I ask that the witnesses respond to the questions promptly. I remind Members that they have 10 business days to submit questions for the record. Members should submit their questions by the close of business on Wednesday, December the 12th.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Pitts. Excellent hearing. Thank you very much for your testimony.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:12 p.m., the subcommittee was adjourned.]