THE USE OF DATA TO STOP MEDICARE FRAUD

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MARCH 24, 2015

Serial No. 114–OS02

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PUBLISHING OFFICE

21–375 WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS

PAUL RYAN, Wisconsin, *Chairman*

SAM JOHNSON, Texas
KEVIN BRADY, Texas
DEVIN NUNES, California
PATRICK J. TIBERI, Ohio
DAVID G. REICHERT, Washington
CHARLES W. BOUSTANY, JR., Louisiana
PETER J. ROSKAM, Illinois
TOM PRICE, Georgia
VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
AARON SCHOCK, Illinois
LYNN JENKINS, Kansas
ERIK PAULSEN, Minnesota
KENNY MARCHANT, Texas
DIANE BLACK, Tennessee
TOM REED, New York
TODD YOUNG, Indiana
MIKE KELLY, Pennsylvania
JIM RENACCI, Ohio
PAT MEEHAN, Pennsylvania
KRISTI NOEM, South Dakota
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri

SANDER M. LEVIN, Michigan,
CHARLES B. RANGEL, New York
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR., New Jersey
JOSEPH CROWLEY, New York
DANNY DAVIS, Illinois
LINDA SÁNCHEZ, California

JOYCE MYER, *Staff Director*
JANICE MAYS, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON OVERSIGHT

PETER J. ROSKAM, Illinois, *Chairman*

KENNY MARCHANT, Texas
MIKE KELLY, Pennsylvania
PAT MEEHAN, Pennsylvania
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri
KRISTI NOEM, South Dakota

JOHN LEWIS, Georgia,
JOSEPH CROWLEY, New York
CHARLES B. RANGEL, New York
LLOYD DOGGETT, Texas

CONTENTS

THE USE OF DATA TO STOP MEDICARE FRAUD

TUESDAY, MARCH 24, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON OVERSIGHT,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:00 a.m., in Room B–319, Rayburn House Office Building, the Honorable Peter J. Roskam, [Chairman of the Subcommittee] presiding.

[The advisory announcing the hearing follows:]

Chairman Roskam Announces Hearing on The Use of Data to Stop Medicare Fraud

House Committee on Ways and Means Subcommittee on Oversight Chairman Peter Roskam (R-IL) today announced that the Committee on Ways and Means Subcommittee on Oversight will hold a hearing on the federal government's use of data analysis—particularly the Centers for Medicare and Medicaid Services' Fraud Prevention System (FPS)—to identify emerging trends, and stop Medicare fraud. This hearing will allow the Committee to hear from both government and non-governmental witnesses on the progress that the FPS has made and what continued efforts are under way to use data analysis in identifying and stopping fraud and waste within Medicare. The hearing will take place on Tuesday, March 24 at 10:00 AM in Room B-318 of the Rayburn House Office Building.

Oral testimony at the hearing will be from the invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

Details for Submission of Written Comments:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, http://waysandmeans.house.gov, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Tuesday, April 7, 2015**. For questions, or if you encounter technical problems, please call (202) 225-3625 or (202) 225-2610.

Formatting Requirements:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be

printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be submitted in a single document via e-mail, provided in Word format, and must not exceed a total of 10 pages. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. All submissions must include a list of all clients, persons, and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

3. Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available at http://www.waysandmeans.house.gov/.

Chairman ROSKAM. Good morning. The hearing will come to order.

And welcome to the Oversight Subcommittee hearing on the use of data to stop Medicare fraud

I think that there is an incredible opportunity, particularly this week, to think about the challenges that the health care system is feeling, and as we are working on a bipartisan basis here on Capitol Hill to think about how it is that we pay for the SGR, also known as the "doc fix," to begin to think about the amount of money that is being contemplated there, and it is really significant.

And yet the amount of fraud and waste and squandering resources on the other end suggests that if we fix the fraud side, we will have a lot more resources to figure out how it is that we can pay for these things to make these systems work better.

And so the reason that we are here today is to strengthen one of the most important Federal programs, that is, Medicare, that obviously provides necessary health care services to millions of our Nation's seniors. Every year Medicare loses billions of dollars through fraud and improper payments, and today we are going to find out what the Administration is doing to stop that.

When we first constituted this Subcommittee at the beginning of the Congress, the Ranking Member and I talked about our shared goal of working together, establishing facts and making government work better for all Americans, and today I have the unique privilege of chairing a hearing on this topic that I know my friend, Mr. Lewis, has worked on for many years, including holding hearings and producing legislation as the chairman of this very same subcommittee.

He is detailed. I think the Democratic Caucus is meeting right now, and I would ask for unanimous consent for him to have leave to give his opening statement upon his arrival.

I know I am speaking for every Member on this Committee when I say that we are extremely concerned about Medicare fraud. It remains a serious and evolving threat, and there are billions of dollars at stake, and there continues to be a lot more work to be done to get ahead of the criminals and to get it under control. So today's hearing is a continuation of the significant work that these Members in Congress have done in the past, and we are going to be taking a look at what the Administration's current effort is and ways that we can improve Medicare payment integrity.

To begin with, I just want to pause and emphasize just how big of a problem this is. Last year the Federal Government lost $124.7 billion in improper payments across 124 programs. Of that $124 billion, one program accounted for $60 billion or so, and that was Medicare.

Because the program is so large and susceptible to abuse, the Government Accountability Office has singled it out as a high risk for fraud every year since they started keeping track in 1990. Historically, CMS has used a method of payment called "pay and chase" in processing Medicare payments, first paying a charge, then later looking back to check on the validity and potentially trying to claw back the money if the payment was made improperly. As you can imagine, that strategy is not very effective.

Time and again we have seen fraudsters hustle the system for a few million dollars, shut down, pop up under a new name, and run their scam somewhere else. The Medicare program is getting outsmarted by these methods, and the proof is the unacceptably high rate of improper payments each year.

In 2010, I proposed a new approach to help CMS work smarter. Instead of "pay and chase," CMS should use the same kind of cutting edge, predictive analytics technology that private companies use successfully to look at transaction data in real time and identify potentially fraudulent charges, stopping the payment before the money goes out the door.

Credit card companies use a similar system to identify a potentially fraudulent charge and stop payment while they further investigate the claim, and the framework for that idea was later enacted as part of the Small Business Jobs Act of 2010.

The system created by CMS to incorporate data analytics to protect Medicare is called the Fraud Prevention System, or FPS. In its first year, FPS got off to a rocky start. Health and Human Services Inspector General could not even certify any of the system's results.

In the second year, ending in July 2013, the IG certified that the system had returned $1.34 for each dollar invested that year, totaling $54.2 million in savings.

The $54.2 million is significant money, but it is literally a drop in the bucket when compared to the $60 billion lost that I referenced earlier, and as it currently operates, FPS is catching less than one percent of improper payments, and I should add, CMS is still primarily relying on the "pay and chase" model to back after money that has already been paid out improperly rather than stopping improper payments on the front end.

I continue to think that the idea behind FPS is sound, but taxpayers are entitled to see the idea implemented with excellence. Each dollar we fail to secure from fraud and improper payments is a dollar that is not going into needed health care services for our seniors, and when we look around at what private companies are doing to protect the integrity of their transactions, it is clear that so far FPS is leaving a lot on the table.

For the first panel, this Subcommittee wants to hear directly from CMS and the Office of the Inspector General about how they are using FPS and other data sources to identify emerging trends in Medicare fraud. We want to know how CMS and OIG are coordinating their efforts with the Department of Justice to share data and to prosecute Medicare fraudsters.

And I will note here that regrettably we invited the Department of Justice to testify about these issues today, but they were unable to provide a witness.

On the second panel, we will hear from two witnesses who previously served in the Administration at DOJ and CMS, respectively, and we will get their insights about how the government is performing on these issues.

Another witness will tell us about how CMS and DOJ are collaborating with the private sector to address fraud issues affecting both Medicare and private insurers.

And finally, we will hear about how Visa, a private sector company, has used predictive analysis to stop fraud. Visa's global rate of fraud is six basis points, meaning 99.4 percent of the $10 trillion in payments it processes are fraud free. That is an impressive track record, and we hope to learn a thing or two from Visa.

We look forward to hearing from all of our witnesses and thank them for their time and their willingness to come today.

Now, as I said, Mr. Lewis is detained. He will be here shortly, and when he comes I will invite him to make his opening statement. And in the interim, why do we not start out? We will hear from our two government witnesses on the first panel, Dr. Shantanu Agrawal—I am sorry—from Centers for Medicare & Medicaid Services, and Gary Cantrell from the Office of the Inspector General for Health and Human Services.

Gentlemen, thank you for your time today. We have already received your written testimony, and you have five minutes. Doctor, if you would like to go ahead, you are welcome.

STATEMENT OF DR. SHANTANU AGRAWAL, DEPUTY ADMINISTRATOR AND DIRECTOR, CENTER FOR PROGRAM INTEGRITY, CENTERS FOR MEDICARE & MEDICAID SERVICES

Dr. AGRAWAL. Thank you.

Chairman Roskam, Mr. Doggett, other Members of the Committee, thank you for the invitation to discuss the Centers for Medicare & Medicaid Services' use of data in its program integrity efforts.

Mr. Chairman, we appreciate your leadership on these issues and your ongoing interest in making sure CMS has the tools and resources necessary to best use data to fight fraud in Medicare. Enhancing program integrity is a top priority for this Administration and an agency-wide effort at CMS.

Since passage of the Affordable Care Act and other critical legislation, CMS' Center for Program Integrity has become increasingly data oriented, using data in a variety of ways to inform our efforts to identify waste, abuse and fraud. CMS is using a number of tools, including innovative data analytics to keep bad actors out of our programs and to uncover vulnerabilities, schemes, and trends quickly before they drain valuable resources from our trust funds.

We have seen important successes from these efforts, and today I would like to highlight two critical ways we use data to identify and prevent waste, fraud and abuse: the Fraud Prevention System and our provider screening processes. Through both of these efforts, CMS is using data to stop issues on the front end and make important strides towards prevention.

Since 2011, CMS has been using its Fraud Prevention System to apply advanced analytics on all Medicare fee for service claims on a streaming national basis by using predictive algorithms and other sophisticated analytics to analyze every Medicare fee for service claim against billing patterns.

The system also incorporates other data sources, importantly, including information on compromised Medicare cards and complaints made through 1–800–Medicare. When FPS models identify egregious, suspect or aberrant activity, the system automatically generates and prioritizes leads for review and investigation by CMS' Zone Program Integrity Contractors, or ZPICs. CMS can use this information to swiftly take actions and stop problematic behaviors.

The FPS has demonstrated an impressive return on investment of five-to-one. In its second year of operation, the Department of Health and Human Services' Office of Inspector General certified CMS' identified savings of more than $210 million in improper Medicare fee for service payments, double the previous year.

These savings are the outcomes of activities, such as revocations of provider billing privileges; the implementation of payment edits; the suspension of payments; and changes in behavior that result from CMS actions.

In addition to saving taxpayer dollars through FPS, CMS has significantly strengthened provider enrollment. CMS now uses a risk-based approach to verify the legitimacy of new or existing Medicare providers by screening those that pose the highest risk to the program, including newly enrolling home health agencies and durable medical equipment companies.

A combination of routine data checks of licensure and criminal records, scheduled and unscheduled site visits—and if anybody is wondering, the unscheduled visits work better—and fingerprinting is used to confirm the validity of providers and suppliers. CMS routinely revokes billing privileges from enrolled providers and suppliers based on the Social Security Administration's complete death master file and CMS' repository of information contained in the OIG's exclusion list, and the Medicare exclusion database.

As a result, we have removed nearly 500,000 Medicare enrollments, which stops these providers from billing the program, and denied thousands of enrollment applications, which means these providers never gained the ability to bill the Medicare program.

In the coming months we will continue our work to transition as many of these data checks into a largely automated process, which improves the efficiency of provider screening while lowering burden on legitimate actors.

While data is a critical part of our work, Medicare fraud, waste and abuse will not be stopped with data alone. The true power of data analytics comes from using results to guide human interventions. Data helps CMS generate leads and take appropriate administrative actions.

Medicare fraud, waste and abuse affects every American by draining critical resources from taxpayers and our health care system. Our health care system should offer the highest quality and most appropriate care possible to ensure the well-being of individuals and populations. CMS is committed to protecting taxpayer dollars by preventing or recovering payments for wasteful, abusing or fraudulent services.

But the importance of program integrity extends far beyond dollars and health care costs alone. It is fundamentally about protecting our beneficiaries and ensuring we have the resources to provide for their care. Although we have made significant progress in stopping fraud and improper payments, more work remains to be done.

I look forward to working with you and the Congress to fully utilize our data analytic systems to protect the integrity of our health care programs and safeguard taxpayer resources.

Thank you.

Chairman ROSKAM. Thank you, Doctor.

[The prepared statement of Dr. Agrawal follows:]

STATEMENT OF

SHANTANU AGRAWAL, M.D.
DEPUTY ADMINISTRATOR AND DIRECTOR,
CENTER FOR PROGRAM INTEGRITY
CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

"THE USE OF DATA TO STOP MEDICARE FRAUD"

BEFORE THE
UNITED STATES HOUSE WAYS & MEANS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT

MARCH 24, 2015

U.S. House Ways & Means Committee
Subcommittee on Oversight
Hearing on
"The Use of Data to Stop Medicare Fraud"
March 24, 2015

Chairman Roskam, Ranking Member Lewis, and members of the Subcommittee, thank you for the invitation to discuss the Centers for Medicare & Medicaid Services' (CMS) program integrity efforts. Enhancing program integrity is a top priority for the Administration and an agency-wide effort at CMS. We have made important strides in reducing fraud, waste, and abuse across our programs and I appreciate the opportunity to discuss CMS' program integrity activities.

Thanks in part to the authorities and resources provided by the Affordable Care Act and the Small Business Jobs Act of 2010, CMS has powerful tools to improve our efforts to detect and prevent fraud, waste, and abuse in Medicare. The fundamental change in the Administration's approach to fraud-fighting is a stronger focus on prevention. Historically, CMS and our law enforcement partners have been dependent upon "pay and chase" activities, by working to identify and recoup fraudulent payments after claims were paid. Now, CMS is using a variety of tools, including innovative data analytics, to keep fraudsters out of our programs and to uncover fraudulent schemes and trends quickly before they drain valuable resources from our Trust Funds.

Our efforts in Medicare and Medicaid strike an important balance: protecting beneficiary access to necessary health care services and reducing the administrative burden on legitimate providers and suppliers, while ensuring that taxpayer dollars are not lost to fraud, waste, and abuse. Fraud can inflict real harm on beneficiaries. When fraudulent providers steal a beneficiary's identity and bill for services or goods never received, the beneficiary may later have difficulty accessing needed and legitimate care. Beneficiaries are at risk when fraudulent providers perform medically unnecessary tests, treatments, procedures, or surgeries, or prescribe dangerous drugs without thorough examinations or medical necessity. When we prevent fraud, we ensure that beneficiaries are less exposed to risks and harm from fraudulent providers, and are provided with

improved access to quality health care from legitimate providers while preserving Trust Fund dollars.

We have seen important success from these efforts. CMS is using a multi-faceted approach to strengthen Medicare by more closely aligning payments with the costs of providing care, encouraging health care providers to deliver better care and better outcomes for their patients, and improving access to care for beneficiaries. We have instituted many program improvements and are continuously looking for ways to refine and improve our program integrity activities.

In addition to CMS' ongoing program integrity efforts, the President's Fiscal Year (FY) 2016 Budget reflects the Administration's commitment to strong program integrity initiatives. Together the program integrity investments in the Budget will yield $21.7 billion in savings for Medicare and Medicaid over 10 years. The Budget also includes 16 legislative proposals that provide additional tools to further enhance program integrity efforts in the Medicare and Medicaid programs. In addition, to better protect seniors and the Medicare program against the risks associated with identity theft,[1] the Budget proposes $50 million in FY 2016 to support the removal of Social Security Numbers from Medicare cards so that millions of beneficiaries will no longer have to fear that their personal identification numbers could be used against them due to a lost, stolen, or misused Medicare card.

Using Data to Identify New Trends in Fraud and Enhance Prevention

CMS is working to achieve operational excellence in addressing the full spectrum of program integrity issues, in taking swift administrative actions, and in the performance of audits, investigations and payment oversight. To support these efforts, CMS is launching an improved contracting approach, the Unified Program Integrity Contractors (UPIC) to integrate the program integrity functions for audits and investigations across Medicare and Medicaid from work currently performed by several existing contractors.

[1] MEDICARE INFORMATION TECHNOLOGY: Centers for Medicare and Medicaid Services Needs to Pursue a Solution for Removing Social Security Numbers from Cards. GAO-13-761: Published: Sep 10, 2013. Publicly Released: Oct 17, 2013.

Strengthening Provider Enrollment

Provider enrollment is the gateway to billing within the Medicare program, and CMS has put critical safeguards in place to make sure that only legitimate providers and suppliers are enrolling in the Medicare program. This enhanced screening requires certain categories of providers and suppliers that have historically posed a higher risk of fraud to undergo greater scrutiny prior to their enrollment or revalidation in Medicare. All Medicare providers and suppliers undergo a baseline screening, including confirmation of the provider's Social Security Number through the Social Security Administration, license and certification through the state licensing boards, as well as searches in the System for Award Management, operated by the General Services Administration (GSA), in terms of Government contracting exclusion (suspension and debarments) and the Health and Human Services (HHS) Office of Inspector General (OIG) exclusion list for all individuals listed on the application.

Under section 1128 of the Social Security Act, the Secretary, through HHS OIG, must exclude individuals and entities from Federal health care programs based on felony or misdemeanor convictions related to the Medicare or Medicaid programs, or related to the abuse or neglect of patients, and has discretionary authority to exclude individuals on a number of grounds, including misdemeanor convictions related to health care fraud. CMS routinely revokes billing privileges from enrolled providers and suppliers based on the Social Security Administration's complete death master file and CMS' repository of information contained in the OIG's exclusion list, the Medicare Exclusion Database (MED). Revocations are retroactive to the date of a provider's respective plea or conviction, and if the provider or supplier submitted claims after that date, CMS demands those payments be repaid.

CMS has historically relied on the MED and GSA list to identify relevant felony convictions because there is not a centralized or automated means of obtaining felony convictions of Medicare providers and suppliers. CMS is currently working on a process to match enrollment data against public and private databases to receive timely felony conviction data. Additionally, beginning in September 2014 and on a phased-in basis, providers and suppliers who were designated to the high screening level must also undergo a fingerprint-based criminal history check to gain or maintain billing privileges for Medicare. The requirement applies to individuals

with a five percent or greater ownership interest in a newly-enrolling durable medical equipment, prosthetics, orthotics and supplies (DMEPOS) supplier or a newly-enrolling home health agency (HHA), as well as any provider that has been subject to certain adverse actions, including prior revocation, payment suspension, or licensure suspension or revocation.

State Medicaid agencies are required to terminate the enrollment of any provider that has been terminated by Medicare or another state Medicaid program for cause. Additionally, CMS has the discretionary authority to revoke Medicare billing privileges where a state has terminated or revoked a provider's or supplier's Medicaid billing privileges. CMS established a process for states to report and share information about Medicaid termination. States have been instructed to report all "for cause" Medicaid terminations, for which state appeal rights have been exhausted, to CMS by submitting a copy of the original termination letter sent to the provider, along with specific provider identifiers, and the reason for Medicaid termination. CMS has revoked 290 Medicare providers based on this information. This prevents bad actors from jumping from program to program.

Revalidation of existing Medicare providers

The Affordable Care Act required CMS to revalidate all 1.5 million existing Medicare providers and suppliers under new risk-based screening requirements. CMS is on track to request the revalidation of all providers and suppliers by the end of this month. Since March 25, 2011, more than one million providers and suppliers have been subject to the new screening requirements, over 470,000 provider and supplier practice locations had their billing privileges deactivated as a result of revalidation and other screening efforts, and almost 28,000 provider and supplier enrollments were revoked.[2]

CMS continues to make improvements in its oversight of provider enrollment. In December 2014, CMS issued a Final Rule that permits revocation of providers or suppliers that demonstrate patterns or practices of abusive billing, permits CMS to deny the enrollment of providers, suppliers, or owners affiliated with an entity that has unpaid debt to the Medicare

[2] Deactivated providers could reactivate over time with updated practice information or after showing evidence of proper licensing.

program, and expands the list of felony convictions that could prevent a provider or supplier from participating in Medicare.

Enrollment Moratoria

The Affordable Care Act provides the Secretary the authority to impose a temporary moratorium on the enrollment of new Medicare, Medicaid, or Children's Health Insurance Program (CHIP) providers and suppliers, including categories of providers and suppliers, if the Secretary determines the moratorium is necessary to prevent or combat fraud, waste, or abuse under these programs. States affected are required to determine whether the imposition of a moratorium would adversely affect Medicaid beneficiaries' access to medical assistance and are not required to comply with the moratorium if there would be an adverse effect. When a moratorium is imposed, existing providers and suppliers may continue to deliver and bill for services, but no new applications will be approved for the designated provider or supplier-types in the designated areas. The moratoria enable CMS to pause provider entry or re-entry into markets that CMS has determined have a significant potential for fraud, waste or abuse while working with law enforcement to use other tools and authorities to remove bad actors from the program.

In July 2013, CMS announced temporary moratoria on new HHAs in and around Miami and Chicago, and ground-based ambulances in and around Houston. In January 2014, CMS announced new temporary moratoria on the enrollment of HHAs in Fort Lauderdale, Detroit, Dallas, and Houston, and on ground ambulances in Philadelphia. CMS is required to re-evaluate the need for such moratoria every six months and on January 29, 2015, CMS extended these existing moratoria for an additional six months. In each moratorium area, CMS is taking administrative actions such as payment suspensions and revocations of billing privileges of HHAs and ambulance companies, as well as working with law enforcement to support investigations and prosecutions.

Fraud Prevention System

CMS is leading the government and healthcare industry in systematically applying advanced analytics to claims on a nationwide scale. Since 2011, CMS has been using its Fraud Prevention System (FPS) to apply advanced analytics on all Medicare fee-for-service claims on a streaming,

national basis by using predictive algorithms and other sophisticated analytics to analyze every Medicare fee-for-service claim against billing patterns. The system also incorporates other data sources, including information on compromised Medicare cards and complaints made through 1-800-MEDICARE. When FPS models identify egregious, suspect, or aberrant activity, the system automatically generates and prioritizes leads for review and investigation by CMS' Zone Program Integrity Contractors (ZPICs). The ZPICs then identify administrative actions that can be implemented swiftly, such as revocation, payment suspension, or prepayment review, as appropriate. The FPS is also an important management tool, as it prioritizes leads for ZPICs in their designated region, making our program integrity strategy more data-driven.

The Small Business Jobs Act requires the OIG to certify the projected and actual savings from the FPS, and also to determine whether CMS should continue, modify or expand the use of the FPS. Since the implementation of the FPS, CMS has demonstrated a positive return on its investment and the OIG found that CMS' ongoing use of the FPS will strengthen efforts to prevent fraud, waste and abuse in the Medicare fee-for-service program. In its second year of operation, the OIG certified CMS' identified and adjusted savings, and the FPS identified or prevented more than $210 million in improper Medicare fee-for-service payments, double the previous year. It also resulted in CMS taking action against 938 providers and suppliers. These savings are the outcome of activities such as revocations of provider billing privileges, the implementation of payment edits, the suspension of payments, and changes in behavior that result from CMS actions.

CMS is also piloting the use of the tool with the MACs to see if they can change aberrant billing behavior by directly contacting providers flagged in the FPS. Based on the small pilot, CMS has seen changes in billing behavior in half of the providers contacted within one month, and of the remaining, additional actions were taken, including self-audit and prepayment review. Another value of expanding the use of the FPS tool is that the MAC and ZPIC may be able to better coordinate audit activity on a specific provider in the same system, reducing burden on the provider and providing a forum for collaboration between contractors.

One of the most important advances FPS brings to CMS' fraud identification capabilities is that the FPS is uniquely capable of evaluating claims for episodes of care that span multiple legacy claims processing systems as well as those that span multiple visits over a period of time. What this means is that FPS can identify billing patterns and claim aberrancies that would be undetectable or difficult to detect by CMS' current claim edit modules or a single contractor reviewing on a claim by claim basis. In addition, FPS now has the capability to stop payment of certain improper and non-payable claims by communicating a denial message to the claims payment system. As recommended by the Government Accountability Office (GAO), CMS successfully enhanced the integration of the FPS and the claims processing system during the second implementation year.[3]

Leadership and coordination across the health care system

CMS remains committed to identifying and taking timely, appropriate action against emerging forms of fraud, waste, and abuse. Prescription drug abuse is a quickly growing problem that has touched providers, pharmacies, and beneficiaries in the Part D program. While the Part D program is strong, CMS knows it must continually improve the program and address vulnerabilities. Based on input from the HHS OIG, GAO, and stakeholders, over the past several years, CMS has broadened its initial focus of strengthening beneficiary access to prescribed drugs to also address fraud and drug abuse by making sure Part D sponsors implement effective safeguards and provide coverage for drug therapies that meet safety and efficacy standards. CMS is coordinating a variety of efforts with Federal and state partners, as well as the private sector to better share information to combat fraud. CMS enhanced its data analysis and improved coordination with law enforcement to get a more comprehensive view of activities in Medicare Advantage and Part D. CMS issued compliance program guidelines to assist Medicare Advantage plans and prescription drug plans in designing and implementing a comprehensive plan to detect, correct and prevent fraud, waste and abuse.

CMS also contracts with the Medicare Drug Integrity Contractor (MEDIC), which is charged with identifying and investigating potential fraud and abuse, and developing cases for referral to

[3] Government Accountability Office Report, "CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness." (GAO-13-104) See http://www.gao.gov/assets/650/649537.pdf.

law enforcement agencies. In September 2013, CMS directed the MEDIC to increase its focus on proactive data analysis in Part D. As a result, the MEDIC identified vulnerabilities and then performed analysis that resulted in notification to plan sponsors to remove records associated with inaccurate data leading to improper payments made in FYs 2011 and 2012. This increased focus on proactive analysis resulted in savings of $4.8 million from decreased provider payments, $21 million for unallowable charges for medications during a hospice stay, and $80 million for Transmucosal Immediate Release Fentanyl drugs without a medically-acceptable indication.

CMS also issued a Final Rule that both establishes a new revocation authority for abusive prescribing patterns and requires prescribers of Part D drugs to enroll in Medicare or have a valid opt-out affidavit on file. Additionally, CMS may now also revoke a prescriber's Medicare enrollment if his or her Drug Enforcement Administration (DEA) Certificate of Registration is suspended or revoked, or the applicable licensing or administrative body for any State in which a physician or eligible professional practices has suspended or revoked the physician or eligible professional's ability to prescribe drugs.

The President's FY 2016 Budget includes a proposal to give the Secretary the authority to establish a requirement that high-risk Medicare beneficiaries only use certain prescribers and/or pharmacies to obtain controlled substance prescriptions, similar to many state Medicaid programs. Currently, CMS requires Part D sponsors to conduct drug utilization reviews, which assess the prescriptions filled by a particular enrollee. These efforts can identify overutilization that results from inappropriate or even illegal activity by an enrollee, prescriber, or pharmacy. However, CMS' statutory authorities to take preventive measures in response to this information presently are limited. Under the President's FY 2016 Budget proposal, the Medicare program would be required to ensure that beneficiaries retain reasonable access to needed medication.

Collaborating with law enforcement and the private sector

Since its inception in 1997, the waste, abuse, and fraud prevention and enforcement efforts in the Health Care Fraud and Abuse Control (HCFAC) program resulted in the recovery of $27.8

billion in taxpayer dollars from individuals trying to defraud Federal health care programs serving seniors and taxpayers. Over the last three years, the average return on investment (ROI) of the HCFAC program is $7.70 for every dollar spent, which is an $2 higher than the average ROI for the life of the HCFAC program.

CMS is committed to working with our law enforcement partners, who take a lead role in investigating and prosecuting alleged fraud. CMS provides support and resources to the Strike Forces, which investigate and track down individuals and entities defrauding Medicare and other government health care programs. Since 2006, CMS has been building the Integrated Data Repository (IDR), a data warehouse to integrate Medicare and Medicaid data so CMS and our partners can access data from a single source. The IDR provides a comprehensive view of Medicare and Medicaid data including claims, beneficiary, and drug information. The IDR provides greater information sharing, broader and easier access to data, enhanced data integration, and increased security and privacy of data, while strengthening our analytical capabilities. The IDR makes fraud prevention and detection efforts more effective by eliminating duplicative efforts. CMS has been working closely with law enforcement to provide training and support in the use of One PI for their needs.

Importantly, these joint efforts have also led to a measurable decrease in expenditures in areas of focus. For example, there has been a dramatic decline in payment for home health care in Miami and throughout Florida. In 2009, claims to Medicare for home health services in Florida were $3.4 billion, and Medicare paid approximately $2.9 billion for home health care services. Just two years later, in 2011, billings to Medicare had dropped to $2.3 billion, a difference of $1.1 billion.

Healthcare Fraud Prevention Partnership

In July 2012, the Secretary of HHS and the Attorney General announced a historic partnership with the private sector to fight fraud, waste, and abuse across the health care system. The ultimate goal of the Healthcare Fraud Prevention Partnership (HFPP) is to exchange facts and information to identify trends and patterns that will uncover fraud, waste and abuse that could not otherwise be identified. The HFPP currently has 38 partner organizations from the public

and private sectors, law enforcement, and other organizations combatting fraud, waste, and abuse. We are continuing to grow strategically by adding new partners and identifying additional overlapping fraud schemes. The HFPP has completed the following four studies to date – Misused Codes and Fraud Schemes, Non-Operational Providers (or "false store fronts"), Revoked and Terminated Providers, and Top-Billing and High Risk Pharmacies – that have enabled partners, including CMS, to take substantive actions to stop payments from going out the door. The HFPP is now in the process of launching three new studies based on successful identification of continuing challenges faced by current and new members.

The President's FY 2016 Budget proposal includes additional support for the HFPP collaboration. The proposal would give CMS the authority to accept gifts made to the Trust Funds for particular activities funded through the Health Care Fraud and Abuse Control Account, including the HFPP. Currently, the account can only receive gifts that are made for an unspecified purpose. This proposal would allow for gifts to be made to support the HFPP directly, and allow both public and private partners to support the anti-fraud program.

Moving Forward

Medicare fraud, waste, and abuse affect every American by draining critical resources from taxpayers and our health care system. Our health care system should offer the highest quality and most appropriate care possible to ensure the well-being of individuals and populations. CMS is committed to protecting taxpayer dollars by preventing or recovering payments for wasteful, abusive, or fraudulent services. But the importance of program integrity efforts extends beyond dollars and health care cost alone. It is fundamentally about protecting our beneficiaries – our patients – and ensuring we have the resources to provide for their care. Although we have made significant progress in stopping fraud and improper payments, more work remains to be done.

Going forward, we must continue our efforts to move beyond "pay and chase" to prevent and identify trends in fraud before it happens, provide leadership and coordination to address these issues across the health care system, and ensure that we take appropriate administrative action as swiftly as possible to stop suspected instances of waste, fraud, and abuse. I look forward to

working with you and the Congress to protect the integrity of our health care programs and safeguarding taxpayer resources.

Chairman ROSKAM. Mr. Cantrell.

STATEMENT OF GARY CANTRELL, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. CANTRELL. Good morning, Mr. Chairman and other distinguished Members of the Committee. I am Gary Cantrell, Deputy IG for Investigations at OIG. Thank you for the opportunity to testify about OIG's efforts to fight fraud, waste and abuse in Medicare.

OIG utilizes a range of tools in this fight, including audits, evaluations, investigations, enforcement authorities, and educational outreach. Combining data analytics with field intelligence, we identify areas most vulnerable to fraud and deploy our resources to ensure the greatest impact from our work.

OIG works closely with the Department of Justice, CMS, and other Federal and State law enforcement partners to bring those who commit fraud against our programs to justice. Our Medicare Fraud Strike Force Team is located in nine cities throughout the country to exemplify this approach.

The OIG and our partners are committed to fighting and preventing fraud, waste and abuse. Our efforts have produced some impressive results. In 2014, our work resulted in record numbers of criminal convictions, civil actions, and program exclusions, and since 1997, we have recovered more than $276 billion for the trust fund. Our return on investment is $7.70 for every dollar spent.

Perhaps even more important, we are seeing strong indicators of a deterrent effect. When we work together to shed light on a program vulnerability, put criminals behind bars, and take appropriate administrative actions, we have the greatest impact, and our analysis reveals significant declines in Medicare payments across several program areas in Strike Force cities where we have focused our efforts.

For example, following Federal enforcement and oversight activities, there have been sustained declines in Medicare payments for durable medical equipment, home health, ambulance, and community mental health centers, or CMHCs. Nationwide, Medicare payments for CMHCs have decreased approximately $250 million annually, and total Medicare payments for ambulance services in Houston are down approximately 40 percent.

In the Miami area, DME payments have decreased by approximately $100 million annually since the launch of the Strike Force, and since 2010, home health payments have decreased nationally more than $1 billion annually.

Despite these successes, more needs to be done. Fraud schemes are constantly evolving and migrating, and some of OIG's top oversight priorities include the rise in prescription drug fraud and schemes involving home-base care.

It is also critical that we protect beneficiaries from harm related to these health care fraud schemes. Rarely are these schemes perpetrated by one provider operating independently. There is often a network of individuals, including business owners, patient recruiters, health care practitioners and sometimes even the patient. Kickbacks in the form of cash or drugs often bind these networks together.

Identity theft is a national problem, and the theft of patient and provider data underpins many of our cases. Removing Social Security numbers from the Medicare card could also protect patient data and disrupt fraud schemes.

Annual Medicare spending is approaching $600 billion. An estimated 10,000 individuals become newly eligible for Medicare every day, and Medicare prescription drug spending alone is projected to rise by $100 billion over the next ten years. As the program continues to grow and evolve, the need to protect the Medicare program and the beneficiaries it serves from fraud has never been more important.

OIG working with our partners will continue using data analytics to target our resources for maximum results, and full funding of the 2016 budget for OIG will enable us to continue our vigorous oversight efforts and further protect programs, beneficiaries, and taxpayers.

And we would like to express our appreciation for Congress' sustained commitment and support for our mission and appreciate the Committee's interest in this vital issue of protecting the Medicare program from fraud.

Thank you for the opportunity to speak today, and I would be happy to answer any questions.

Chairman ROSKAM. Thank you, Mr. Cantrell.

[The prepared statement of Mr. Cantrell follows:]

Testimony Before the United States House of Representatives
Committee on Ways and Means:
Subcommittee on Oversight

"Fraud in Medicare"

Testimony of:

Gary Cantrell
Deputy Inspector General for Investigations
Office of Investigations
Office of Inspector General
U.S. Department of Health and Human Services

March 24, 2015
10 a.m.
Location: Rayburn House Office Building, Room B-318

Testimony of:
Gary Cantrell
Deputy Inspector General for Investigations
U.S. Department of Health and Human Services, Office of Inspector General

Good morning Chairman Roskam, Ranking Member Lewis, and other distinguished members of the Oversight Subcommittee. I am Gary Cantrell, Deputy Inspector General for Investigations for the Office of Inspector General (OIG), U.S. Department of Health and Human Services (HHS). I appreciate the opportunity to testify about OIG's efforts to combat Medicare fraud, a top priority. OIG is a leader in the fight against Medicare fraud. We use data analytics to detect and investigate Medicare fraud and to target our resources for maximum results. Those results have included, for example, almost $15 billion in investigative receivables and more than 2,700 criminal actions in the past 3 years. Data-driven efforts are key to staying ahead of the evolving Medicare fraud schemes we uncover, which can involve complex criminal networks and too often cause patient harm in addition to financial loss. Our partnerships with other Government entities and the private sector are also invaluable to our enforcement successes. But we are not focused solely on enforcement. The best way to combat fraud is by preventing it in the first place, and OIG's oversight efforts support all aspects of program integrity. We also strive to cultivate a culture of compliance in the industry through various efforts, including guidance.

OIG IS A LEADER IN THE FIGHT AGAINST MEDICARE FRAUD

OIG's mission is to protect the integrity of the HHS programs and operations and the health and welfare of the people they serve. Fighting fraud in Medicare is a critical component of that mission. Medicare spending in 2013 totaled almost $583 billion, and the program served more than 52 million aged and disabled individuals.[1] Protecting those beneficiaries and the integrity of that Federal spending is paramount.

OIG advances our mission through a robust program of audits, evaluations, investigations, enforcement actions, and compliance efforts. In today's testimony, I focus on our investigation and enforcement activities, led by OIG's Office of Investigations, in collaboration with our attorneys, evaluators, auditors, and data analytics experts. The Office of Investigations is the law enforcement component of OIG and investigates fraud

[1] Data from *Medicare Trustees Report 2014*, available at http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/ReportsTrustFunds/downloads/tr2014.pdf.

and abuse against HHS programs and holds wrongdoers accountable for their actions. Our special agents have full law enforcement authority and affect a broad range of actions, including the execution of search warrants and arrests.[2] We use state-of-the art investigative techniques and innovative data analytics to fulfill our mission.

OIG investigations have produced record-setting results. During the last 3 fiscal years (FY2012-FY2014), OIG investigations have resulted in $14.8 billion in investigative receivables (dollars ordered or agreed to be paid to government programs as a result of criminal, civil, or administrative judgments or settlements); 2,709 criminal actions; 1,172 civil actions; and 10,363 program exclusions.

The return on investment for our work is significant. OIG and our HHS and Department of Justice (DOJ) partners have returned $7.70 for every $1 invested in the Health Care Fraud and Abuse Control Program (HCFAC).[3] HCFAC is OIG's largest funding source. Since HCFAC's inception in 1997, the HCFAC program activities have returned more than $27.8 billion to the Medicare Trust Fund. HCFAC's continued success confirms the soundness of a collaborative approach to identify and prosecute the most egregious instances of health care fraud, to prevent future fraud, and to protect program beneficiaries.

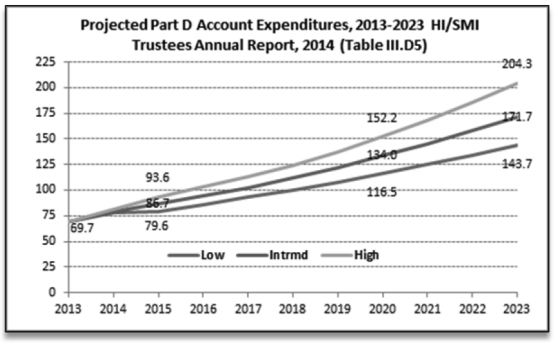
OIG USES DATA ANALYTICS TO DETECT AND INVESTIGATE MEDICARE FRAUD AND TO TARGET OUR RESOURCES FOR MAXIMUM RESULTS

OIG is a front-runner in the use of data analytics to detect and investigate health care fraud. We use innovative analytic methods to analyze billions of records and data points to identify trends that may indicate fraud, geographical hot spots, emerging schemes, and individual providers of concern. At the macro-level, we analyze data patterns to assess fraud risks across Medicare services and provider types and geographically to prioritize and deploy our resources. At the micro-level, we use data analytics, including near-real-time data, to identify fraud suspects and conduct our investigations as efficiently and effectively as possible.

Our approach to fighting prescription drug fraud provides an example. Prescription drug abuse is a serious national problem. OIG has been monitoring the growth in Medicare Part D spending for drugs, which totaled $69.7 billion in 2013 and is projected to total $171.7

[2] Inspector General Act of 1978.
[3] Data from the *FY 2014 Health Care Fraud and Abuse Control Program Report*, available at http://oig.hhs.gov/publications/docs/hcfac/FY2014-hcfac.pdf.

billion by 2023.[4] These estimates alone underscore the need for strong program integrity and enforcement efforts. However, that trend is just one consideration. We combine our field intelligence with data analytics to assess vulnerabilities across the program and to deploy our special agents to investigate the most egregious cases of suspected fraud. For example, we worked with OIG's evaluators to develop indicators of questionable billing for Part D drugs that may be associated with fraud and abuse based on our experience with prescription drug investigations. OIG evaluators designed studies using sophisticated data analytics to identify questionable billing by retail pharmacies, prescribers with aberrant patterns, individuals writing prescriptions without authority to prescribe, and Schedule II drugs billed as refills. These studies generated numerous law enforcement leads, resulting in multiple ongoing investigations. They also identified systemic vulnerabilities in the Part D program and made recommendations to CMS to better prevent fraud.



Data Analytics Have Been a Key Factor in the Success of Our Medicare Fraud Strike Force

The remarkable success of the Medicare Fraud Strike Force (Strike Force) showcases the effectiveness of our use of data analytics to detect and investigate health care fraud. Strike forces began in March of 2007. In 2009, HHS and DOJ announced the creation of the Health Care Fraud Prevention and Enforcement Action Team, a joint agency initiative known as HEAT. A key component of HEAT is Strike Force, which harnesses the efforts of OIG and

[4] The Board of Trustees Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds, *2014 Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds*, July 2014.

DOJ, including headquarters, Offices of U.S. Attorneys, and the Federal Bureau of Investigation, along with State and local law enforcement, to fight Medicare fraud in geographic hotspots. The Strike Force teams use near-real-time data to pinpoint fraud hot spots and aberrant billing as it occurs. This coordinated and data-driven approach to identifying, investigating, and prosecuting fraud has produced record breaking results. Since their inception in March 2007, Strike Force teams have charged more than 2,097 defendants who have collectively billed the Medicare program for more than $6.5 billion.[5]

HEAT actions have led to a 75 percent increase in individuals charged with criminal health care fraud during the initial stages, and the program has maintained significant enforcement success throughout its history.[6] Through HEAT, we have expanded Strike Force teams to operate in nine locations: Miami, Florida; Detroit, Michigan; southern Texas; Los Angeles, California; Tampa, Florida; Brooklyn, New York; southern Louisiana; Chicago, Illinois; and Dallas, Texas.

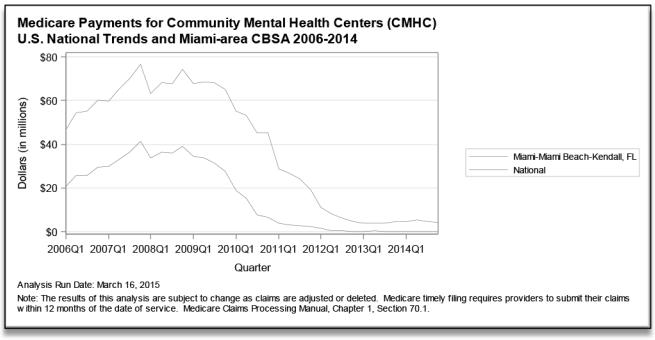
In a recent example, a national Strike Force operation in May 2014 resulted in charges against 90 individuals, including 27 doctors, nurses, and other medical professionals, for their alleged participation in multiple Medicare fraud schemes spanning many health care services. Collectively, the doctors, nurses, licensed medical professionals, health care company owners and others were charged with conspiring to submit approximately $260 million in fraudulent billings.[7] The cases are currently being prosecuted and investigated by Strike Force teams.

Our Data-Driven Approach Produces Measurable Results

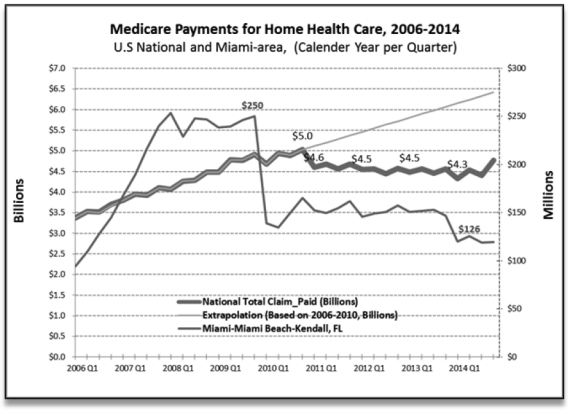
As a result of our data-driven enforcement efforts, we have seen strong and sustained declines in Medicare payments, both nationally and in specific geographical areas of increased enforcement. Our criminal prosecutions and monetary recoveries have increased, while we have seen a measurable decrease in payments for certain fraud-prone health care services. In one example, following targeted enforcement and other oversight activities, payments for Community Mental Health Centers (CMHCs) nationally decreased from $70 million to under $5 million per quarter following Federal enforcement and oversight action.

---

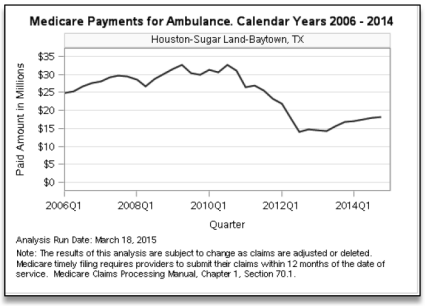
[5] Data from the FY 2014 *Health Care Fraud and Abuse Control Program Report*, available at http://oig.hhs.gov/publications/docs/hcfac/FY2014-hcfac.pdf.
[6] See *HEAT Task Force,* available at http://oig.hhs.gov/fraud/strike-force.
[7] See *Medicare Fraud Strike Force charges 90 individuals for approximately $260 million in false billing*, available at http://www.hhs.gov/news/press/2014pres/05/20140513b.html.



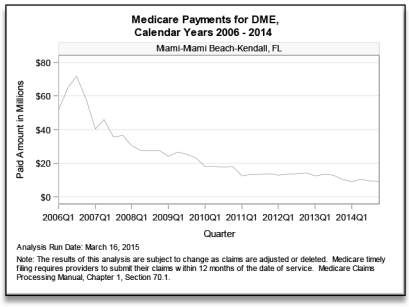
Coordination between the Strike Force teams and the Centers for Medicare & Medicaid Services (CMS) has also contributed to a dramatic decline in payment for home health care in Miami and throughout Florida. After OIG uncovered billing schemes relating to home health outlier payments, CMS put into effect a limit on the percentage of outlier payments that each home health agency (HHA) can claim. Since 2010, Medicare payments for home health care nationally decreased by more than $250 million per quarter, more than $1 billion annually.



We have also seen sustained declines in Medicare payments for durable medical equipment (DME) and ambulance services in targeted areas following Federal enforcement and oversight action. Total Medicare payments for ambulance services in Houston, one of the targeted geographic areas, are down more than 40 percent from $32 million to $18 million per quarter since 2010.



In 2007, numerous federal oversight and administrative initiatives were launched by CMS, OIG, and others, including the Medicare Fraud Strike Force. Miami-area DME payments decreased from over $40 million per quarter in 2007, before the Strike Force's first takedown, to $15 million per quarter in 2011 - with approximately $100 million in annual savings thereafter. These unprecedented results highlight our continued need for strong data analytic efforts to detect and investigate health care fraud.



MEDICARE FRAUD SCHEMES DRAIN BILLIONS OF DOLLARS AND OFTEN HARM BENEFICIARIES

Fraud Evolves and Migrates

As our health care system evolves, so do the associated fraud schemes. OIG monitors Medicare payments to detect fraud schemes through data analytics and real-time field intelligence from our agents and program integrity partners. Fraud schemes can recur over long periods of time, or emerge as new schemes develop. For example, billing for home health services that are not received is a recurring fraud scheme. By its very nature, this fraud is difficult to detect if both the patient and physician conspire with a fraudulent home health agency to bill for services that were not rendered. An emerging variation of this theme is a beneficiary who receives adult daycare services billed as home health services. Not only is the billing of these services misrepresented, but the services are neither allowed nor medically necessary.

Fraud schemes also migrate. Fraud migration can be associated with enforcement efforts, such as targeted Strike Force action; administrative efforts, such as billing edits and changes in payment policy; or simply because fraud is known to be transient. For example, increased enforcement effort in a specific geographical area may result in migration of criminals to a different geographical area to continue their criminal activity. Fraud also expands and replicates in certain geographical areas as criminals collaborate with one another. If a fraud scheme is successful and continues uninterrupted, criminals will duplicate the scheme, even if the original criminal mastermind has moved to another area. OIG and other program integrity partners diligently track fraud migration of both types and respond as needed to the constantly evolving landscape of health care fraud.

Medicare Fraud is Often Perpetrated by Complex Criminal Networks

Description of Fraud Schemes
OIG continues to investigate complex health care fraud schemes perpetrated by criminal networks. These groups take a systematic, organized approach to committing fraud and can establish hierarchies within their networks. Criminal networks have become a pervasive problem in fraud schemes involving home health, DME, prescription drugs, transportation, and medical clinic settings. Criminal networks may either solicit persons to use as business owners for a sham corporation, or may steal physician or other identities to use for billing false claims to Medicare. They often hire recruiters to buy lists of Medicare patient names and identification numbers or identify parties willing to participate in the

fraud schemes. These groups pose a huge threat to the integrity of the Medicare trust funds because their primary objective is to organize with the intent of stealing as much money from Medicare as quickly as possible.

Enforcement Action

We have worked diligently to stop criminal enterprises by strategically partnering with other law enforcement entities and DOJ. In a recent Strike Force case, an organized criminal network perpetrated a $6.2 million Medicare fraud scheme involving Miami HHAs. The owners of the HHAs solicited payments from and offered bribes to other businesses to participate in the fraudulent billings. The HHAs used patient recruiters to find complicit Medicare patients and then paid kickbacks for the use of their identities in billing Medicare for home health and therapy services that were never provided. Co-conspirators included clinic owners, therapists, and complicit Medicare beneficiaries. Two of the subjects in the case were each sentenced to serve over 5 years imprisonment, and both were ordered to pay over $6.2 million in restitution. Others are awaiting sentencing in this matter.

Our investigation of a Michigan pharmacist unraveled a sophisticated criminal enterprise. Twenty-six defendants were convicted for defrauding Medicare of nearly $58 million. A pharmacist concealed his ownership of 26 pharmacies through the use of straw-owners consisting of physicians, fellow pharmacists, and associates. The pharmacy owners offered and paid kickbacks, bribes, and other inducements to prescribers in exchange for their writing fraudulent prescriptions for Medicare patients. The leader behind the criminal enterprise was sentenced to 17 years in prison and ordered to pay $18.9 million in restitution, and 5 of his co-conspirators have been sentenced to a combined 19 years in prison and ordered to pay more than $8.4 million in restitution.

Along with our law enforcement partners and DOJ, we investigated the largest Medicare fraud scheme ever perpetrated by a single criminal enterprise successfully charged by DOJ. Armenian nationals established phantom medical clinics using stolen physician identities to submit entirely fictitious bills to Medicare. Patients did not receive treatments and doctors did not perform services in these "phantom clinics." The criminals successfully operated over 118 phantom clinics responsible for submitting $163 million in false claims to Medicare. One of the leaders of this fraud scheme was sentenced to 125 months in prison, and over 28 defendants were charged in total.

Medical Identity Theft Harms Medicare and Its Beneficiaries

Description of Fraud Schemes
Medical identity theft in relation to Medicare occurs when a beneficiary's personally identifiable information (PII) is stolen and then used to fraudulently bill Medicare for medical services, equipment, or prescription drugs. Medical identity theft is on the increase;[8] it is rampant and is a key element in many of the health care fraud schemes investigated by OIG.

Medical identity theft is often accomplished with the use of recruiters or marketers. Recruiters entice beneficiaries to give their identifying information (including their Medicare numbers or Health Insurance Claim Numbers) by promising the beneficiaries some kind of kickback. This can be in the form of money, services, equipment, prescriptions, or narcotics. Other avenues of illegally acquiring beneficiary PII include the use of insiders who may work in the health care profession and have access to large amounts of beneficiary PII. These insiders steal large volumes of beneficiary PII and then sell it to co-conspirators who have the ability to bill Medicare using this information.

Enforcement Action
Although it may be difficult to predict when and where a fraudulent entity will commit Medical identity theft in the furtherance of health care fraud, OIG has had successes in ensuring that such entities are investigated and prosecuted for these actions.

OIG investigated an HHA owner who paid illegal kickbacks to patient recruiters to obtain the information of Medicare beneficiaries; this information was then used to submit over $12 million in false claims to Medicare for home health services that were not medically necessary or were not provided. The HHA owner also created fake patient files in an attempt to fool a Medicare auditor and make it appear as though home health services were provided and were medically necessary. This subject has pleaded guilty to Medicare fraud and tax fraud.

OIG investigated a hospice health care fraud case in which the owner paid another individual large sums of money to illegally obtain names and PII for multiple Medicare beneficiaries. The hospice owner then used that illegally obtained beneficiary information

[8] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, February 2015, p. 2, available at http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

to fraudulently bill Medicare for millions of dollars of hospice services that were never provided or were for beneficiaries who were not eligible for the hospice services. The hospice owner was sentenced to 70 months imprisonment and 3 years of supervised release. The individual who sold the beneficiary PII for illegal use was sentenced to 14 months imprisonment and 3 years of supervised release for her part in the conspiracy.

OIG investigated a pharmacy chain owner who engaged in a health care fraud scheme by submitting false claims for prescription refills. The pharmacy owner billed Medicare and Medicaid for prescription refills when the beneficiaries had not requested refills and indeed did not receive the refills. The medications targeted for these refills were often expensive HIV and cancer medications intended for very ill customers. The pharmacy owner, along with co-conspirators, falsely used the names and PII of hundreds of beneficiaries to conduct this fraud. This subject was convicted by jury of health care fraud and aggravated identity theft.

OIG Prioritizes Fraud Cases That Jeopardize Patients' Health or Safety

Description of Fraud Schemes

As previously noted, expenditures in Medicare Part D are increasing significantly. The sales of most medications occur legally and go to patients with a documented need. However, OIG is seeing an increasing amount of fraud in Part D and has a wide portfolio of work involving pharmaceutical matters, including prescription drug diversion.[9] The prescription fraud schemes are complex crimes involving many co-conspirators, including health care professionals, patient recruiters, pharmacies, and complicit beneficiaries. Often it involves other crimes, such as criminal enterprises and medical identity theft. OIG has made Part D fraud one of its top priorities. Our concern is prompted not only by program financial losses, but also by the predictable patient harm that occurs when prescription drugs are not used in their intended manner.

Enforcement Action

In an egregious example of patient harm, a 34 year-old traveling health care technician accessed Fentanyl while on duty. Fentanyl is a powerful pain medication and anesthetic and is a controlled substance. The technician was aware he was infected with the hepatitis C virus. While on duty, he would take the syringes of Fentanyl, inject himself with the drug, refill the syringes with saline, and replace them for use on unsuspecting patients. During this process, he contaminated the syringes with his infected blood. The syringes, now

[9] See *Spotlight on Drug Diversion*, available at http://oig.hhs.gov/newsroom/spotlight/2013/diversion.asp.

tainted with hepatitis C, were injected directly into patients, thereby infecting them with the virus. At least 45 of the patients contracted hepatitis from these injections. After an investigation by OIG and law enforcement partners, he received a 39-year sentence.

Another example of controlled drug fraud involved a physician who wrote illegal prescriptions for complicit beneficiaries, who were transported by the vanload to his practice. There they received medically unnecessary prescriptions for oxycodone-based products. The pseudo-patients used Medicare, Medicaid, and private insurance cards to pay for the prescriptions, then passed more than 700,000 pills to 6 different drug trafficking organizations. The physician along with 61 of his associates received a combined 253 years in prison. The physician himself received 20 years and was ordered to forfeit $10 million.

Prescription drug fraud and diversion are not limited to controlled substances, but also involve expensive, non-controlled substances, which are often not dispensed by the pharmacy. Both medication groups lead to patient harm when the drugs are not used in medically necessary or approved manner.

An example of non-controlled drug fraud involved a Detroit area hematologist-oncologist. The physician prescribed and administered aggressive chemotherapy and other infusion therapies to patients who did not need them or did not have cancer. He exploited vulnerable patients with a fearful diagnosis, solely to increase billings to Medicare and private insurers. Approximately $225 million in claims were submitted to Medicare over 6 years. The physician has pleaded guilty, and is awaiting sentencing.

OIG COLLABORATES WITH GOVERNMENT AND PRIVATE SECTOR PARTNERS DOMESTICALLY AND GLOBALLY TO COMBAT HEALTH CARE FRAUD

OIG continuously looks for ways to enhance the relevance and impact of our work by engaging and working with domestic and international partners. For example, because of the need for international assistance to locate and apprehend fugitives from our health care investigations that have left the United States, OIG partners with lNTERPOL, the Bureau of Diplomatic Security, and other law enforcement agencies. We currently have over 170 fugitives from our health care fraud investigations. In 2011, OIG established a Most Wanted Fugitive Web site to assist in locating fugitives who are running from health care fraud charges. Since OIG's Most Wanted Fugitives Web site was launched, more than 50 fugitives have been captured. OIG is also actively engaged in the Global Health Care Anti-Fraud Network (GHCAN), which was founded in 2011 to promote partnership and

communication between international organizations in order to reduce and eliminate health care fraud around the world.[10]

Domestically, OIG collaborates with internal and external stakeholders to combat health care fraud, as demonstrated by our leadership in both the Healthcare Fraud Prevention Partnership (HFPP)[11] and The National Health Care Anti-Fraud Association (NHCAA). HFPP is a groundbreaking partnership between the Federal and private sectors to share data and information for purposes of detecting and combating fraud, waste, and abuse in health care. The HFPP was created as a voluntary public-private partnership, between the Federal Government, State officials, private health insurance organizations, and health care anti-fraud associations. NHCAA is the leading national nonprofit organization focused exclusively on combating health care fraud and abuse.[12] The NHCAA mission is to protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of health care fraud and abuse.

OIG RECOMMENDS PROGRAM INTEGRITY IMPROVEMENTS TO HELP PREVENT MEDICARE FRAUD

Bringing fraud perpetrators to justice is fundamental to OIG's mission; however, enforcement alone will not solve the problem. The most effective way to fight fraud is to prevent it from occurring. One of the ways OIG seeks to achieve that goal is by making recommendations to address fraud vulnerabilities and better safeguard the Medicare program and its beneficiaries. Below are highlights of key OIG recommendations to help prevent some of the fraud schemes outlined in my testimony. For further details and additional OIG recommendations, see OIG's *Compendium of Unimplemented Recommendations* issued earlier this month.[13]

- **Prescription Drug Abuse: CMS should restrict certain Part D beneficiaries to a limited number of pharmacies or prescribers.** This practice, known as "lock-in," is currently used by some State Medicaid programs and could help reduce inappropriate drug utilization by Part D beneficiaries.[14]

[10] For more information on GHCAN, visit: http://www.ghcan.org/.
[11] For more information on HFPP, visit: http://hfpp.cms.gov/.
[12] For more information on NHCAA, visit: http://www.nhcaa.org/.
[13] The *Compendium* is available online at http://oig.hhs.gov/reports-and-publications/compendium/files/compendium2015.pdf.
[14] *Part D Beneficiaries With Questionable Utilization Patterns for HIV Drugs*, OEI-02-11-00170, August 2014.

- **Medicare Part C and D Fraud Reporting: CMS should require Medicare Part C (Medicare Advantage) and Part D plan sponsors to report fraud and abuse incidents.** Oversight of Medicare Part C (Medicare Advantage or MA) and Medicare Part D is hampered by a lack of accurate, timely, and complete data on fraud and abuse incidents that would facilitate oversight efforts.[15]

- **Inappropriate Home Health Care: CMS should enhance its oversight mechanisms to improve compliance with the home health "face-to-face" requirement.** HHAs are required to obtain documentation that the provider who certifies that a Medicare beneficiary needs home health care had a face-to-face encounter with that beneficiary. This safeguard is intended to reduce inappropriate payments for home health care, but OIG found high rates of noncompliance.[16]

- **Social Security Numbers on Medicare Cards: Removing Social Security numbers from Medicare cards is one step that would help protect the PII of Medicare beneficiaries.**[17] Experts in health care program integrity advise that Medical Identity Theft is a prevalent and increasing crime that is closely linked to Medicare fraud, and additional safeguards are needed to protect the identities of beneficiaries.

CONCLUSION

The need to protect the Medicare program and the beneficiaries it serves from fraud and harm has never been more important. OIG, working with our internal and external partners, will continue using data analytics to target our resources for maximum results. We would like to express our appreciation to Congress for their sustained commitment towards our mission and appreciate the Committee's interest in the vital issue of protecting our Medicare program from fraud. This concludes my testimony. I would be happy to answer your questions. Thank you.

[15] *MEDIC Benefit Integrity Activities in Medicare Parts C and D*, OEI-03-11-00310, January 2013.
[16] *Limited Compliance With Medicare's Home Health Face-to-Face Documentation Requirements*, OEI-01-12-00390, April 2014.
[17] *CMS Response to Breaches and Medical Identity Theft, OEI-02-10-00040,* October 2012.

Chairman ROSKAM. Mr. Marchant is recognized.

Mr. MARCHANT. Thank you, Mr. Chairman.

Gentlemen, thanks for being here today.

If I could take you to a town hall meeting in my district, there is always going to be someone that stands up usually in their upper 60s or 70s and their question is, "When are you going to stop waste, fraud and abuse?" and then they tell a story about someone they know or some doctor that they know or some story that they saw on the front page of the newspaper or the lead-in for last night's news story. So it is pretty confusing for the folks back home. They do not quite understand why their trust fund is being drained. They do not understand why the government, as big as it is and as many billions of dollars are being spent, that there does not seem to be any more progress made.

FPS, ZPIC, HC, FAC, RAC, CDAC, CPI, all these are terms that we can throw out, but they really are basically meaningless to the people that we represent.

So my question is: in plain English, what could I say back to them directly? Both of you have given excellent testimony today at a technical level of what is happening, but when you read the statistics, the amount of fraud is actually going up, and I think last year it went from $60 billion in improper payments, up about $16 billion. That is an eight and a half percent to 13 percent increase.

So what can I say to them about what is really happening and why can I tell them that we are making very concrete progress?

Mr. Agrawal.

Dr. AGRAWAL. Sir, thank you for the question, and I can tell you, I am an emergency medicine physician, and having taken care of literally thousands of Medicare beneficiaries myself, I know how involved they are in the program and how much they care about its longevity.

I would answer this way. You know, I would like to come back a little bit later if it is possible and really talk about the differences between improper payments and fraud, but to answer your question about how you discuss this with beneficiaries, I think there are a few important messages.

One, we have got a lot of tools at our disposal in order to go after all manner of waste, abuse and fraud. I highlighted a couple of tools in my opening statement, between advanced analytic systems like the FPS; very importantly, our provider enrollment systems which make sure that providers and suppliers meet all the requirements to interact with those beneficiaries, from licensure to having legitimate sites of operation. These two things are incredibly important operating together.

But we have additional resources and approaches to rooting out these issues. We conduct prior authorization and other prepayment reviews. Just last year we stopped the payment of over $5 billion from prepayment medical review. That stops the dollars from going out the door in the first place.

We have competitive bidding. So there are a lot of tools that we utilize that should be emphasized, and we need to continue to build them. You know, it is not a process that is done.

I think secondly I would say get involved. As I mentioned earlier, Medicare beneficiaries love the program. They want it to last and

be well funded, and what we see is that when beneficiaries are involved, they can be very helpful and important sources of information and leads. We get 40,000 complaints, on average, from Medicare beneficiaries every year related to program integrity, and we integrate those complaints into our existing analytics systems and models. Those complaints inform our investigations and, quite a few of them lead to real results.

So their involvement is critical, and I would ask for them to continue to remain involved.

Mr. MARCHANT. Thank you.

Mr. CANTRELL. I will echo what he was just saying about the beneficiaries, the Medicare patients, being involved in this. We know that they care about the program. We want to get tips from them. If they suspect fraud, we want them to call us, 1–800–HHS–TIPS. There is a great deal of information they can provide to us to know what is happening on the ground.

We work very closely with the Senior Medicare Patrols throughout the country, giving presentations to seniors in order to identify and report suspected fraud. So that, first, I think is critical that they get involved.

Second, you know, part of my job is getting bad actors out of the program, and so we have excluded over 4,000 individuals and entities from participation in the Medicare program just this last year, and every year around 3,000 people are removed from the program, ineligible to participate after our exclusion authority.

So we continue to focus our efforts on getting bad actors out of the program. I am very much encouraged by the developments at CMS to have a provider screening process that keeps bad actors out of the program in the beginning. That is one of the most effective ways we can avoid some of these problems. Keep the bad people out of the program to start with. Do not let them bill us.

So we support all of the preventive efforts that are taking place at CMS. We want to work with them to improve those efforts.

Mr. MARCHANT. Thank you, Mr. Chairman.

Chairman ROSKAM. Mr. Meehan is recognized.

Mr. MEEHAN. Thank you, Mr. Chairman, and thank you for this very, very important hearing, and thank you for the work that you do. The focus, saving these dollars, is so critically important so that we can direct them to the actual care.

Dr. Agrawal, you identified and you used the work to make the difference between improper payments and fraud. What is the difference there?

Dr. AGRAWAL. Yes, thank you for that. I think it is a very important question.

Every year we are required in the Medicare and Medicaid programs to measure an improper payment rate. We do that based on a series of audits, and every year we publish that rate so that it is transparent to the public.

I think what is important to realize is that the drivers of the improper payment rate are not the same as the drivers of fraud. Sixty percent of the improper payment rate is due to documentation issues. That means that there is insufficient documentation in the medical record to justify the service that was delivered.

Now, fraud is not something that every provider or physician commits. In fact, just a small minority do. But I can tell you, being a physician, that documentation issues are something that even the most legitimate, well-meaning provider can commit.

Mr. MEEHAN. By its very nature you are going to see patterns develop with fraud where the improper documentation should not be developing patterns.

Dr. AGRAWAL. You know, our experience is a little bit to the contrary, which is that when you are a fraudster and legitimate payment patient care is not your priority; you are not spending the majority of your day at the bedside trying to take care of Medicare beneficiaries; you have plenty of time to document very effectively.

Mr. MEEHAN. So actually they are doing a better job.

Dr. AGRAWAL. They can do quite well, and we see standardized notes, other template driven notes that actually would pass a number of different checks looking at the medical record.

It is the legitimate providers, the ones that are spending the majority of the time——

Mr. MEEHAN. Well, that opens up the door, and, Mr. Cantrell, please jump into this as well, which is the investigations and the use of predictive analysis is really moving the ball forward.

I had the good fortune of serving as a United States Attorney with one of the health care task forces that were set up, and it was a great step forward, but one of the other things that I really appreciated was it is one thing to take somebody out of qualification for a system. It is another thing to send them to Federal prison, and that is the kind of thing that really gets people's attention.

What is being done to find the right balance with the OIG and with the resources that you have and in collaboration with other particularly law enforcement resources to take some of these 40,000 leads that you get and direct them to places where there can be criminal investigations and people can be held accountable not so they just reap themselves and come back again in a different format, but they do a little time in Leavenworth.

Mr. CANTRELL. Yes, I will say we are working very closely with law enforcement partners across Federal and State and local law enforcement. We have the Medicaid Fraud Control Units that exist in every State. We work very closely with them. We are working more than ever with the DEA because of the prescription drug abuse problem and the fraud problem that exists there.

So there are opportunities for us to share this information between the FBI, the DEA, the OIG and other law enforcement partners so that we are focusing our resources in the right areas.

Mr. MEEHAN. How is that being done so that there is a regular collaboration and coordination? Because my experience is oftentimes it is not a bad thing, but a lot of these things are housed in the Civil Division, and so you are getting a lot of work that is done. Oftentimes people are proud of the work that they have done, and even within the institution people are proprietary. They want to protect the investigation. They do not want the criminal guys getting involved in my work.

What are you doing to assure that there is real effort to look at the most effective way?

And let me ask the extent to which either of you are engaging in grand jury investigations, using the potential resources to break those schemes that you identified?

Oftentimes they are larger parts of roles, while we have people that are susceptible to grand jury subpoenas that are part of those networks, drug dealer or whomever.

How much effort is being put into really getting away from predictive analysis and really tying it effectively with law enforcement resources?

Mr. CANTRELL. The key is turning data into action. So we have lots of identification of suspect providers. It is turning that information into an investigation, gathering the evidence necessary for prosecution. We absolutely utilize grand juries. We work with our partners, and information sharing on any particular investigation happens daily throughout the country. There are——

Mr. MEEHAN. What do you do to make sure that it is happening to make it actually do a good job?

Actually, Dr. Agrawal, just the numbers indicate you are just starting on your efforts, not the same history or longevity. So there is a recognition, but at the same time, the numbers are more compelling in the form of impact in terms of, you know, predictive analysis turning into recoveries.

What are you doing to make more timely referrals so that from the outset you are working with law enforcement on your side?

Dr. AGRAWAL. I think that is a great question. So you are absolutely right that the authorities that CMS has now are unique in its history. The administrative authorities to stop payments on the front end, suspend anywhere from, you know, a claim at a time to 100 percent of all the payments that a provider gets, and we have been working diligently to build those authorities, utilize them efficiently and effectively because I think what we see or what we have been focusing on is let us stop the flow of dollars for bad actors and then absolutely work with law enforcement to take other steps in the criminal justice system and if possible, put them in jail.

We rely obviously very strongly on law enforcement to pick the ball up at that transition point where we cannot go past administrative action. I think that partnership is definitely critical as long as we are also stopping the flow of dollars on the front end so that they are not taking advantage of the trust funds.

And while I agree that figures of folks entering jail are really important, I would highlight the importance of 500,000 enrollments that are no longer able to build a program, and literally hundreds if not thousands of enrollment applications that are denied. These folks will never get a chance to send a claim. That is as preventive as it gets.

Mr. MEEHAN. Thank you, Mr. Chairman. I yield back.

Chairman ROSKAM. Mrs. Noem is recognized.

Mrs. NOEM. Doctor, FPS does not work very well, does it?

Dr. AGRAWAL. I agree. I think there are lots of tools that we should use, balancing both prevention and recovery.

Mrs. NOEM. My understanding is that using FPS, that that is supposed to help CMS identify claims before they are paid out, fraudulent claims; is that correct?

Dr. AGRAWAL. Yes. The system has lots of different capabilities. So, on the one hand, it can actually deny claims that simply do not meet payment requirements.

Mrs. NOEM. And under the Affordable Care Act, there was more authorities given as well?

Dr. AGRAWAL. Correct.

Mrs. NOEM. And so how many fraudulent claims have been stopped using FPS going out the door?

Dr. AGRAWAL. I do not know that I can give you that. We can get the number for you later, of actual claims denials. But, again, the FPS has capabilities that allow us in some cases if a payment policy is simply not met to deny the claim. No payment goes out the door.

In other circumstances it makes our investigation more efficient and effective so that we can stop perhaps the payment of all claims. A hundred percent payment suspension can be put in place. We can work with law enforcement. We can work with our own boots on the ground staff, conduct the investigation that then allows us to take a more stringent administrative——

Mrs. NOEM. Are claims being flagged today and not being paid using FPS?

Dr. AGRAWAL. Yes.

Mrs. NOEM. They are being, and you can give us those numbers if we need them?

Dr. AGRAWAL. Sure, yes.

Mrs. NOEM. That would be wonderful.

So my only question then is why the improper payment rate is going up.

Dr. AGRAWAL. Again, I think we have to separate improper payments from fraud. Fraud is a legal determination made by the criminal justice system.

Mrs. NOEM. But FPS is still utilized to help stop improper payments as well, not just fraud, correct?

Dr. AGRAWAL. You know, initially because of the focus on fraud and abuse, obviously the legitimate and necessary focus, we designed a lot of our models in the FPS to directly address issues of extreme outlier behavior that we could then take significant administrative actions against and work with law enforcement about, and our referral rate has actually been steadily increasing to law enforcement.

What we see now as the system has matured is we can move it upstream and try to address other types of improper payments. So, for example, we have worked with our Medicare administrative contractors who conduct medical review on a daily basis, and in a pilot we are actually utilizing the FPS to better focus their medical review efforts.

That is not the same community of providers as we have been very focused on in our work because they are extreme outliers. This community is not so much an outlier. They are probably legitimate providers that are just not billing the program ideally.

Mrs. NOEM. So necessarily at the beginning you were not looking at certain providers, only some that you identified could be potentially participating in fraudulent behavior?

Dr. AGRAWAL. Well, I think we want to be very careful with our administrative authorities because they can be extremely disruptive. A hundred percent payment suspension can put some providers out of business, and so——

Mrs. NOEM. How many Medicare providers are there?

Dr. AGRAWAL. There are between 1.5 and 1.6 million enrolled providers.

Mrs. NOEM. And FPS allows you to look at their behaviors and identify traits that may be fraudulent?

Dr. AGRAWAL. We see four and a half million claims per day in FPS that address all of those provider types. We identify extremely aberrant outlier claims, and the system actually helps us prioritize not only the claims, but the providers for further investigation.

Mrs. NOEM. So not just fraudulent but also improper?

Dr. AGRAWAL. Well, again, we are well in front of the criminal justice process. We do not determine that something is fraudulent. We determine that it is an outlier and either should be paid or should not be paid.

Mrs. NOEM. So can you tell me why CMS has not used crowd source fraud prevention in the past?

Dr. AGRAWAL. Well, I think the small business——

Mrs. NOEM. It uses more of the analytics and that has not been utilized by CMS, correct, through FPS?

Dr. AGRAWAL. The FPS is an advanced analytic system. So what it does is it takes existing models, and you asked about crowd sourcing.

Mrs. NOEM. Yes.

Dr. AGRAWAL. We take input from a wide variety of sources. I guess that is the definition of crowd sourcing.

Mrs. NOEM. Okay. So that is being used.

Dr. AGRAWAL. In order to develop these models, we get that input from our Zone Program Integrity Contractors. We get it from law enforcement. We even incorporate information from our beneficiary complaints, which is, I guess, another form of crowd sourcing. All of those things can feed and create, allow the development for these models that then look at the claims themselves.

Mrs. NOEM. Okay. Do you have any regulatory or statutory or anything that is in statute that would prevent you from being able to use more crowd sourcing? Is there anything that would tie your hands from being able to rely even more on those analytics?

Dr. AGRAWAL. You know, I think we have a variety of ways of getting input. I am not sure specifically, but we can perhaps take that question back.

One source that I did not highlight yet is we actually are in a public-private partnership with a number of private plans. I guess that is another form of crowd sourcing where we exchange best practices and data with them, and that has also been a really useful source of leads and information for us.

Mrs. NOEM. And is that useful when you are dealing with fraud prevention or improper payments?

Dr. AGRAWAL. You know, in our world, these things really run together. I mean, there is not a sharp line when you say, well, this

claim has now moved from sort of waste to abuse or fraud. Again, we do not make that fraud determination.

Mrs. NOEM. But you did say earlier in your statement, did you not, though that you were focused mainly on fraud prevention to begin with and were not as concerned with improper payments.

Dr. AGRAWAL. We have not——

Mrs. NOEM. But that is how you developed your FPS system.

Dr. AGRAWAL. We started the FPS focus has been on some of the highest outlier because those outliers really do merit the administrative actions and other activities that law enforcement can generate against them. You know, they stand far and above other providers, even compared to their specialty or compared to their geographic peers.

As the fraud prevention system has matured, we are trying to pilot and think of ways of moving it even further upstream to address legitimate providers that are not trying to push the envelope into abuse and fraud, but are ally, you know, just not meeting certain payment requirements or misusing modifiers, misusing certain codes, to see if we can get the system to help focus our efforts on the right set of providers that——

Mrs. NOEM. Well, considering the amount of improper payments and the fact that those numbers go up, I think that is a great place to focus.

Thank you. Appreciate it.

Chairman ROSKAM. Mr. Kelly is recognized.

Mr. KELLY. Thank you, Chairman, and thank you for both being here.

I come from the private sector, and what I compare a lot of what you do is to what I have done. I am an automobile dealer, and I have got to tell you that I had a discussion with one of our General Motors service people today, and what I am having trouble understanding is with the data that we collect, I mean, the IRS has absolutely no problem finding out who deposits what where and actually can freeze your accounts when they see something being done improperly, even if it is not proved yet.

I think the confusion is when I look at the amounts of dollars that we are talking about, and if it is really as high as it is, if we have this data, if you go to an automobile, you have its birthdate. The day it is produced has a serial number. From that time to the time it is scrapped we know who owns that car, where that car is, and everything about it.

What I have trouble understanding is whether it is improper payments or whatever, fraud, you are still using taxpayer money that is being used in a wrong way. I mean, we are arguing now over a budget and worried about how we are going to defend a sequester and defense is about $100 billion. We are talking about Medicare and Medicaid paid out $77.4 billion in improper payments. That is money that probably could be used better elsewhere.

So my question comes down really if we have all of this analytical data, and I go back to my years in the car business. A couple of years ago General Motors had a problem with ignitions. They said if you have too much weight on your key chain, it turns the car off. Well, I am still in the automobile business. You know, we had to go back to owners of 2005 and 2006 cars. We have cars that

ran off the road and gone into a river, retrieved and rebuilt. General Motors is still responsible for the safety recalls.

If you were to drive your car into our service department today, Doctor, and it is a General Motors car, I can use through the VIS program, the vehicle identification system, I can find every single repair done to that car, the day it was done, the mileage that was on the car, the technician that did the work on the car, which would be the doctor working on somebody; the parts that were used, and if it was truly done that way.

So I am constantly sitting down with General Motors. They go across all this data and say, "You know what? You guys seem to have a higher repair rate when it comes to brakes that does not match up with what happens in your area."

So all of this data that we collect, we collect the data, but we are not getting any closer to getting this fixed, and what I really worry about is we are talking about $125 billion of taxpayer money that has been wasted, and $77 billion of it is through Medicare and Medicaid programs. And there has to be some way with the collection of this data.

Who is analyzing the data and who is looking at it? It cannot be that we do not know where the improper payments are being made, and whether it is fraud or improper payments, to me it is the same thing. It is wasted taxpayer dollars.

Mr. Cantrell, you all have access into data that is incredibly deep into everything, and as I said, the IRS, I mean, listen. They know every day who deposits money across the country in different banks. We can ferret out those people, but we cannot find where 77 and a half billion dollars of improper payments are going?

That to me is inconceivable in a government that has data and has the ability to track every phone call we make, every movement we make, but we cannot find out where this money is going and say, "My God, this is taxpayer money that is being wasted in a country that is looking to put money where the best return is on it for the people who put it in, the taxpayers."

We are still playing in the dirt with this stuff and still trying to figure it out.

So all the data that you are doing as Mr. Meehan talked about, who are we going after and why are we going after?

I have got to tell you something. If you are an automobile dealer and you have these kind of numbers, one of two things is going to happen to you. First of all, you are going to lose your franchise, and secondly, you are going to get tried in a court for improper payments and for fraud.

So tell me: where are we going with this? Where do you see this going?

Because the numbers have gone up, and listen. I have a collection agency that collects money for me. After it goes beyond 180 days, I am not going to go chasing somebody. I do not have time to do it, but we turn it over to a collection agency. Do you know what we pay them? We pay them 35 cents on the dollar that they retrieve.

So please tell me where we are going with these program and how are we protecting taxpayers' money?

Dr. AGRAWAL. I think the protection of taxpayer dollars is absolutely important. So I think what is important also is not to view any specific tool or process as a stand-alone. We use these things together to try to be as preventing and effective in our actions as possible.

The FPS, the automated provider screening system, these are examples of tools that we have at our disposal. We have other tools, prior authorization stops payments from being made that do not meet our requirements. Prepay reviews, post pay reviews; we have a moratorium that has been implemented in different parts of the country that stops the enrollment of providers because, again, we know that that gateway to Medicare is so important that if we stop bad actors at the door, it is highly preventive and stops the flow of dollars.

All of these things have to work in concert to really drive down all manners of waste, as you identify.

One thing I would also add is outreach and education to the provider community is central in this. I am not purporting to educate the really, really bad actors that just want to steal from the program, but again, 60 percent of the improper payment rate that is driven by documentation challenges, we absolutely need to be working with providers to educate them on our documentation requirements and get that documentation to improve.

I think what you will see is that the improper payment rate can come down because of issues like documentation, but the dollars going out will not necessarily change because the providers will be better educated to meet our requirements that they are documenting appropriately.

The contention is not that the services were not provided or that they were not necessary. It is just that the documentation did not match. We can do a much better job outreaching to these physicians and get that level of awareness improved.

Chairman ROSKAM. Mr. Crowley is recognized.

Mr. CROWLEY. Thank you, Mr. Chairman. Thank you for holding this hearing today as well. I think it is important to remember that the Congress has a responsibility to enact laws but also for oversight purposes. So I appreciate you doing this in a responsible way.

Doctor, welcome. Mr. Cantrell, welcome as well.

On the next panel we will have a witness from Visa, and while CMS and Visa both use predictive modeling, I can only assume that health care is not the same as consumer purchases. You cannot return a repaired knee, for instance, after you have used it.

How is CMS different from a credit card company? And how do these differences affect how CMS does their forward fighting job?

Dr. AGRAWAL. Yes, thank you for that question.

I think we are very different from a credit card company, even though some of our technology and the way we utilize it can look similar on the surface.

There are three big differences I would highlight. One is medical claims are highly complex, I think more complex than the typical financial transaction on a credit card.

Second, the medical claim is really just a shadow of what actually happened in the clinical setting. For anyone to know what ac-

tually occurred in that clinical action you have to look at the underlying medical record, which typically does not come to CMS or any payer alongside the claim.

And third, we have major access to care issues that we want to keep from occurring just because of payment denial.

So let me talk a little bit more about these. First, on the complexity, medical claims are not unidimensional financial transactions. They have information about the provider, which we have 1.5 to 1.6 million of in our program. They contain information about the beneficiary, which we have over 50 million of in our program. And they utilize a language of codes and modifiers. We have more than 11,000 of those codes that can be billed on a Medicare claim.

Those things can all be combined in various combinations that make analyzing a claim far more sophisticated and involved a process than looking at dollar amounts coming from a particular vendor, you know, attached to a particular credit card.

Looking at aberrancies connecting these claims over time can be very challenging and far more involved, I think, than the typical financial transaction.

Second, medical review or medical record. So the claim is a bill, but it was generated after there was a clinical interaction that is really documented in the medical record. The medical record does not come to CMS with the claim, nor does it go to any payer typically.

We only see medical records when we audit claims, and we audit far less than one percent of claims, given that we get over a billion claims per year. So oftentimes in order to corroborate that a claim is actually aberrant, we have to look at the underlying medical record and see what was aberrant about that clinical interaction, again, requiring more documentation than you typically need in a financial transaction.

And third, access to care. When we deny a claim, whether it is one claim or a series of claims, we are denying payment to a physician or provider and denying a claim about a service that a beneficiary may really need. We want to be very careful when doing that because we do not want to cause access problems in our program because of an admittedly very vigilant and very productive program integrity approach. These things always have to hang in the balance with each other.

We know that we are not denying payment for a TV. We are denying payment for what could be a legitimate medical service, and we want to make sure we do that very carefully.

Mr. CROWLEY. Mr. Cantrell, before you respond if I could just for the sake of time and get another question in and you can also elaborate on this first question as well, but we all know that health care fraud goes beyond Medicare and Medicaid. How is CMS and other agencies within the Federal Government working to involve the private sector anti-fraud efforts?

Mr. CANTRELL. Sure. I will start. The Health Care Fraud Prevention Partnership is something that CMS is leading and we are participating in since the very beginning with conversations about developing this partnership that includes private payers. There is a lot we can learn from each other.

Fraud, as you said, does not just affect government programs. It affects private insurance as well. So we often see and we do see the same schemes perpetrated against both public and private, and we work very closely in certain investigations to ensure that those private funds are recouped when someone is filling from both programs.

So that partnership is meant to increase and build upon that relationship, begin sharing data, and I think that is going to be important for us going down in the future.

Dr. AGRAWAL. I agree with everything that Mr. Cantrell has said. The only thing I would add is we are also working, you know, beyond the partnership context, which I certainly agree with. We are working to extend our reach into other private plans.

So Medicare Part C plans, Part D plans. We have been working very hard in the agency to get and counter data, other sources of data from these plans so that we can better assess the kind of utilization that is occurring.

We recently at the end of last year extended our enrollment requirements into Part D so that we could have direct line of sight on prescribers in Part D, and you know, they currently relate mainly to Part D plan sponsors, but you know, we are extending our authority there so that we can roll out many of the same enrollment and screening approaches that we have in A and B to Part D.

We are also doing the same on the Medicaid side and looking to work much more closely with Medicaid managed care plans in the private sector.

Mr. CROWLEY. Thank you.

Thank you, Mr. Chairman.

Chairman ROSKAM. Mr. Holding is recognized.

Mr. HOLDING. Thank you, Mr. Chairman.

I want to jump right into the questioning and pick up again on a theme that Mr. Meehan touched on regarding interagency coordination between CMS, HHS and DOJ.

So to the both of you, do you think this interagency coordination is as good as it can be? Dr. Agrawal, you can start.

Dr. AGRAWAL. Thank you.

I think it can always be improved. So we have done a lot in terms of data sharing. Basically every system that I have access to law enforcement has access to as well. That includes our fraud investigations database, our FPS that we have been discussing, the integrated data repository at CMS. That is a large cache of a huge number of Medicare claims and other analytical tools.

So we have certainly done a lot to try to make sure that law enforcement entities have access to all the data that CMS can provide, and I am sure we can do more than——

Mr. HOLDING. When FPS is generating leads, you know, you see the anomalies and you find the leads and you prioritize them; so do you turn around and share those directly with OIG?

Dr. AGRAWAL. We give OIG real time direct access to the system itself so they can see leads as they are being generated. In addition, we——

Mr. HOLDING. Does OIG take advantage of that? I mean, do you see the leads there and do you proceed——

Mr. CANTRELL. We use other systems they have made available to us more directly than the actual Fraud Prevention System. We have tools like the IDR, the Integrated Data Repository, 1PI. These are tools that we did not have five years ago.

So I will say the access to data has been an area of great improvement over the last five years or so, and the partnership has led directly to that. We have over 200 individuals from our office who have direct access to this Medicare claims data that we did not have before. Now we have access to prescription drug data that we did not have before through these systems.

I think there are definitely areas that Dr. Agrawal mentioned before, Medicare managed care, Medicaid data, and prescription drug data, where we can improve upon that access to data and monitor——

Mr. HOLDING. So you do not have access. Is that an obstacle then, not having access to that specific data there?

Mr. CANTRELL. We have access to parts of that data, but it is not the same level of access, kind of real time access that we have for fee for service data. So there are definitely some opportunities there to build upon what we have done in fee for service so that we can have that level of near real time access to managed care data.

We know there is fraud out there, but we just do not have visibility right now into Part C really.

Mr. HOLDING. So do you have any way of evaluating or measuring the quality of your coordination? Is there a standard by which you can measure it?

Mr. CANTRELL. I think it is very subjective in terms of that. We have so many leads that come from so many sources, and CMS, the referrals we get from the contractors are just one small part of that. In fact, I think it is about 10 to 15 percent of the leads we get, cases that we open are coming from CMS referrals.

We work with our law enforcement partners. That is the bulk of the information we get. Whistleblowers have always been the greatest lead.

Mr. HOLDING. It seems like you get a lot of leads and a lot of information coming in, but they are not being prioritized. They just kind of come into a basket and you try to figure out.

Mr. CANTRELL. They are absolutely——

Mr. HOLDING [continuing]. Gets leads and you prioritize them. The OIG is getting a bunch of information from a lot of different sources, and do you have a method for prioritizing them?

Mr. CANTRELL. We absolutely do. So we have a process. You know, every lead that comes in the office goes through an analysis by our Special Agents in Charge, our Assistant Agents in Charge, the investigators. They balance it against existing workloads and determine based on whether there is potential harm to patients, the financial impact on the case, what level of evidence has been provided up front. Is it a whistleblower or is it an anonymous lead with nothing really to corroborate that information?

Mr. HOLDING. Right.

Mr. CANTRELL. So we prioritize continuously.

Mr. HOLDING. So in the next panel we are going to have some witnesses. I have read their written testimony, and they point out

if you could share all of this information across the entire spectrum, it would be a much more effective way to combat waste, fraud and abuse. Now, I understand there are privacy concerns, but do you all see a way forward to share this data uniformly across the spectrum of stakeholders in here who want to combat waste, fraud and abuse?

Dr. Agrawal, do you want to hit that?

Dr. AGRAWAL. Sure, absolutely.

Mr. HOLDING. We are running out of time, so make it quick.

Dr. AGRAWAL. I will do my best.

Mr. HOLDING. All right.

Dr. AGRAWAL. I have not been known for making it quick, but I will try.

So I think that is absolutely right. You know, one of the principles behind the Health Care Fraud Prevention Partnership that Mr. Cantrell mentioned is exactly data sharing. I think for it to be effective it has to be purposeful, purpose driven, right? So it is not just a huge mass of data without any guidelines for what that data means or why we are sharing it.

In the partnership we have taken a very steady, objective driven approach to sharing that data. What is it that we are trying to accomplish? What is the minimum amount of data that we need to exchange in order to meet that objective?

So that we are not just exchanging a bunch of data that then overwhelms systems, overwhelms staff time to sift through it. We are doing it in a very purposeful driven way. I think that is the key to all of this so that, you know, we are really achieving impact with all of this data work.

Mr. HOLDING. Mr. Cantrell, I will allow you to follow up in writing. Thank you.

Thank you for your indulgence, Mr. Chairman.

Chairman ROSKAM. Mr. Smith is recognized.

Mr. SMITH OF MISSOURI. Thank you, Mr. Chairman.

My understanding is that the FPS generates leads for investigations by showing anomalies in claims data. I want to know if there is a risk that the FPS system would flag legitimate claims and send them for investigations to a contract. Could this potentially tie up resources on legitimate claims instead of going after actually fraudulent ones?

Doctor, what does CMS do to mitigate this concern?

And does CMS have any standard procedures in place to screen leads from the FPS before sending them on to the ZPICs?

Dr. AGRAWAL. Yes. Thank you for the question.

So our screening and prioritization process starts up front when the model is being developed. So we develop these models working with our contractors that know what is happening on the ground. We develop them working with law enforcement and get their input on not just what is outlier behavior because anybody can find that in a data set, but really the outlier behavior that we ought to be most concerned about, that we can take administrative action against, that might be threatening to the health and safety of our beneficiaries.

And that is, I think, very specific, experience driven knowledge, that we can in viewing the models right at the front end so that

we are sifting out, you know, outlier behavior that is otherwise pretty innocent.

Secondly, even when, you know, once claims start streaming through the system against the model, there is an internal prioritization based on just how many times you are hitting that model or a variety of models. So the more models you hit, the worse you look as a billing provider or supplier.

And I think the system does a great job of both helping us further prioritize things just on a very technology, data-driven manner.

And finally and extremely importantly, we do not take administrative actions without human beings getting involved, except where it is very clear that a single claim does not meet payment requirements, right? We can deny that kind of claim, but when you are trying to build a case, you need to do other on the ground work. You need to talk to the provider. You need to get medical records. You need to interview beneficiaries.

That human interaction makes sure that we are not implementing an administrative action against an otherwise legitimate provider.

Mr. SMITH OF MISSOURI. What is the rate of false positives in the leads generated by the system?

Dr. AGRAWAL. I am not sure that it makes sense actually to speak in terms of a false positive rate because, again, there are so many filters that stand between a claim coming in and being labeled aberrant or flagged in some way and an administrative action being taken. Those filters are both technology driven as well as human driven as I described.

Our focus has been let us not take an administrative action against a provider-supplier that is legitimate or has a billing problem that we can correct through education and outreach. We want to reserve the administrative actions for those providers and suppliers that are really egregious. The only manner of correcting their behavior is the administrative action or they have demonstrated a consistent unwillingness to follow our policies.

So in that sense, you know, because there is not just an automated trigger leading to an action, it does not really make sense to speak in terms of a false positive rate.

Mr. SMITH OF MISSOURI. So there is no like data to say that there is any kind of false positives?

Dr. AGRAWAL. I do not think that there is. It is a question that I can take back to our analysts and see if they track anything like that. You know, I think what we actually spend more of our time on is rolling out models and then, you know, getting input from our contractors, from other sources to help us decide is the model working or not.

And where the model is not working, we can make refinements to get it to improve.

Mr. SMITH OF MISSOURI. Okay. That leads to my next question. According to GAO, in 2012, only five percent of all fraud contractor leads came from the FPS. Do you have updated numbers on that?

Dr. AGRAWAL. Not that I am aware of, but again, I can take that back and see if there are updated numbers.

You know, that GAO report was quite early, as you know, in the development of the FPS. As we were building the technology, we had outstanding questions about how to integrate that with our existing work and what portion of the work it should drive.

I think what the GAO found was something like ten percent of all of our work was initially driven by the FPS. As the FPS matures, takes on more models and its adoption rate has increased, I expect that number has gone up, but again, we can take that as a request back to determine.

Mr. SMITH OF MISSOURI. That would be great.

Once the contractor gets the lead, what happens?

Dr. AGRAWAL. So a variety of actions can be taken. One thing that we have tried to do to make the FPS system more user friendly is by trying to present information in a way that makes it more actionable immediately for the contractor. So they do not get just a bunch of data and numbers. They actually get this data organized in a way that helps them do their investigative work.

So what they will do often is they will take the data from the FPS. They can utilize other systems like 1PI to do any additional analysis that needs to be done. They can conduct very manual processes, like interviewing providers, interviewing beneficiaries, conducting site visits, conducting medical review of the underlying medical record, and then ultimately building that case for an administrative action or law enforcement referral.

Chairman ROSKAM. Thank you.

Dr. Agrawal, I have got a few questions for you. As I was reading your testimony and then listening to you this morning, I felt like I was the sales manager listening to a salesman who had been out working hard making a bunch of sales calls and was coming in and saying, "Look. I called on this customer and I have done this and I took this person to lunch, and I feel kind of like the sales manager that is saying, 'Hey, where are the orders? Where is the final product?'"

And I recognize that you are in a complicated milieu, and I am not here for a second saying that the responsibility that you have is easy or that I have got the Peter Roskam five-point easy solution for solving things. Yes, I have got that on a laminated bookmark for you, my friend.

[Laughter.]

Chairman ROSKAM. So I accept at face value that this is terribly complicated. But when I opened, I opened with this idea and that is, look, we are really struggling on Capitol Hill right now to fund a super important program as it relates to Medicare. These choices that are before us are all revenue seeking choices basically, and this SGR deal that is being negotiated, the "doc fix," is really, really hard. It is hard on providers, and it is hard on seniors, and it is hard on everybody.

And then I look across the table at you, figuratively, based on your responsibility, and I think you have got the answer. You have got the money, and you have this incredible responsibility.

And I listen today and I read, and I feel underwhelmed by the direction that things are going. I just want to put something up on the board, which is sort of my frame of reference.

And you exchanged with Mr. Crowley and you made the argument, look, this is different than a Visa bill, and I accept that it is kind of different than a Visa bill, but I do not think it is this different. So Visa is doing $10 trillion. I mean that is thousands of billions of dollars on an annual basis and their numbers are practically de minimis compared to 12 billion or a 12 percent rate.

There was something that you said in your testimony. You had it in your written testimony. It jumped out at me, and you reiterated it today. I just want to read a sentence to you and tell you how it struck me. So this is what you said, and it is not a bad thing, but just sort of the way in which it was presented, I perceived it differently than what you were trying to communicate.

So this is what you said. "When FPS models identify an egregious suspect or aberrant activity, the system automatically generates and prioritizes leads for review and investigation by CMS' Zone Program Integrity Contractors."

Now, you would say that and you would say, hey, that is a good thing. I read that and I say you have got to be kidding me. This process is so slow and so ridiculous and so hamstrung that it is this identifying leads and all of this sort of process?

We are going to hear later on, I think, from Ms. Frizzera, who is going to give us an example in Miami. You may have seen her testimony, but an example in Miami where they identify this stuff and say this is a real problem. She goes to the IG, and it is slow, slow, slow. Meanwhile money is going out the door.

So I think what you are hearing from many folks on this Committee is the level of activity is significant. Nobody is arguing that you are not working hard. But what we are saying is this has to improve, and this is not like a hope and a dream sort of improvement. This has to improve because this amount of money going on, and you know these numbers better than I do; you are marinating in this stuff; these numbers have to improve because it is simply unsustainable and the public is losing confidence and so forth.

So here are a couple of questions. You started to address this when Mrs. Noem was asking, but I do not think you got to it. Why is the improper payment rate going up?

Dr. AGRAWAL. I think as I mentioned earlier one of the biggest drivers of the improper payment rate is documentation. So here again I think we see the balance of the more vigilant on program integrity and then at the same time potentially driving up the rate.

One of the biggest drivers of the improper payment rate is the home health face to face requirement now which is part of the Affordable Care Act. I think we can all agree that a clinician seeing a beneficiary who needs home health services and having that interaction be face to face, documenting the need for home health is a strong solution. It helps address one of the areas that we know has been endemic with aberrancies and problems, home health services.

While I think the concept makes a lot of sense, the idea is very clear. Providers have a hard time documenting that face to face encounter, and so the home health improper payment rate has now jumped to over 50 percent, in large part driven by this, I think, well meaning, well intentioned, well thought out face to face requirement.

So one could argue let us eliminate the requirement, but I think that is not the right answer clinically, right? The right answer for us is educate these otherwise legitimate providers and get them to raise their level of documentation so that it meets our standard. That would bring down the improper payment rate.

You can see this in a wide variety of clinical circumstances, and again, you know, so you can see——

Chairman ROSKAM. You think that there has been a new factor that has been introduced. The new factor is a new requirement, and that is influencing the payment rate or the improper payment rate.

Dr. AGRAWAL. There is a variety of new factors, correct.

Chairman ROSKAM. Okay. I have got it.

Do you have confidence that that is the intervening cause, and that that is it alone?

Dr. AGRAWAL. Yes. We do not just measure a high level of improper payment rate. We drill that down to the specific provider categories, the types of services that are leading that rate.

Home health is consistently elevated, and it has gotten higher. DME supplies are consistently elevated. Skilled nursing facilities, consistently elevated. So a lot of our activities around lowering the rate focus on the areas of the highest errors.

Chairman ROSKAM. But why does FPS only have an impact on one percent of Medicare claims?

Dr. AGRAWAL. I think FPS is a new system. In part that is the answer, right? So the initiating legislation, as obviously you well know, came out in 2010. This is our third year of operations. Our maturity in building the system has improved dramatically every single year.

If your point is we need to do more, we are totally aligned on that. We want to do more. I have a staff that works——

Chairman ROSKAM. Well, what is holding you back? I mean, one percent just seems incredibly underwhelming.

Dr. AGRAWAL. You know, we have made a lot of investments in data analytics to identify leads for our work. Those investments are paying off. I think what we need to focus on is getting much more efficient from lead to final action.

Certainly I spend a lot of my time focused on making our contractors more efficient, measuring their performance, making sure that we are paying them to do the work that we want, and getting the kind of end results that we are looking for.

So, again, it is a continuum of activities. It is not just get a lead and take an action. We do have to meet a bar for taking an action. We do need to be fair to providers, even the bad actors, to make sure we are doing this the right way, and we want to do it in a way that does not victimize the innocent, legitimate providers that are just doing their work.

Chairman ROSKAM. How can you not know the number of claims that have been stopped by FPS?

Dr. AGRAWAL. We do. I will get you that number. I can give you a dollar amount as well as the number of claims.

Chairman ROSKAM. Okay. I know that you use all of these tools in conjunction with one another, but how do you identify whether one program, especially FPS, is working in particular?

So what is the metric to say, if you are only hitting up against one percent, what is the metric to say it is working at all?

Dr. AGRAWAL. The FPS, you mean?

Chairman ROSKAM. Yes.

Dr. AGRAWAL. Well, we have a very viable metric. We are working with the Office of Inspector General. As you know, the statute required certification of our savings numbers. We have engaged in an audit every single year since the FPS has been implemented, including this year, and the OIG certified both our identified savings numbers as well as the adjusted number. So I think that is an extremely viable metric of the financial impact of FPS.

In addition, what we published in our report last year are all the actions that FPS has led to beyond the financial impact, right? We have taken administrative action against more than 900 providers and suppliers because of the FPS, not all the other processes that we have, which are numerous, but specifically because of the FPS.

We have initiated new cases and investigations because of the FPS. We have made existing cases get more efficiently to outcome because of the FPS. Again, that is a focused piece of work and audit on the FPS, but my point, I think, continues to be the FPS is one tool at our disposal. Look at the broader picture and you will see a picture where we really have moved from a "pay and chase" model to a recovery—I am sorry—a prevention based model.

Chairman ROSKAM. So the funding for FPS is coming to a close. Where are we on that?

And if so, how are you paying for it?

Dr. AGRAWAL. So at the end of this fiscal year we will have exhausted the initial funds given to us through the Small Business Jobs Act, and what we are doing is transitioning the FPS to utilizing other existing program integrity funds.

Chairman ROSKAM. Getting back to your point that this is a more complicated system than Visa, does that not create more opportunities for you though? Does that not actually create more data points and more opportunities to say, "Now that is looking weird and that is looking off and that is inconsistent," and so forth, rather than just trying to figure out if Joe Crowley is buying, you know, $10,000 worth of stereo equipment on——

Mr. CROWLEY. Mr. Chairman, keep me out of it if you do not mind.

[Laughter.]

Chairman ROSKAM. Do you follow me? I mean, you have got a lot of data. You have got a lot of stuff, and to your own point, look, this is highly complicated and integrated, but does that not create more opportunity, sort of more facets to look at?

And if they are off, you can see the hues and the angles are off, and it just does not make sense. So do not pay it.

Dr. AGRAWAL. Yes, that is very interesting. So I think we are trying to utilize every available opportunity to take administrative action. So, again, we have lots of tools. We can conduct the site visits that I mentioned. We have the enrollment screening requirements. We have analytic systems like the FPS. We can conduct social network analysis that looks at how one provider relates to another providers, especially as——

Chairman ROSKAM. You see, if all of that is happening well, then the number gets closer to the Visa number.

Dr. AGRAWAL. But again, this number is the improper payment rate, right? So these providers do not necessarily need to be kicked out of the program. They have a problem which is documentation or providing the right service in the wrong location, but those are not the same types of problems that we want to address by kicking folks out of the program. Those are the problems that everyday clinicians have.

Chairman ROSKAM. Yes, but you are arguing how many angels can dance on the head of a pin here. We are still talking about 12.7 percent of money, dollars, that are going out the door, dollars that cannot be used for the "doc fix," for example.

So I understand that there is a distinction that in some cases is an important distinction with a difference, but in this case it is sort of a distinction without a difference. The money is still the money. You are still at 12.7 percent.

I mean Visa is not just lapping you. Do you know what I mean? You are not even in the same order of magnitude with them.

And I guess it comes down to this, and let me just close by this. I think both sides of the aisle have a very high expectation of what you are doing, and you are viewed as the trustee of literally billions of dollars. Yes, it has gotten more complicated over the years. The fraudsters and the hustlers are totally on top of their game, and they are super aggressive and super bright, but we have to have an improvement all the way around.

And, yes, it is a more complicated system than buying a stereo and so forth, but out of that complication comes a real opportunity in terms of more exposure. And so I think the sense that you are getting from this Subcommittee today is that we look with an urgency about what you are doing, and we are rooting for you, but we are disappointed. Actually I am, and I know, listen, nobody wants to disappoint people, but that is all said. We have got to improve this whole scene.

So I appreciate your coming in, and I appreciate very much your disposition.

Oh, and we have been joined by the gentlelady from Tennessee. So let me yield to her for a question as well.

Mrs. BLACK. And thank you, Mr. Chairman. I apologize for being tardy. It is, as you know, a very busy day, but a very interesting subject, and I appreciate being able to ask a question.

So Mr. Agrawal, I want to ask you: your FPS system, I understand it is working better this year; is that correct?

Dr. AGRAWAL. Yes.

Mrs. BLACK. Okay. So you mentioned the public-private partnership. Are they also working better this year?

Dr. AGRAWAL. I think that partner has continued to grow and expand, yes.

Mrs. BLACK. Okay. So, Mr. Cantrell, are CMS and law enforcement partnerships also working better this year than last year?

Mr. CANTRELL. We are constantly in a state of improvement I would say.

Mrs. BLACK. Do you think that it is working better this year than it was?

Mr. CANTRELL. Our access to data is better than it ever has been. I think we are working very closely to identify that point in time where we turn from administrative action to investigation and prosecution.

Mrs. BLACK. So you both say that it is working better, and yet what we see is an increase rather than a decrease in the fraud. So can you address that, why that might be the case?

Mr. Cantrell, do you want to go first?

Mr. CANTRELL. Sure. I think, one, we have greater visibility. We are seeing more in the data. So we are able to identify more suspect providers. That is potentially part of it, just the fact that we can now see more than we used to be able to see through the data and identify potentially fraudulent providers. That is part of it.

We have seen an increase in our criminal convictions. Once people get past, you know, the front lines of defense of prevention, there are more of them committing fraud against the program than we are actually identifying and convicting. I think that is a product of our deploying our resources based on the data to the areas where the fraud is greatest.

So our Strike Force teams have increased criminal convictions because we are putting our resources in areas where there is the most fraud and the greatest amount of risk. So I think that in part is due to just our being more effective and putting our resources where they can have the greatest impact.

Mrs. BLACK. Would you like to also answer, Mr. Agrawal?

Dr. AGRAWAL. I actually think that was a very complete answer. I agree with it.

Mrs. BLACK. Well, as the chairman has already said, you know, we applaud you for continuing work, but when we see that the numbers are increasing rather than decreasing, and I certainly understand that now that you have a better system where you can identify them that you are going to see more of that.

But we have got to be able to tell our constituents that we are doing everything we can with their tax dollars to make sure we are protecting them. So I will be very interested to hear as you move forward about the successes rather than what we are seeing, the increases.

Thank you.

Thank you, Mr. Chairman.

Chairman ROSKAM. Dr. Agrawal, one other question. Can you divide out how much is fraud versus improper payments?

Dr. AGRAWAL. No, that is a very challenging question. So there is not a ready answer for that kind of question. There is no methodology currently that determines that a claim is fraudulent versus something else.

The center has actually been working on devising such a methodology. We have an initial pilot that we will be launching looking at home health claims.

As you can imagine, in order to figure out that a claim is fraudulent you have actually got to do all of the work in terms of figuring out what is underneath that claim. Was the beneficiary seen? Is there a face to face encounter? Is the order legitimate? Were serv-

ices given? All of that stuff and put it together in a picture of that claim to tell you, yes, this claim is potentially fraudulent or not.

So we have devised such a methodology. We will be rolling it out and trying to arrive at the first real fraud rate in a particular benefit category, but there is currently no such rate that we are aware of.

Chairman ROSKAM. It seems amazing to me. I mean really foundational that you do not have that capacity to be able to discern one from the other. I mean, I am really surprised by that because how do you know how to direct resources then?

Dr. AGRAWAL. Yes. That is a really important question. So the reason it is challenging is because fraud is a legal determination.

Chairman ROSKAM. I understand that it is challenging.

Dr. AGRAWAL. Well, it is more. So, yes, it is hard, but if it takes a legal determination to say that a claim is fraudulent, then that quickly leaves the sphere of control that we have. Right? I mean, that is a criminal justice determination.

What we can do is establish that services were not granted, which is often very indicative of fraud.

Chairman ROSKAM. Look. There is a difference though. So let us not parse the legal stuff. The prosecutors may not be able to prove in a court of law intent and all that sort of stuff, but you know when something is not just a physician who did not check the right box off or write the right sort of question. That is poor documentation.

But if there is a malicious intent to get at this, that is not bad documentation, and it seems like it is a super important point, particularly as it relates to the third point you made in talking to Mr. Crowley, and that was kind of your inherent defensiveness about, hey, this is an access to care issue and if we pull the plug on this, then it is going to adversely impact patients and so forth.

So I find it amazing that you cannot discern between these two, and there is probably nothing that you are going to say right now that is going to take away that sense of wonder.

And we were just joined by the Ranking Member, and with your welcome, Mr. Lewis. I understand that you have been detained. You are now recognized if you would like to be for your opening statement, which can kind of be a closing statement, but it is a good statement nevertheless.

Mr. LEWIS. Well, thank you very much, Mr. Chairman. I must apologize to you and other Members for being late. I had to be over in the other side of the Capitol, another body, to introduce a candidate that the President has nominated to become the Deputy Attorney General. So that kept me.

I understand that we are going through the question phase?

Chairman ROSKAM. We just finished with the first panel.

Mr. LEWIS. Okay. Could I yield to Mr. Crowley to raise a question?

Chairman ROSKAM. Yes.

Mr. CROWLEY. Thank you. Thank you, Mr. Lewis, and thank you, Mr. Chairman.

I think, Doctor and Mr. Cantrell, the image that the chairman has placed is interesting when you look at the difference between

what is then the private sector in terms of Visa and banking fraud, and the number 12.7 percent is an incredible number to look at.

I was wondering though that under the Affordable Care Act you have been given new tools to help go after fraudulent works. Could you describe for us, Mr. Cantrell, some of those new tools in terms of criminal prosecutions and, I believe, denying a real moment by doctors who have conducted willful acts of fraud?

And could you also tell us what would happen to those new tools if the Affordable Care Act were to be undone?

Mr. CANTRELL. Well, I think most of the tools that we were given in the Affordable Care Act are administrative tools that CMS deploys. We were given an initial amount of funding which allowed us to increase our boots on the ground, our agents out in our Strike Force cities, which has been very helpful.

Some of the administrative tools that CMS does have, we worked with them to deploy those tools to stop payments as early as we can in our investigations to support the stoppage of payments in fraud cases.

Dr. AGRAWAL. So you are absolutely right. The Affordable Care Act gave the agency a number of new tools. They provide enrollment standard that you discussed.

We are on a five-year cycle now. We are validating every single provider and supplier in Medicare. We will do that every five years. We are actually at the end of our first five-year cycle.

After nearly being complete with that revalidation process, over 500,000 enrollments have been removed from the program so they can no longer bill.

Mr. CROWLEY. So have doctors actually been disenrolled?

Dr. AGRAWAL. Doctors, DME suppliers, home health agencies, absolutely.

Mr. CROWLEY. For fraudulent acts?

Dr. AGRAWAL. Well, for not meeting enrollment requirements.

Mr. CROWLEY. Under the Affordable Care Act.

Dr. AGRAWAL. Yes.

Mr. CROWLEY. The new tools you were given.

Dr. AGRAWAL. Absolutely.

Mr. CROWLEY. So would that be a tool that would be taken away from CMS if the Affordable Care Act is unmined?

Dr. AGRAWAL. Yes. Our approach to screening and enrollment and revalidation is almost entirely dependent on the Affordable Care Act.

Mr. CROWLEY. So is it fair to say that some of the tools that you have and that you are now employing are starting to make their way through the system and people are beginning to understand just the serious nature of what ought to have been obvious in the first place in terms of the fraud that had been taking place both by physicians and patients? Is that something that you think is happening now?

We should expect to see this number go down?

Dr. AGRAWAL. I think there is a strong sentinel effect of our activities that is beginning to take hold. So, you know, revocation allows us to kick a provider out of Medicare, essentially stopping all Medicare reimbursement. That is very disruptive for the majority of providers.

OIG can actually take a more disruptive action, obviously a very positive one, which is exclusion, and that does not allow them to participate in any Federal program, and I think being able to take on data from the OIG about who has been excluded, being able to take our own revocation actions, they have significant sentinel effects. People see that and say, "I think I need to fly straight," or, "I want to fly straight because I do not want to run afoul of this."

Mr. CROWLEY. Right. So folks who are watching us on C–SPAN or pay attention to this hearing today, this is an opportunity to send a message loud and clear that the sheriffs in town now have new tools.

Dr. AGRAWAL. Yes, sir, all people watching C–SPAN.

Mr. CROWLEY. Under the Affordable Care Act that were not in place before that, and that if they go astray of the rules and of the law, that they will fully be prosecuted under the Affordable Care Act; is that correct?

Dr. AGRAWAL. Yes, sir.

Mr. CROWLEY. I appreciate it.

Mr. Chairman, I do appreciate your hearing today, and I do think this number is a serious number that needs to be addressed. I also believe under the Affordable Care Act and the tools that have been given to CMS and to the Administration as well as over on Justice, that we are going to see that number come down.

And with that, I yield back to the gentleman from Georgia.

Mr. LEWIS. I yield back, Mr. Chairman.

Chairman ROSKAM. I would like to thank our panel for being with us this morning. I appreciate your time and your courtesy and your willingness to invest it with us, and you are dismissed, and we will welcome our second panel to join us.

Well, as we have previously announced, I now recognize Mr. Lewis for his opening statement.

Mr. LEWIS. Mr. Chairman, thank you for holding this hearing and for your work on this important issue.

I also would like to thank all of the witnesses for being here today. Thank you for giving of your time.

On July 30th, 1965, President Lyndon B. Johnson signed a bipartisan law to establish Medicare and Medicaid. It was a great step in realizing a long overdue promise to America's seniors. The Federal Government would never forget the lesson of the Great Depression, where the sick, the poor, and the downtrodden felt hopeless and forgotten.

The success of Medicare did not just happen overnight. It took decades of work, study and negotiation to develop this sacred pact with seniors. For years our predecessors on this very committee worked tirelessly to get the package just right.

We have a responsibility to do everything in our power to ensure that this program continues for generations yet unborn. Today there are about 54 million senior citizens and persons with disabilities who depend on Medicare. These people are our parents, our neighbors and our friends. Every American, especially those who work their entire lives, deserves a Federal safety net. They are entitled to a program that works.

I want to thank the Administration for working with us to fight fraud in the Medicare program. Nearly 50 years ago this Congress

made historic progress in ensuring that every American has a chance to live a healthy, long life. The Affordable Care Act continues that dream. This landmark health care law provided the government with better tools to prevent fraud.

Just last year, the government and Anti-fraud Program recovered more than $3 billion from individuals and companies who tried to defraud the program. In the last three years, this Administration has recovered seven dollars for every dollar spent on anti-Fraud investigations.

These savings have real benefits for Americans who rely on Medicare every single day. We must do all we can to protect Medicare. It is not a Democratic issue or a Republican issue. It is an American responsibility.

Today I look forward to learning what more is needed to fight Medicare fraud and protect this important national treasure.

Again I would like to thank the witnesses for their hard work. Thank you for your testimony.

And thank you, again, Mr. Chairman, for allowing me to read my opening statement, which is later than opening.

I yield back.

Chairman ROSKAM. Always welcome.

Mr. LEWIS. Thank you.

Chairman ROSKAM. Thank you.

Well, we would like to welcome Charlene Frizzera, former Acting CMS Administrator; Kirk Ogrosky, former Deputy Chief of Department of Justice Criminal Fraud and now at Arnold & Porter; Mark Nelsen, Senior Vice President for Risk Products at Visa; as well as Lou Saccoccio, CEO of National Health Care Anti-Fraud Association.

Thank you all for your time today. You heard the previous panel I am sure, and so feel free to interact with things that you heard before either that you agreed with or other points of view or you disagreed with. That I think would be helpful for us today.

We have got your written testimony. It is part of the record, and now you are each recognized for five minutes and then we will follow on with the questions.

So, Ms. Frizzera, welcome.

STATEMENT OF CHARLENE FRIZZERA, PRESIDENT AND CEO, CF HEALTH ADVISORS

Ms. FRIZZERA. I want to thank Congressman Roskam and the Committee Members for inviting me today to talk a little bit about Medicaid fraud.

During my time at CMS, I worked there for over 30 years, and I served as the Regional Administrator in the Philadelphia Regional Office. I was the Director of the Medicaid and CHIP Program under Tom Scully. I was the Chief Operating Officer under Mark McClellan, and I was eventually the Acting Administrator from January of 2009 until Don Berwick and Marilyn Tavenner came.

The reason I think that is important is over a 30-year career span at CMS, I can tell you every Administration wanted to fight fraud, but you know, as I think you will see from my testimony today, based on my visit in Miami, you know, a lot really has not

happened, and I think that there are many ways that particularly the Fraud Prevention System can be used to really do a much better job of detecting and preventing fraud.

I do want to just start out by saying the people at CMS work incredibly hard every day. You know, they have very difficult jobs, and it is easy for me on the outside now to come and tell you what they should do, but as you heard today, there are so many different pressures on them from the beneficiaries to providers to, you know, folks on the Hill to their own internal demands that it is very difficult to really do this job.

However, I do think in the Fraud Prevention System there are some pretty significant changes that can be made fairly easily to make a big improvement in detecting fraud.

As fraud evolves, we must realize that our systems to detect fraud and prevent fraud must change as well. Re-evaluating some of the rules and processes that govern what the agency can do to protect and prevent fraud and the technologies available today that could aid us in better detection and prevention may provide better solutions.

The goal of the Fraud Prevention System is to identify and prevent fraud, waste and abuse in the Medicare fee for service program. The system identifies questionable billing patterns and aberrancies and provides information through an alert system report to the ZPIC contractors. The ZPICs are then tasked to follow up the investigations on particular providers.

To evaluate the effectiveness of the FPS system, there should be clear accountability of the savings attributable to the FPS. The usage of the adjusted savings metric by CMS makes it very difficult to separate the results of FPS from the results that you would get from the many varied systems that were mentioned earlier today.

It is difficult to assess the real returns of FPS when you do not have a control group or any other method to compare it against. Under the current system, the ZPICs get information from many sources, one of which is the FPS. In some cases some of those leads' generations are more reliable than the FPS, and of course, the ZPICs do and should follow the most reliable leads.

But the overlap of effort and lack of accountability attributable to the savings make the evaluation of the effectiveness of FPS difficult and makes it hard to measure FPS against what the ZPICs could have accomplished on their own without FPS.

The impact of FPS to date has been to get more data more quickly to contractors, but the problem is it still uses today the silo-driven fee for service data system that is not multivariate and is limited in its design. We currently have access to greater amounts of data and technology to share that data in a much greater capacity than is used by the FPS.

First, the current system is set up to detect fraud based on historical patterns. We are only able to predict fraud that copies a familiar pattern and are not able to identify new patterns of fraudulent behavior. By limiting our data sets to these variables, we miss associations that could be identified with broader data sets integrated into the system.

By limiting our data sources and only using historical patterns, we may very well be allowing more effective fraud schemes over

time since we are effectively handing over our play book to those looking to commit fraud.

Second, our ability to create informational association should be interagency, as you heard this morning, and should use a more dynamic and open network rather than a closed, fully proprietary system. Under the current contracting rules, the government owns the data and owns the intellectual property. Both of these discourage innovation.

I appreciate the concerns about providing data more broadly and the concern about not owning the intellectual property. However, there exists a faulty underlying assumption in the approach that CMS has the best data and the best fraud tools available in their use.

A reasonable solution would be to allow the use of information from authorized sources, those sources that CMS already entrusts with other pieces of intellectual property, States, commercial plans, contractors and other areas of program integrity outside of the Medicare fee for service program to create a more robust database that will allow for connections that are potentially being overlooked due to the lack of a unified database of information.

The technology available today in the private sector has the ability to rapidly integrate a greater number of data sets and make more efficient associations between this data than is currently being used. The ability to use these more advanced systems and processes is limited by the rules and processes under which CMS is required to operate.

When I was Acting Administrator, actually Mr. Ogrosky and I were in Miami together, and you know, I saw the inability of CMS to be able to stop billings from providers that had aberrant billings on the spot. I saw the lack of the ability to close down a physical site that was simply a storage unit because decisions had to be made and those cases had to be referred to others to decide what to do and whether to continue to pay or not.

You know, watching that is pretty difficult when you see just Medicaid dollars flowing out the door, and there is absolutely nothing you can do to stop that.

Doing something the same way, expending a different answer does not work. Keeping the rules and the process the same will not allow for new ideas and innovation to take place. To truly stay one step ahead of fraud, we need to design a system of processes and procedures that integrate the wealth of information and data available to use today to analyze and detect fraud.

This should include not just better technology, but a systemic and holistic, overall, and redesign of the people and processes that we use in our program integrity efforts. We should give those tasks with identifying and preventing these schemes the best information, procedural architecture and flexibility to ensure the continued integrity of government health care programs and payments.

Thank you.

Chairman ROSKAM. Thank you.

[The prepared statement of Ms. Frizzera follows:]

Congressional Testimony of Charlene Frizzera
President and CEO, CF Health Advisors
Committee on Ways and Means Subcommittee on Oversight
March 24, 2014

I want to thank Congressman Roskam and the other committee members for inviting me to testify today about predictive analytics for detecting Medicare fraud. My name is Charlene Frizzera and I had the pleasure to work at CMS for over 30 years. During my time at CMS I worked in the Medicare and Medicaid programs and on broader health reform initiatives with the passage of the ACA. I served as the Regional Administrator in the Philadelphia Regional Office under Nancy Ann DeParle, the Deputy Director of the Medicaid and CHIP programs under Tom Scully the Chief Operating Officer under Mark McClellan and was the Acting Administrator from January, 2009 until Marilyn Tavenner and Don Berwick came to CMS.

The people who work at CMS believe in the responsibility of taking care of beneficiaries and work hard to fulfill that goal. However, they are often faced with goals that change significantly over time and rules and procedures that can often prevent them from applying more rapid or innovative solutions to their goals. The one thing that we have learned is that fraud is hard to detect and stop. Preventing fraud is so difficult because the schemes and participants are constantly changing, adapting, and evolving to elude enforcement actions.

As fraud evolves, we must realize that our systems to detect and prevent fraud must change as well. I believe that the two main areas that should receive greater attention from lawmakers are the rules and processes that govern what the agencies can do to detect and prevent fraud and the technologies available today that can better aide us in better detection and prevention.

The Fraud Prevention System (FPS)
The goal of the FPS is to identify and prevent fraud, waste, and abuse in the Medicare Fee-For-Service program. The system identifies questionable billing patterns and aberrancies and provides information through an alert system report to the Zone Program Integrity (ZPIC) contractors. The ZPICs are then tasked with the follow up investigation of the provider.

The success of FPS is measured by the amount and speed with which it helps CMS and law enforcement detect fraud and how much potential fraud it uncovers. This is a different metric than simply looking at the amount that CMS actually recovers causing some difficulty in evaluating the performance of the program. The CMS June 2014 Report to Congress on the Fraud Prevention System Second Year Implementation indicated that FPS has saved $210.7M in its first two years of implementation and $54.2M in adjusted savings, which is money that is already returned or likely to be returned. CMS indicated the return is $5 to every $1 invested, however, the GAO, in their June 2014 report to Congress on the FPS, indicated the return was $1.34 for every $1.00 invested. This difference seems to be the inclusion by CMS of savings that either

cannot be substantiated or were not attributable to FPS. The usage of the adjusted savings metric by CMS makes it very difficult to separate the results of the FPS from the results of the ZPICs more generally.

In order to determine savings, there should be a clear accountability of the savings directly attributable to FPS. You can't improve the system if you are not able to justify the real results of the impact of the FPS. Further, it is difficult to assess the real returns of the FPS when we have no control group or other method to compare the FPS against. Under the current system ZPICs get information from many sources, one of which is the FPS. Contractors are held to performance standards and want to stop or prevent as much fraud as possible. In some cases, leads generated by other sources (i.e. beneficiary complaints) are more reliable than those of FPS. In these cases, the ZPIC does and should go with the lead that is the most reliable. The overlap of effort and lack of accountability attributable to the savings, makes an evaluation of the effectiveness of FPS difficult and makes it even more difficult to measure the FPS against what the ZPICs could have accomplished on their own.

Better Approaches to Using Technology

The impact of FPS to date has been to basically get data more quickly to contractors, but it uses the data as it exists today built off of a silo driven FFS database that is not multi-variant and is limited in its design. We currently have access to greater amounts of data and the technology to share that data in a much greater capacity than is utilized by the FPS.

The legislation provides broader authority for CMS to engage the industry than it had taken advantage of. The current FPS develops software to do predictive analytics. However, the definition of predictive analytics is limited to identifying providers that have similar circumstances of known bad actors and then linking them through addresses or phone numbers. This system makes sense, but is fundamentally limited for several reasons.

First, it is set up to detect fraud that is based on historical patterns. This approach is productive, but limits our thinking to exclude other ways that we could identify fraudulent behavior before a historical pattern has been established. Therefore, we are only able to predict fraud that copies a familiar pattern and are not able to identify new patterns of fraudulent behavior as quickly. By limiting our data set to these variables, we miss associations that could be identified with broader data sets integrated into the system. For example, using Tax Identification Numbers from the IRS would allow us to create links between entities that may be different providers in different states with normal spending patterns, but are linked to a single individual who is perpetrating the fraud across multiple provider entities so as to avoid detection. By limiting our data sources and only using historical patterns, we may very well be allowing more effective fraud schemes over time since we are effectively handing over our playbook to those looking to commit fraud.

Second, our ability to create informational associations should be inter-agency and use a

dynamic, more open network of information rather than a closed, fully proprietary system. Under the current contracting rules, the government owns the data and the intellectual property driving the system. Both of these discourage innovation. I appreciate the concerns about providing data more broadly and the concern about not owning the intellectual property. However, there exists a faulty underlying assumption in this approach that CMS has the best data and fraud detection tools available. We currently do not fully know if there are commercial insurance plans, other private third-party program integrity contractors, or even Medicaid programs that have better systems or tools to detect fraud than our current systems. A reasonable solution would be to allow the use of information from 'authorized sources', those sources that CMS already entrusts with other pieces of intellectual property, such as States, commercial plans, and contractors in other areas of program integrity outside the Medicare FFS system, to create a more robust database that will allow for connections that are potentially being overlooked due to a lack of unified database of information.

Our current closed system does not allow for this type of analysis. For example, on the second page of the Executive Summary on the 2014 Report to Congress, CMS highlights in a box on the top of the page that they prevented $700,000 of inappropriate billing. This was accomplished by the FPS identifying inappropriate billing, having the contractor conduct a site visit, interviewing beneficiaries, and reviewing medical records. This is a good accomplishment that clearly was the result of a lot of hard work and coordinated effort. The real question though is whether this could have been accomplished with a more effective use of non-traditional data. Was this provider already excluded from commercial or Medicaid plans for fraud? Now, in this specific example, that might not be the case, but since there is no inter-agency coordination currently we don't know the answer. A simple matching of excluded providers from Medicaid agencies and Medicare Advantage plans may have yielded the same result with greater speed and less resources.

The technology available today in the private sector has the ability to rapidly integrate a greater number of data sets and make more effective associations between this data than is currently being used by CMS. The ability to use these more advanced systems and processes is limited by the rules and processes under which CMS is required to operate.

My Experience with the Miami Regional Office

To highlight these issues, I wanted to leave you with a personal experience that I had while I was the Acting Administrator. I travelled to the Miami Regional Office for a site visit to better understand what the current issues with the program integrity process were at that time. The staff in Miami first showed me a list of the top ten physicians with the highest billing in one county. The top three were off the charts. This information is similar to what the FPS currently provides to the ZPICs today. When I asked them what they do with this list, they told me they send it to the OIG for a decision on whether they will "take the case". In the meantime, CMS continues to pay the claims. Once they get an answer from OIG which could take months, many are no longer in practice so they cannot be found and the money is never recovered. As simple change in the rules to expedite this process or freeze payments pending the OIG investigation could have saved months of fraudulent claims from being paid. The FPS does have systems in place that

certainly improve on this process, but the delayed decision-making still hampers our system today.

Later, on the same visit, we then got in the car and drove to check out the physical locations of some of the providers. One of the sites was a storage space. When I said we should stop paying claims, they told me we couldn't until the NCS, the Medicare contractor that handled provider enrollment, visited the location and verified what we had just seen. Today, anyone with access to the internet can use Google Maps to almost instantly call up a picture of the street view of any address in the country. Now, this will of course not always provide the immediate answer in all potential fraud cases, but using technology to increase the speed and efficiency of the process of fraud detection is clearly a first step. Our understanding of the uses of technology should not be limited to simply the claims data and better algorithm to predict abhorrent spending. There can potentially be greater gains from thinking about how we can apply outside technologies to streamline and ease the human decision making factors that drive prevention.

My experience in Miami left me frustrated with the current rules and procedures that limited the ability, even as the Acting Administrator, to put a swift end to clear cases of fraud in the Medicare program. Since leaving the government, I have had the opportunity in the private sector to witness the technological capabilities available today and to better understand new approaches to program integrity efforts that could further strengthen the efforts of CMS if implemented.

Conclusion

Doing something the same way and expecting a different answer doesn't work. Keeping the rules and process the same will not allow any new ideas and/or innovation to take place. A combination of new thinking and the use and existence of new technology are important considerations in continuing to improve the government's effort to fight fraud, waste and abuse.

The ability of CMS to fight and prevent fraud in the Medicare system is limited to the information it has available and the rules that govern the procedures to investigate and stop fraud. Those looking to commit fraudulent schemes do not face the same limitations. The majority of program integrity initiatives to date have simply been to add new systems and processes on top of an existing infrastructure that has not kept pace with technological innovation and the programmatic changes that have occurred.

Lastly, fraud is not limited to the Medicare FFS system. Commercial plans, Medicaid programs, the Treasury Department, and other commercial entities are currently trying to address these same issues with fraudulent schemes designed to take advantage of lapses in program integrity in the health care system. Today, we have the technological capabilities to integrate these efforts and communicate information and best practices with speed and efficiency. To truly stay one step ahead of fraud, we need to design a system of processes and procedures that integrate the wealth of information and data available to us today to analyze and detect fraud. This should include not just better technology, but a systemic and holistic overhaul and redesign of the people and processes

that we use for program integrity efforts. Those looking to commit fraud face no legal or procedural barriers to develop and operate fraudulent schemes. We should give those tasked with identifying and preventing these schemes the best information, procedural architecture, and flexibility to ensure the continued integrity of government healthcare programs and payments.

Chairman ROSKAM. Mr. Ogrosky.

STATEMENT OF KIRK OGROSKY, PARTNER, ARNOLD & PORTER LLP

Mr. OGROSKY. Chairman, Ranking Member, Members of the Subcommittee, thank you very much for asking me to come and testify today.

The first thing I want to say is that fraud by very definition is a non-self-revealing offense. What that means is that criminals who intend to steal from Medicare fraud are trying to stay away from the system. They are not trying to be detected. They are trying to stay a step ahead of law enforcement.

And like all enforcement endeavors, what I want to tell you is law enforcement depends on the victim of a crime to report a crime. So it is up to CMS to come in and say, "We have been defrauded," and CMS is truly the victim here, but they are the victim representing taxpayers all across the United States.

So I unfortunately have spent almost 20 years working in health care fraud, first as an Assistant United States Attorney in Miami, and I am going to tell you a story about Ms. Frizzera and me in just a moment. I have also been on the board of Lou's organization, and I have been in this business for 20 years, and I hope this Subcommittee and other Members of Congress can put me out of business because I am done. Fraud just keeps getting worse and worse and worse, and I would prefer not to be dealing with it.

So what is critical here? Timely information, timely information from CMS going to law enforcement; information not about what is paid, you know, after several weeks of claims processing, but what is billed; what is billed by criminals. That is what is helpful to law enforcement.

And no matter how many agents and prosecutors and people are assigned, having access to what is billed is really critical, and it is that timely information that makes it possible for prosecutors and agents and others in enforcement to move forward.

And let me just talk about the timeliness for a second. Without timely information, that means that law enforcement is working on stale cases, old cases. Witnesses are gone. You cannot use proactive techniques like a wiretap or a search warrant because the criminals are gone. Money is transferred out of bank accounts today in seconds. It is not written by checks in weeks.

So effective law enforcement lives and breathes on immediate access to information.

Criminals can make decisions in seconds. Government needs to be able to make decisions in seconds. If a code does not pay, a criminal bills something else. It is that simple.

If an audit is coming, a known audit is coming, they prepare for it, and like the representative from CMS said, he is exactly right. You will never see better medical records than those prepared by criminals waiting for an audit.

The medical records where we talk about things that are missing in the record, those are busy practitioners who are treating patients. The medical records that I have seen that look perfect have been in the most egregious criminal cases where people have stolen ten, $20, $100 million for providing no care; cases where people

have been billed for prosthetic limbs who had their limbs; cases where medicine was whipped up in the back rooms of fly-by-night pharmacies where patients did not need it and did not get it.

The case that Ms. Frizzera and I worked on was fascinating because it involved the home health care services that CMS provides that should be saving taxpayer money because it should keep people out of the hospital, but what we saw in Miami was people were diagnosed falsely with conditions that they claimed to be homebound.

I will tell you personally I worked on cases where we went to interview witnesses that were supposed to be homebound, and we could not find them because they were at work, and then when we did find them, they were cutting their grass. And what we found was that they not only were not homebound, they did not have the diseases or conditions with which they had been diagnosed.

And when you take those people to trial and they have providers that are trying these cases, they say, "Well, everyone in our business had the same diagnosis. Every one of the claims we submitted got the same treatment, and we got paid." So that is a real problem that needs to be solved.

So how do we solve that? And back in 2006, we had an idea in the Department of Justice. Rather than wait for the victim of the crime to respond, we were going to look at known fraud schemes in high crime areas. We were then going to take medical professionals who look at the claims and say, "You know what? We do not need to pay for a prosthetic limb for someone who has their limb. We do not need to pay for home care for people who are not homebound."

Those are the types of things that we sought to target, and then accessing that data coupled with the medical personnel and the law enforcement all working together, classic community policing was very effective.

Predictive analytics and modeling and today's technology is even better than it was back in 2006 and 2007. The claims data points should be used by the government to stop the payment of these criminal claims. That is the only way to get this done.

One of the Members of the Subcommittee asked an excellent question. It relies on the coordination and cohesiveness of all of the constituent government agencies that work on this. CMS and their contractors, OIG, DOJ, everyone at the State level at the MFCU, they have to be on the same play book, and they have to be working off the same material.

Thank you.

Chairman ROSKAM. Thank you.

[The prepared statement of Mr. Ogrosky follows:]

Testimony of:
Kirk Ogrosky
Partner, Arnold & Porter LLP
Adjunct Professor of Law
Georgetown University
Former Deputy Chief, Fraud Section, Criminal Division
Former Assistant U.S. Attorney, Southern District of Florida
U.S. Department of Justice

Hearing Title: "Use of Data to Stop Medicare Fraud"
House Committee on Ways and Means
Subcommittee on Oversight

Good morning, Mr. Chairman and distinguished Members of the Subcommittee. Thank you for the opportunity to testify about fraud, waste and abuse in our Medicare program. My experience working in law enforcement and private practice has taught me that, notwithstanding improvements in enforcement techniques over the past ten years, Medicare remains vulnerable to criminals intent on stealing. Further, fraud will not be reduced or eradicated with a "pay-and-chase" enforcement system that relies on criminal prosecution and civil litigation. To protect Medicare and provide needed care for generations to come, we simply must find a way to stop paying fraudulent claims. As such, the use of predictive analytics and modeling to identify and stop fraudulent payments should be the focus of our efforts.

The overwhelming majority of physicians, nurses, healthcare professionals, and companies in this country work tirelessly and honestly to provide care for Medicare beneficiaries. It should always be noted that fraud is the exception, not the rule. The men and women within the Office of Inspector General in the U.S. Department of Health and Human Services (OIG), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), Centers for Medicare & Medicaid Services (CMS) and its contractors, and the state Medicaid Fraud Control Units, should be commended for the work they do to improve and protect the programs. Based on my experience, the government has some of the best and brightest. Yet, notwithstanding these efforts, more can be done to protect taxpayer money.

Fraud control is a difficult business.[1] Those who work to identify fraud are shining a light on what some label a lapse in oversight, and those who fail to identify fraud are promoting the *status quo*. To move forward with an effective fraud identification, deterrent, and policing system, all constituent governmental agencies need to collaborate on setting key strategic priorities and grow a culture that encourages innovation and information sharing.

---

[1] *See* Malcolm K. Sparrow, *Fraud Control in the Health Care Industry: Assessing the State of the Art*, Nat'l Inst. of J., p. 3 (Dec. 1998), *available at* https://www.ncjrs.gov/pdffiles1/ 172841.pdf (Professor Sparrow's research was supported under grant number 94-IJ-CX-K004 by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. His research served as one of the bases which led to the creation and implementation of the *Medicare Fraud Strike Force* model of prosecution).

Pay-and-Chase Enforcement

Recent years have produced increases in the number of individuals being prosecuted, but these cases are still the by-product of a "pay and chase" model of enforcement. Paying out funds and asking law enforcement to try to recover them is a flawed and outdated model. Only with systemic design changes that prevent the payment of fraudulent claims will the amount of fraud be significantly reduced. In this regard, Medicare[2] can learn a great deal from credit card issuers and private health insurance companies. With advances in the ability to analyze claims data, the goal of the system should be to detect fraudulent claims when they are submitted, identify the perpetrators, and to use prosecution sparingly to punish and deter.

Medicare Claims Data

The submission of a claim for payment is an essential piece of evidence in every criminal investigation. In fact, the claim serves as an element of proof that every prosecutor and juror must examine. As a lynchpin of prosecution, jurors intuitively recognize the intent behind providers who submit medically impossible claims. Unfortunately, jurors often are confronted by providers who assert that before the claim was paid, Medicare had the required information and knowingly decided to pay the claim.

CMS contractors typically pay Medicare claims based upon information contained in a Form 1500. If the Form 1500 is correctly filled out, the claim is usually processed and paid without further inquiry or preauthorization. Without understanding more than the information on the form, it is not possible to ascertain whether the service or item was reasonable or necessary. Since 2007, the government has made strides in an effort to use aggregated claims data to identify trends and patterns indicative of fraud, waste, and abuse. As technology continues to improve the ability to examine and analyze vast quantities of data, it is imperative that our federal programs and law enforcement stay ahead of those intent on taking taxpayer funds.

Effective government oversight and enforcement requires collaboration across agencies. And it also requires innovative techniques, such as sophisticated examination of claims data, including predictive analytics and modeling to identify aberrant or otherwise suspicious patterns at the time claims are submitted. There are more opportunities to come as electronic health records (EHR) containing considerable supporting documentation offer new ways for the government to analyze data.

---

[2] Medicare is fundamentally a trust based system. Medicare promptly pays providers and suppliers based on a trust that they order and provide what is reasonable and necessary. Without removing this trust, the question is how to implement changes to the system that balance the risks associated with governmental interference and effective program oversight. Data analytic techniques utilizing the three-prong approach discussed above sought to achieve identification of aberrant behavior without encroaching on the trust granted to providers.

Standing alone, aberrant claims patterns should not be construed as proof of fraud. Aberrations are simply a signal that may require further analysis. This is why the process used by the *Medicare Fraud Strike Force* between 2007 and 2010 required a three-prong approach to claims analysis: (i) prompt access to usable claims data with national means data [CMS and contractors]; (ii) healthcare professionals who understand standards of care and treatment regimens examining aberrations [DOJ and OIG]; and (iii) law enforcement agents with knowledge of communities and current fraud schemes [FBI and OIG]. Without the three components working together, Medicare claims data was an ocean of information that produced more false leads than usable intelligence. After medically unexplainable or impossible claims were indentified, then the traditional work of OIG and FBI agents would begin. In short, access to "big data" opens the door, but access is only attained when true community-based knowledge is coupled with the input from professional healthcare personnel.

Restructuring the Fight Against Fraud

Given estimated fraud losses, I remain concerned that the existing enforcement apparatus is not focused on stopping the payment of fraudulent claims. Criminal prosecution should be the tool of last resort reserved for the most severe perpetrators, not the principal tool used to deter systemic fraud. Time and again, whether it's bogus durable medical equipment claims, unneeded home health agency visits, fake infusion clinics, unnecessary ambulance transports, phony community mental health centers, sham physical and occupational therapy providers, and so on, the payment of obviously false claims must cease. Further, Medicare must be alert to the fact that criminals do not simply stop when claims are denied.

In conclusion, decades of expanding law enforcement, parallel criminal, civil and administrative investigations, do not address systemic weaknesses that allow the payment of obvious false claims. Civil enforcement also has been flooded with hundreds of cases where whistleblowers articulate the issues and DOJ attorneys are required to investigate the issues brought to their attention. While successful at returning a small portion of annual spending to the trust fund,[3] civil and administrative processes should have independent enforcement priorities and agendas. When claims data analysis identifies patterns of waste or abuse, civil and administrative tools, including the False Claims Act, should be used to further the goals of a collaborative system. While whistleblowers play an important role in providing information to the government, so too can a thorough analysis of claims data. There is no need to wait for whistleblowers to drive the enforcement agenda where matters of abusive practices can be evaluated when claims are filed.

---

[3] Since the creation of the HCFAC account, enforcement programs have estimated a return to the trust fund of $27.8 billion. *See* Annual Report of the Departments of Health and Human Services and Justice, *Health Care Fraud and Abuse Control Program* FY 2014, p. 1 (March 19, 2015). The FY 2014 recovery under the HCFAC was reported as $3.3 billion. *Id.* Medicare was billed over $1.2 trillion dollars that year, and paid roughly $400 billion. FCA case recoveries make up the bulk of financial recoveries and yet they do not typically focus on the worst offenders, but instead focus on those capable of settling a case.

Chairman ROSKAM. Mr. Saccoccio.

STATEMENT OF LOUIS SACCOCCIO, EXECUTIVE DIRECTOR, NATIONAL HEALTH CARE ANTI-FRAUD ASSOCIATION

Mr. SACCOCCIO. Thank you. Good morning. Chairman Roskam, Ranking Member Lewis, and other distinguished Members of the Subcommittee, I appreciate the opportunity to testify today on behalf of the National Health Care Anti-Fraud Association, or NHCAA, on the topic of how the use of data analytics can help protect seniors and taxpayers from Medicare fraud.

The United States is projected to spend $3.2 trillion on health care in 2015 and generate billions of claims from health care service providers and product providers. Medicare alone accounts for $633 billion in annual spending, representing more than 54 million beneficiaries.

Additionally, our Nation's health care system hinges upon a staggering amount of data spread across the health care claims adjudication systems of numerous payers. Medicare Parts A and B alone process 4.5 million claims a day.

Given the complexity of the health care system as well as the sheer volume of activity, the challenge of preventing fraud is daunting. There are two strategies which NHCAA believes can be successful in this complex environment. The first is the application of data analytics, including predictive modeling of health care data to identify potential fraud and abuse.

The second is anti-fraud information sharing among all payers of health care, including the sharing of information between private insurers and public programs.

The "pay and chase" model of combatting health care fraud, while necessary in certain cases, is no longer tenable as the primary method of fighting this crime. Clearly, the best way to detect emerging fraud patterns and schemes in a timely manner is to aggregate claims data as much as practicable and then to apply cutting edge technology to the data to detect risks and emerging fraud trends.

One example of the use of analytics at CMS' Fraud Prevention System that Dr. Agrawal already testified with respect to that system and how it operates. It is quite understandable that many are anxious to see immediate, positive results from the investments already made in adopting predictive modeling analysis to Medicare data.

NHCAA would encourage continued patience regarding the use of predictive modeling and data analysis for combatting fraud. It will take time to effectively refine and adjust models for such a large and complex system as Medicare in order to realize the full potential that these power tools offer.

It is also important to note, however, that while the use of data analytics is a key tool in the detection of fraud, it is not a panacea. Anti-fraud units responsible for ensuring the integrity of our Federal health care programs must be staffed sufficiently to meet the challenge that fraud and abuse present.

As we focus on the promise of technology, we must not overlook the vital need for adequate staffing of smart, analytical, insightful

and committed fraud fighting professionals both in the prevention area and also in the law enforcement area.

The second key element in the fight against health care fraud is information sharing. Health care fraud does not discriminate between types of medical coverage. Health care providers who commit fraud build multiple payers, both private and public. 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.

It is precisely this reason why the share of preventive and investigative information among payers is crucial for the effective identification and prevention of health care fraud. Payers, whether private or public, who limit the scope of their anti-fraud information to data from their own organization or agency are taking an uncoordinated and a piecemeal approach to this problem.

Our experience at NHCAA as champion and facilitator and champion of anti-fraud information exchange has taught us that it is very effective in combatting health care fraud. NHCAA's coordinated private-public anti-fraud sharing routinely helps our private side members and our government partners to safeguard and recover funds that would otherwise be lost to fraud.

Another major initiative focused on data analytics and the sharing of anti-fraud information is the Health Care Fraud Prevention Partnership which was launched in 2012. The partnership is a point initiative of the U.S. Department of Health and Human Services and the Department of Justice. It is a voluntary public-private partnership between the Federal Government, States, health insurance plans, and health insurance associations which aims to foster a proactive approach to detect and prevent health care fraud across public and private payers.

NHCAA believes the Health Care Fraud Prevention Partnership is a necessary next step of information sharing. It uses the exchange of payer data, including Medicare data, to conduct targeted studies in particular fraud risk areas.

In summary, harnessing the enormous quantities of data on Medicare in order to identify and predict fraud holds great promise. We support continued investment of resources to enhance and expand CMS' Fraud Prevention System in Medicare.

Additionally, anti-fraud information data sharing among private and public payers of health care is critically important and should be encouraged and strengthened. Health care payers cannot work in isolation and expect to be successful in detecting and preventing health care fraud.

Thank you for allowing me to speak today, and I will certainly answer any questions that may have.

Chairman ROSKAM. Thank you.

[The prepared statement of Mr. Saccoccio follows:]

Statement of Louis Saccoccio

Chief Executive Officer

National Health Care Anti-Fraud Association

on

The Use of Data Analysis to Identify Emerging Trends and

Stop Medicare Fraud

Before the

U.S. House Committee on Ways and Means

Subcommittee on Oversight

March 24, 2015

Testimony of:
Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association

Good morning, Chairman Roskam, Ranking Member Lewis, and other distinguished Members of the Subcommittee. I am Louis Saccoccio, Chief Executive Officer of the National Health Care Anti-Fraud Association (NHCAA). I appreciate the opportunity to discuss with you how the use of data analytics can help protect seniors and taxpayers from Medicare fraud.

NHCAA was established in 1985 and is the leading national organization focused exclusively on combating health care fraud. We are uncommon among associations in that we are a private-public partnership—our members comprise more than 80 of our nation's most prominent private health insurers, along with nearly 130 federal, state and local law enforcement and regulatory agencies that have jurisdiction over health care fraud who participate in NHCAA as law enforcement liaisons.

NHCAA's mission is simple: To protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution and prevention of health care fraud and abuse. The focus of this mission remains constant regardless of whether a patient has health coverage as an individual or through an employer, Medicare, Medicaid, TRICARE or other federal or state program.

I am grateful for the opportunity to discuss the problem of health care fraud with you. In my testimony today, I draw upon our organization's three decades of experience focusing on this single issue. Health care fraud is a serious and costly problem that plagues our health care system, undermines our nation's economy and affects every patient and every taxpayer in America.

The extent of financial losses due to health care fraud in the United States, while not entirely known, is estimated to range from $75 billion[1] to an astounding $640 billion a year[2]. To be sure, the financial losses are considerable, but health care fraud is a crime that also directly impacts the quality of health care delivery. Patients are physically and emotionally harmed by it and as a result, fighting health care fraud is not only a financial necessity; it is a patient safety imperative.

Shockingly, the perpetrators of some types of health care fraud schemes deliberately and callously place trusting patients at significant risk of injury or even death. While distressing to imagine, there are cases where patients have been subjected to unnecessary or dangerous medical procedures simply because of greed. Patients may also unknowingly receive unapproved or experimental procedures or devices. Health care fraud is clearly not just a financial crime, and it is certainly not victimless.

Health care fraud is a complex crime that can manifest in countless ways. There are many variables at play. The sheer volume of health care claims makes fraud detection a challenge. For example, Medicare Parts A and B alone process 4.5 million claims per day. Add to that the fact that fraud can conceivably be committed by any one of the 1.5 million providers of services and products in Medicare, and that those committing fraud have the full range of medical conditions, diagnoses, treatments and patients on which to base false claims. Plus, detecting health care fraud often requires the knowledge and application of clinical best practices, as well as knowledge of medical terminology and specialized coding systems, including CPT and CDT codes, DRGs, ICD-9 codes, and the forthcoming ICD-10 codes.

Plainly, health care fraud can be a challenging crime to prevent and detect. There is no single solution that will solve the problem and the landscape I describe demands that anti-fraud efforts be multi-faceted. A wide range of tools is essential to wage an effective and comprehensive battle against health care fraud.

---

[1] Young, Pierre L. and LeighAnne Olsen, "The Healthcare Imperative: Lowering Costs and Improving Outcomes." Institute of Medicine of the National Academies, 2010. http://www.nap.edu/openbook.php?record_id=12750.
[2] De Rugy, Veronique, and Jason J. Fitchner, "Is Federal Spending Too Big to be Overseen?" Mercatus Center, January 15, 2015. http://mercatus.org/publication/federal-spending-too-big-be-overseen.

My testimony today focuses on two elements which NHCAA believes are critical to successfully combating health care fraud. The first is the crucial role of data analytics, predictive modeling and other technology solutions in being able to prevent precious health care dollars from being lost to fraud. The second is the importance of anti-fraud information sharing among all payers of health care, including the sharing of information between private insurers and public programs.

I. Data analysis and aggregation are essential tools in the health care fraud detection and prevention efforts.

The United States is projected to spend $3.21 trillion[3] dollars on health care in 2015 and generate billions of claims from health care service and product providers. Medicare alone accounts for $633 billion[4] in annual spending, representing more than 54 million[5] beneficiaries. Our nation's health care system hinges upon a staggering amount of data spread across the health care claim adjudication systems of numerous payers. Given the diversity of providers and payers and the complexity of the health care system — as well as the sheer volume of activity — the challenge of preventing fraud is enormous.

We have learned that it is more cost effective to detect and prevent fraud prior to paying a fraudulent claim than to chase the lost dollars after the fact. The "pay and chase" model of combating health care fraud, while necessary in certain cases, is no longer tenable as the primary method of fighting this crime. Clearly, the only way to detect emerging fraud patterns and schemes in a timely manner is to aggregate claims data as much as practicable and then to apply cutting-edge technology to the data to detect risks and emerging fraud trends.

One of Medicare's assets in terms of fraud detection is the enormous amount of data the program generates and collects. According to the most recent Health Care Fraud & Abuse Control

[3] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.
[4] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Table 03 National Health Expenditures; Aggregate and per Capita Amounts. Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.
[5] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Table 17 Health Insurance Enrollment and Enrollment Growth Rates. Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.

Program (HCFAC) report, [6] the CMS Integrated Data Repository (IDR) contains a comprehensive and accurate set of Medicare provider, beneficiary and claims data from Medicare Parts A, B, and D dating back to January 2006. We believe that harnessing and applying analytics to that data could ultimately yield very powerful, game-changing results. The Centers for Medicare and Medicaid Services (CMS) has been dedicating significant resources to facilitate an operational shift to prepayment anti-fraud efforts, including the application of predictive models and other algorithms to Medicare claims through its Fraud Prevention System (FPS). The Small Business Jobs and Credit Act of 2010 established predictive analytics technologies requirements for the Medicare fee-for-service program.

As a result, CMS's Fraud Prevention System (FPS) was launched July 1, 2011. The technology used is similar to that used by credit card companies and financial institutions to detect and prevent fraud. The system, employed by CMS and its program integrity contractors, analyzes Medicare claims data, applying models and algorithms to identify providers and suppliers exhibiting a pattern of behavior that is indicative of potential fraud. Analysis through the FPS includes the use of rules to filter fraudulent claims and behaviors, the detection of anomalies in claims data, predictive assessment against known fraud cases (i.e., predictive modeling), and the use of associative link analysis. This process results in the assignment of risk scores on specific claims and providers which are prioritized for program integrity analysts to review and investigate.

CMS has submitted reports to Congress assessing the first[7] and second[8] years of implementation of the FPS that reveal significant gains and successes. It is quite understandable that many are anxious to see immediate, positive results from the investments already made in adopting predictive modeling and analysis. On that point, NHCAA would encourage continued patience regarding the use of predictive modeling and data analysis for combating fraud. It will take time to effectively refine and adjust the models for such a large and complex system as Medicare in

[6] U.S. Department of Justice, U.S. Department of Health and Human Services. The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2014. March 19, 2015.
[7] Centers for Medicare & Medicaid Services. Report to Congress: Fraud Prevention System, First Implementation Year. 2012. Accessed March 19, 2015. http://www.stopmedicarefraud.gov/fraud-rtc12142012.pdf
[8] Centers for Medicare & Medicaid Services. Report to Congress: Fraud Prevention System, Second Implementation Year. June 2014. Accessed March 19, 2015. http://www.stopmedicarefraud.gov/fraud-rtc06242014.pdf

order to realize the full potential that these powerful technologies offer. Despite the challenges, NHCAA strongly supports this effort.

Many private sector health insurers also have recognized the importance of data analytics to help detect potential fraud and devote resources to apply these tools to enhance their fraud prevention efforts. Seventy-seven percent of respondents to NHCAA's 2013 Anti-Fraud Management Survey[9] (a biennial survey of our private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units) indicated the use of some form of data analytics in their anti-fraud work, including predictive modeling, retrospective modeling, predictive scoring models, data mining queries, billing patterns and rules.

NHCAA supports efforts among its members, both public and private, to shift greater attention and resources to predictive modeling, real-time analytics and other data intensive tools that will help detect fraud sooner and prevent it before it occurs. Investment in innovative health care fraud prevention, detection and investigation tools and programs is vital and should be encouraged.

It is important to note, however, that while the use of data analytics is an important tool in the detection of fraud, it is not a panacea. Predictive analytics can generate leads for further inquiry and can help form the basis for the suspension of payments, but it has not been used as the sole basis for the suspension of payments by private health insurers without additional follow-up and corroboration.

Many of the data analysis and aggregation tools and systems being developed and brought to market are incredibly powerful and can produce potential leads at a pace that can quickly exceed what the finite investigative resources can handle. There is much attention being given to predictive modeling and prepayment analytics, and with good reason. However, the need for "boots on the ground" is as great as it has ever been. Technology professionals and data analysts will be in increasing demand as the use of prepayment technologies grows. And the leads and

[9] The National Health Care Anti-Fraud Association. NHCAA Anti-Fraud Management Survey for Calendar Year 2013. Washington, DC. 2014.

information developed by data analytics will continue to require, in many instances, skilled investigators and medical record reviewers with clinical backgrounds available to act on the information.

It is important that the anti-fraud units responsible for ensuring the integrity of our federal health care programs are staffed sufficiently to meet the challenge that fraud and abuse present. As we focus on the promise of technology, we mustn't overlook the vital need for smart, analytical, insightful, and committed fraud-fighting professionals. We must maintain a multi-prong approach to fighting health care fraud that strikes a balance between technological resources and human resources. So as we continue to extol the promise of cutting-edge technologies for combating health care fraud, waste and abuse, we must also champion the continued investment in human capital. We recommend that in its allocation of funding for anti-fraud efforts in Medicare and Medicaid, Congress recognize the necessity of building a workforce with the numbers, depth, specialization and skill necessary to be successful.

II. The sharing of anti-fraud information among all payers – government programs and private insurers alike — is crucial to successfully fighting health care fraud and should be encouraged and enhanced.

The vast majority of providers of health care services and products bill multiple payers, both private and public. For example, a health care 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 or abuse, each payer is limited to the claims it receives and adjudicates and is not privy to claims information collected by other payers.

Currently, there exists no single repository of all health care claims similar to what exists for property and casualty insurance claims.[10] The complexity and size of the health care system, along with understandable concerns for patient privacy, likely make such a database impracticable. Nevertheless, the absence of such a tool limits the effectiveness with which health

[10] ISO ClaimSearch. See https://claimsearch.iso.com

claims (housed in the discrete databases of individual payers) can be analyzed to uncover potential emerging fraud schemes and trends.

In this environment, fraudsters bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme. Health care 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. It is precisely this reason why the sharing of preventive and investigative information among payers is crucial for successfully identifying and preventing health care fraud. Payers, whether private or public, who limit the scope of their anti-fraud information to data from their own organization or agency are taking an uncoordinated and piecemeal approach to the problem.

Our experience as a champion and facilitator of anti-fraud information exchange has taught us that it is very effective in combating health care fraud. Government entities, tasked with fighting fraud and safeguarding public programs, and private insurers, responsible for protecting their beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest.

NHCAA hosts several anti-fraud information sharing roundtable meetings each year during which private health plans and representatives of the FBI, the Investigations Division of the Office of the Inspector General for the Department of Health and Human Services (HHS-OIG-OI), State Medicaid Fraud Control Units, the Centers for Medicare and Medicaid Services (CMS), TRICARE, and other federal and state agencies come together to share information about emerging fraud schemes and trends. Other information sharing methods employed by NHCAA include fraud alerts, NHCAA's SIRIS database of health care fraud investigations, and our Request for Investigation Assistance (RIA) process which allows government agents to easily query private health insurers regarding their financial exposure in active health care fraud cases as a means to strengthen developing investigations. NHCAA-coordinated private-public

anti-fraud information sharing routinely helps our private side members and our government partners to safeguard and recover funds that would otherwise be lost to fraud.

The Department of Justice (DOJ) also recognizes the benefit of private-public information sharing. Many U.S. Attorney Offices sponsor health care 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. In fact, eighty-seven percent of respondents to NHCAA's 2013 Anti-Fraud Management Survey[11] report that they share case information at law enforcement-sponsored health care fraud task force meetings.

Additionally, DOJ developed guidelines for the operation of the Health Care Fraud & Abuse Control Program (HCFAC) established by HIPAA which provide a strong basis for information sharing. The "Statement of Principles for the Sharing of Health Care Fraud Information between the Department of Justice and Private Health Plans"[12] acknowledges the importance of a coordinated program, bringing together both the public and private sectors in the organized fight against health care fraud.

Despite DOJ's recognition of information sharing as an anti-fraud tool, NHCAA, along with other organizations, saw the need to improve and expand the cooperation and anti-fraud information sharing between the private and public sectors. This concept was a topic of focus during the National Health Care Fraud Prevention Summit hosted by the Department of Justice and the Department of Health & Human Services in January, 2010, in which NHCAA and numerous private insurers participated. This summit set into motion a determined effort to develop and establish a more formalized partnership between government agencies and private sector health insurers. It was envisioned that such a partnership would facilitate anti-fraud information exchange by creating a process to exchange not just investigative information, but to allow the exchange of private and public payer data in a way that could lead to earlier and more effective detection and prevention of fraud.

[11] The National Health Care Anti-Fraud Association, The NHCAA Anti-Fraud Management Survey for Calendar Year 2013 (Washington, DC, NHCAA, July 2014).
[12] United State Department of Justice. Statement on the Principles for the sharing of Healthcare Fraud Information. Updated Sept 2014. See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

After more than two years of discussions and meetings involving several interested parties, including NHCAA, the Healthcare Fraud Prevention Partnership (HFPP) was formally announced on July 26, 2012, at the White House. The HFPP is a joint initiative of the U.S. Department of Health & Human Services and the Department of Justice. It is a voluntary public-private partnership between the federal government, state officials, private health insurance organizations, and health care associations which aims to foster a proactive approach to detect and prevent health care fraud across all public and private payers. NHCAA believes that the HFPP is the necessary next step that takes the information sharing work NHCAA has done, and will continue to do, to a higher level of complexity and effectiveness through the sharing of actual payer data through designated, targeted studies of particular fraud risk areas.

The HFPP has an Executive Board that provides strategic direction and input for the partnership and shares information with the leadership of member organizations. In addition there are two committees:

- The Data Analysis and Review Committee (DARC) focuses on the operational aspects of data analysis and review and the management of the data analytics.
- The Information Sharing Committee (ISC) focuses on sharing the aggregated results and the individual best practices of the participants both internal to the partnership and to external stakeholders.

While the HFPP does not intend to create a national-level all-claims database, it has established several principles and goals that hinge significantly upon the concept of information and data sharing. HFPP partners will work together to combat fraud by:

- Engaging in value-added data-exchange studies between the public and private sector partners.
- Leveraging analytic tools and technologies against this more comprehensive data set.

The partnership and its committees employ a “study-based” approach for data sharing, whereby studies are proposed, planned, executed and analyzed. Smaller, more targeted groups of partners

are typically convened to conduct specific studies. An important aspect of the HFPP is the use of a Trusted Third Party (TTP) to serve as a data-exchange entity for the studies. As envisioned, the TTP conducts HFPP data exchanges, research, data consolidation and aggregation, reporting and analysis. The TTP does not share the source of the data during an exchange in order to keep the identity of the data source confidential.

The HFPP has already completed several studies associated with fraud, waste or abuse that have yielded successful results for participating partners, including studies examining "false store fronts" or "phantom providers," entity revocation/termination lists, misused codes and top billing pharmacies. The misused codes study, for example, examined claim codes, or claim code combinations, that HFPP partners had assessed to be frequently associated with fraud, waste or abuse in the previous six to 12 months, and were associated with large-dollar claims or high utilization. The resulting data exchange proved successful. Schemes and codes that were not thought to be problematic by certain partners were highlighted in the exchange results. The process also confirmed known schemes and misused codes. Further analysis will be conducted and sharing of the results will continue.

At present, the HFPP has nearly 40 partners, including CMS, and it will continue to grow. Ideally the HFPP will foster a national scope by encouraging the participation of eligible public and private entities in the health care industry that are willing and able to meaningfully contribute health care data.

While NHCAA and the HFPP work to promote and improve the effectiveness of data exchange and anti-fraud information sharing, many NHCAA members remain reluctant to fully participate in anti-fraud sharing activities for fear of the potential legal risk such sharing raises. For example, some health insurers are hesitant to share data or information that could lead to litigation brought by health care providers who may be the subject of the shared data or information.

While some states provide immunity for fraud reporting (typically to law enforcement and regulatory agencies, although protections, as well as reporting requirements, vary by state), there exists no clear federal protection for insurers that share information with one another about suspected health care fraud. The absence of such protection creates a chilling effect that leads some organizations to determine that the risk of sharing information outweighs the potential benefit. Although the decision to avoid the risk may seem to make sense to a particular company, the decision results in a negative impact on the overall fight against health care fraud.

In 1996, the Government Accountability Office (GAO) conducted a study titled, "Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts."[13] It examined the issue of immunity and included views and recommendations from NHCAA. The GAO found broad support among federal and state officials, as well as insurers and state insurance commissioners, for a federal immunity statute. Several federal officials interviewed for the report recommended immunity for insurers sharing fraud-related information with other insurers. It's worth noting that this report also examined the idea of establishing a centralized health care fraud database to enhance information sharing and support enforcement efforts.

Based on this report, there seemed to be wide support for federal protections for sharing anti-fraud information. However, the legislation that would have implemented these ideas was not enacted (S. 1088, 104th Congress[14]). Now, nearly 20 years later, we remain essentially in the same situation with regard to immunity. However, the difference is that rather than spending $1 trillion[15] annually on health care as we did 20 years ago, today we spend $3.21 trillion.

NHCAA believes that we should remove unnecessary obstacles that inhibit fraud fighting efforts, and that providing protections for individuals and entities that share information and data concerning suspected health care fraud is a reasonable and prudent step to take. The GAO report

[13] Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts, the Government Accountability Office, May 1996. http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GGD-96-101/html/GAOREPORTS-GGD-96-101.htm
[14] Senate Bill 1088, 104th United States Congress. "Health Care Fraud and Abuse Prevention Act of 1995," Sponsor: Senator William Cohen. http://www.gpo.gov/fdsys/pkg/BILLS-104s1088is/pdf/BILLS-104s1088is.pdf
[15] National Health Expenditure Data, historical 1960-2012, Centers for Medicare and Medicaid Services, Office of the Actuary. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/tables.pdf

discussed above remains relevant to this discussion and may offer worthwhile models to consider.

Conclusion

Health care fraud costs taxpayers billions of dollars every year, and fighting it requires focused attention and a commitment to innovative solutions. There is no silver bullet for defeating health care fraud. A winning fraud prevention strategy for Medicare must be multi-faceted. We believe the following are all necessary components of a successful anti-fraud program:

- The use of data analytics and aggregation;
- A commitment to sharing anti-fraud information among payers;
- The application of rigorous screening processes for providers entering the program;
- The development and adoption of innovative investigative methodologies;
- The continuous investment in an adequate and skilled anti-fraud workforce;
- The aggressive pursuit of criminal prosecutions and the imposition of civil penalties for those who commit fraud; and
- The education of consumers and providers.

The schemes devised by perpetrators of health care fraud take many forms, and those perpetrators are exceptionally opportunistic. As a result, we must stay vigilant and strive to anticipate and identify the risks, and develop strategies to meet them. Right now, harnessing the enormous quantities of data produced by our health care system in order to identify and predict fraud holds great promise. We support continued investment in both time and resources to enhance and implement data consolidation and data mining techniques, including predictive modeling, under Medicare.

Additionally, anti-fraud information and data sharing among private and public payers of health care are critically important and should be encouraged and strengthened. Health care payers cannot work in isolation and expect to be successful in detecting and preventing health care fraud. The establishment of federal protections for those individuals and entities engaged in anti-

fraud information and data sharing would be a major step in encouraging this essential activity, and also would lend strong support for the growth and success of the HFPP as it moves forward. In our view, the HFPP signals a new era of private-public collaboration full of possibility, representing as a significant step in preventing fraud in Medicare and our entire health care system generally.

Chairman ROSKAM. Mr. Nelsen.

STATEMENT OF MARK NELSEN, SENIOR VICE PRESIDENT FOR RISK PRODUCTS AND BUSINESS INTELLIGENCE, VISA INC.

Mr. NELSEN. Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, my name is Mark Nelsen. I am a Senior Vice President of Risk Products and Business Intelligence with Visa. Thank you for the invitation to appear before the subcommittee to discuss some of the ways Visa uses predictive analytics and data insights to help prevent fraud.

While I am not an expert in health care or here to speak to the specifics of Medicare fraud, I do want to share what Visa does in the payments industry to combat fraud as our experience and perspective may be of useful insights to the subcommittee.

For more than 50 years Visa has enabled consumers, businesses and governments to make and receive payments across the globe. Visa works behind the scenes to enable hundreds of millions of transactions each day powered by our core processing network, VisaNet. We invest heavily in advanced fraud fighting technologies to help make digital commerce more convenient, reliable and secure.

As a leader in security, we recognize that there is no silver bullet to protect against fraud. A layered approach that includes a combination of technology, processes, and people is required to prevent fraud, and the use of data analytics is a critical component in making this effective.

Last year alone Visa processed more than 66 billion transactions in global commerce across more than 200 countries. Since the 1990s, Visa payment volume has increased more than 1,000 percent, while the rates of fraud actually declined by two-thirds over the same time period.

Predictive analytics are one of the core tools Visa uses to help limit fraud and make commerce more secure by identifying suspicious transactions before fraud can happen.

Our use of modeling and analytics helps us keep our fraud rates low and stable at less than 6/100 of a percent, that is, six cents for every $100 spent. Visa's analytics are among the most advanced in the payments industry. We evaluate up to 500 unique data elements to spot suspicious transactions as they occur.

Visa uses a continuous feedback loop which enables our stakeholders to inform us in the event that fraud does occur. This allows us to identify patterns across the industry to help predict fraudulent behavior before a transaction is completed.

Visa's advanced authorization is a foundation of our analytics capabilities and provides an instantaneous rating of a transaction's potential for fraud. We examine such factors as account history, geo location, transaction velocity, recent fraud, and other relevant information. This rating occurs as part of the transaction authorization process and enables financial institutions to make a more informed decision about whether to accept or decline the transaction.

All of this happens today in the background for every single transaction that Visa processes in less than one millisecond. Visa

is also beginning to provide this same type of intelligence to merchants.

A recent pilot with Chevron resulted in a 23 percent reduction in the rate of fraudulent transactions at automated fuel pumps. This service is now live at more than 25 gas stations nationwide. This new initiative highlights the value that analytics can bring to address an area where we have seen higher propensity for fraudulent activity.

Another key element of security and fraud prevention that we apply is a method called the common points of purchase. We search millions of transactions to identify unique locations that show a pattern of suspicious activity. We look at historical data to build a picture of what is normal, including typical daily spend amounts, the approved-declined rates, average ticket size, average cross-border spend, and other data elements.

We then compare that picture to what is happening now, and we look for deviations. The deviations become signals that lead to the source for a potential data compromise and allows us to further improve our analytics and prevent fraud.

Criminals know we are searching for patterns, and so we are constantly working to improve our analytics. We incorporate new sources of data as they become available, such as device information, geo location, and we are constantly working to enhance our modeling techniques to yield the best possible results.

As criminal attack vectors evolve, we, too, follow suit and continue to improve, refine and advance our fraud fighting solutions through significant investment, innovation and constant vigilance.

So in closing, the reality is criminals, whether they are cyber, health care, or other types of fraudsters, will always exist, and their tactics will continue to evolve and try to game the system. But the good news is there are sophisticated tools available to help manage these threats. Criminals are a common foe, and each sector must work together to protect against their respective challenges.

Thank you again for the opportunity to testify today. I would be happy to answer any questions.

Chairman ROSKAM. Thank you all for your insight.

[The prepared statement of Mr. Nelsen follows:]

Statement of

Mark Nelsen

Senior Vice President, Risk Products and Business Intelligence

Visa Inc.

House Ways & Means Subcommittee

on

Oversight

Hearing on

The Use of Data to Stop Medicare Fraud

March 24, 2015

Chairman Roskam, Ranking Member Lewis and Members of the Subcommittee, my name is Mark Nelsen and I am Senior Vice President, Risk Products and Business Intelligence with Visa Inc. Thank you for the invitation to appear before the Ways & Means Subcommittee on Oversight to discuss some of the ways Visa uses predictive analytics and data insights to help prevent fraud. I hope my testimony will provide members valuable perspective as the Subcommittee examines ways to help reduce Medicare fraud. While I am not an expert in healthcare or here to speak to the specifics of Medicare fraud, I did want to share what Visa does in the payments industry to combat fraud as our experience and perspective might be useful to the Subcommittee.

For more than 50 years, Visa has enabled consumers, businesses and governments to make and receive payments across the globe. As a global payments technology company, we connect financial institutions, merchants and governments around the world with credit, debit and prepaid products. Visa works behind the scenes to enable hundreds of millions of daily transactions, powered by our core processing network – VisaNet. Visa invests heavily in advance fraud-fighting technologies to help make digital commerce more convenient, reliable and secure.

As a leader in security, we recognize that there is no silver bullet solution to protecting against fraud. There are many different payment environments and types of fraud. A layered approach that includes a combination of technology, processes and people is required to prevent fraud, and the use of data analytics is a critical component in making all three of these areas effective.

Last year alone, we processed more than 66 billion transactions in global commerce across more than 200 countries. Since the 1990s, Visa payment volume has increased more than one thousand percent, while the rate of fraud actually declined by two-thirds over the same time period.

One of the core tools Visa uses to help limit fraud and make commerce more secure is predictive analytics to identify suspicious transactions before fraud can happen. Our use of data, modeling and analytics help us keep our fraud rates low and stable at less than six hundredths of a percent – that's six cents for every hundred dollars transacted.

Predictive Analytics

Visa's analytics are among the most advanced in the payments industry and have helped to identify and prevent billions of dollars of fraud. We evaluate up to 500 unique data elements to spot suspicious transactions as they are occurring, making it more difficult for criminals to use stolen information. We've invested in developing processes and analyzing the data we have to differentiate the good transaction behavior from the bad. This allows us to identify patterns across the payments industry to help predict potentially fraudulent behavior before a transaction is completed. A key aspect in identifying these patterns is the continuous feedback loop we have built to ensure that financial institutions are able to inform Visa in the event that fraud does occur.

Visa Advanced Authorization is the foundation of our analytics capabilities and provides an instantaneous rating of a transaction's potential for fraud by examining such factors as transaction history, geo-location, transaction velocity, recent fraud and other

relevant information. This rating occurs as part of the transaction authorization process and enables the issuer to make a more informed decision about whether to accept or decline the transaction, right at the point of sale. As Visa has visibility across our global network with thousands of issuers, we can use this valuable information to help detect potential fraud. All of this happens today, in the background of every single transaction that Visa processes, in less than a millisecond.

Visa is also beginning to provide this same type of intelligence to merchants. A recent pilot with Chevron resulted in a 23% reduction in the rate of fraudulent transactions at automated fuel pumps. The service is now live at more than 25,000 gas stations nationwide. We believe that providing intelligence to our key stakeholders enables everyone to improve their stewardship of trust in the payments ecosystem. This new initiative highlights the value that analytics can provide to address an area where we have seen a higher propensity for fraudulent activity.

Common Point of Purchase Detection

Another key element of security and fraud prevention that we apply is a method called “Common Point of Purchase” or “CPP.” Card issuing banks and payment networks use advanced analytical tools to search millions of transactions in order to identify those unique locations that show a pattern of genuine transactions followed by suspicious activity on the same card. Such a pattern can indicate a data breach. As with Visa Advanced Authorization, we look at historic data to build a picture of what’s normal for merchants and the individual accounts used at each location. What is the typical daily spend amount? What is the typical approve/decline rate? What is the average

ticket size? What is the average cross-border spend? We then compare that picture to what is happening now, and look for deviations. The deviations become signals that lead to the source of a potential data compromise and allow us to further improve our predictive analytics to prevent future fraud.

Criminals know we're searching for patterns, so we are constantly working to improve our analytics. We incorporate new sources of data as they become available, such as device identification and geo-location, and we are constantly working to enhance our modeling techniques to yield the best possible results. As criminal attack vectors evolve, we too follow suit and continue to improve, refine, and advance our fraud fighting solutions through significant investment, innovation and constant vigilance.

In closing, the reality is that criminals, whether they are cyber, healthcare or other fraudsters, will always exist and their tactics will continue to evolve to try to game the system. But the good news is there are sophisticated tools we are developing and evolving to manage these threats. At Visa, we are able to view transactions across the entire ecosystem and use this information to constantly refine our analytics. More data means that we can more quickly identify trends and work to find new ways to sharpen the analytics to identify trends more quickly. We have a centralized processing system and a strong feedback loop from our stakeholders. This allows us to monitor and respond quickly. Of course, technology cannot completely eliminate human error or internal threats, so it remains critical for businesses to adopt strong policies that are

effectively implemented by their employees. Criminals are a common foe and each sector must work together to protect against their respective challenges.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Chairman ROSKAM. I will turn now to Mr. Marchant on the majority side.

Mr. MARCHANT. Thank you, Mr. Chairman.

In listening to the first panel it became very obvious that there was a lot of theory, a lot of concept, a lot of analytics, and probably more information that they had the ability to act on. I found that to be very discouraging.

In listening to your testimony, it sounds like there is a very large gap between this panel and that in that you are saying that with that kind of information, if it is used properly, this problem is solvable and we can actually make some progress on this.

Is that a correct analysis?

Ms. FRIZZERA. Well, I will start. I will say I totally agree with you, and you heard the first panel. They have more data than they know what to do with.

What I in my testimony, oral and written, what I really talked about is that is true, but there is technology today that can take that data and put it together and make it more useful.

The problem is, as I also mentioned, you know, the government does not want contractors to keep the intellectual property of the product, and I appreciate that because then the government gets stuck with one contractor and, you know, you are sort of beholden to them.

But you know, you have to figure out a way: how do I get new technology? How do I let people keep their intellectual property but do a better job at analyzing that data?

You know, there are folks today that have technology that can identify fraud, waste and abuse before it happens. The problem we have today is we have the claims which are after the fact. So you need to have somebody who can actually engineer that data.

So it is more, you know, the people that we talk to who can do this are more engineers versus statisticians and researcher. You get an engineer and let them reengineer something, that is a very different concept than taking what we have today and appreciate for CMS under all the rules and restrictions they have on them, they do not really have the ability to do that, but that really is, in my opinion, the answer to really trying to make this work much better in the future.

Mr. OGROSKY. Yes, sir. I think there is more data in the system than most people could possibly know what to do with. The question is: how do you design models that are effective at rooting out fraud?

My experience is that the more data points that you have, the easier it is to look for aberrations, and an aberration does not mean fraud. An aberration just means you need to look further.

So what I mean by that is we know in the United States that you do not need a prosthetic limb if you have your legs. So you can look for a diagnosis code, and then look for the product that treats it. You can match disease states with treatments. We know what the standards of care are.

If you see a provider that is treating outside of the standard of care on everything, you will know that that is a real problem. That is why years ago at DOJ we really used nurses to look at those

claims to say these treatments do not match the diagnosis. That is a very simple way.

When all of the patients from one provider do that, it tells you you should not be paying those claims, but it is hard to take action on that in a law enforcement context if you are not learning about it for several years.

So steps have been made to the point now where the question is can law enforcement learn of that at the time the claims start to roll in and can they make those changes, and the more data, it is a question of how to harness that data and create those models to narrow and focus on real criminal fraud.

Mr. SACCOCCIO. Well, you know, the law enforcement piece of it is important and getting timely information to law enforcement is certainly important. But I think the real problem is on the prevention side.

Once the dollars are out the door, once you have law enforcement involvement, you have already in some way lost in the sense that those dollars are lost. So I think any solution really has to focus on prevention, and it has to focus in such a way that CMS could make timely, real time decisions that say, "Hey, wait a minute. We are not going to pay this claim."

You know, they do have suspension authority now. They do have certain things that they do from an administrative standpoint, but I think they have to be somewhat more aggressive, and there is going to be pushback from the provider community. There is no doubt about it, but you have to be more aggressive in saying, "Hey, there is something suspicious here. We are going to stop paying and we are going to stop paying until we figure out whether or not there is a problem."

If there is no problem then we send the check, but right now although there is a focus on prevention, I think to a certain degree there is still the tendency to pay that claim and then figure it out after the fact.

So I think they could do a lot better job on the prevention side, and you know, they have to improve their Fraud Prevention System to be able to do that.

Mr. MARCHANT. Mr. Nelsen.

Mr. NELSEN. Trust in payments is critical to our business, and at Visa we spend more on security than any other part of our business, and so we have architected our solutions so that we can look at all of these data points in real time.

I mentioned in the statement that we create the likelihood of fraud in less than one millisecond, and that comes with a lot of investment and a lot of hard work. It is very hard to pull that off, but it does just require constant investment in these technologies, constant evolution of the models as fraud migrates and as fraud evolves, but that has been the key to our success, is this constant innovation and use of technology as we can.

Mr. MARCHANT. Thank you.

Chairman ROSKAM. Mr. Lewis.

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

Let me thank each one of you for being here, for taking the time to provide us with very important and valuable information.

Mr. Saccoccio.

Mr. SACCOCCIO. Saccoccio. Yes, sir.

Mr. LEWIS. Well, I do not want to mess up your name. So I will not try to pronounce it again.

Mr. SACCOCCIO. Saccoccio.

Mr. LEWIS. Saccoccio. Well, thank you very much.

I am deeply troubled about the fraud cases that harm the recipients of Medicare. Are there other examples that you did not list in your prepared testimony?

Mr. SACCOCCIO. As far as harm to patients, yes. I mean, you know, we often talk about the dollars when we talk about health care fraud, but oftentimes patients are actually harmed, physically harmed, by health care fraud. Unnecessary services are provided. Look what happens on the pharmacy side with the misuse of prescription drugs. Many deaths occur in that arena.

Every year at our annual conference we give an award for Investigation of the Year, and several years ago we actually gave the award for an investigation involving a pain management physician that actually because of the treatments, the fraudulent treatments he was providing, he actually killed two or three patients, and he was sentenced to life in prison under the health care fraud law.

But there are many examples where patients are physically harmed by health care fraud, and I think you have to look at fraud in the Medicare system and throughout the system, not just as a financial issue, as egregious as that is, but as a patient safety issue as well.

Mr. LEWIS. Could you tell the Members of the Committee where there is greater fraud, with individual physicians, health providers, or with institutions like a hospital or clinic?

Mr. SACCOCCIO. Well, that is difficult to point out. Certainly there are some hot areas in health care fraud, and again, not to denigrate any particular type of provider, but certainly home health care has been a hot area. DME has been a hot area. Community mental health I know has been a hot area recently, and they migrate from time to time.

But I would say normally the vast majority of fraud I would say is not so much in the physician area, but in other types of health care providers. That is not to say there are not physicians that are involved in health care fraud, but you will often see that it is in the DME area or home health care or nursing homes, those kinds of facilities where there seems to be higher rates of fraud than, say, your typical physician.

Mr. LEWIS. Are there certain areas of the country where there is a greater degree of fraud?

Mr. SACCOCCIO. Oh, definitely. The Justice Department, their Strike Forces under the HEAT Program focus on certain geographic areas because they are hot areas as far as fraud. Certainly although a lot of work has been done down in Miami and Dade County, still Florida and Dade County are certainly a hot area. Certainly California; certain areas in New York, Houston, Detroit, those areas; there are certain areas where organized crime and enterprise type criminals who enter the system strictly to commit fraud seem to focus their attention.

Mr. LEWIS. Thank you very much, Mr. Chairman. Thank you, sir.

Chairman ROSKAM. Mrs. Noem.

Mrs. NOEM. Mr. Nelsen, can you give me a percentage approximately of what you spend on fraud prevention in relation to the amount of transactions that you conduct in a year's time?

I am just wondering about costs, how much that really is, and if it is feasible for a program such as CMS to utilize.

Mr. NELSEN. You know, we do not disclose how much we spend on security, but like I mentioned it is the single biggest expense of our innovation. So when we look at our global technology spend, security is our highest amount. So I cannot give an exact number, but it is extremely important to us as a business.

Mrs. NOEM. Did it become more feasible as you grew? I mean, I am wondering about volume as well having an impact on the ability to continuously invest in technology.

Mr. NELSEN. Yes, it has. It is interesting. If you look over the past 30 years, our fraud rates used to be much higher, but we continuously invest in both technology, such as chip technology, encryption and data standards, and data analytics is also a core part of that investment.

So it is a combination of both data analytics and technology, but over the time period, over the 30 years, the fraud rate continues to get lower, and we are at near historic lows now, but we still strive to get even lower fraud rates. Our goal is to get it down. We are at six basis points today, but our goal is to get it lower.

So I think that is everyone's goal. There is always opportunity to reduce fraud if you continue to invest in the technology.

Mrs. NOEM. And smaller companies you believe are able to utilize the same technology that you do?

Mr. NELSEN. They can. There is a lot of newer technology available today than there was ten years ago. So ten, 20 years ago when Visa was developing our solutions, it was all proprietary built, but today if you look, there are more software solutions in the marketplace that are using machine learning technologies to help implement and basically better analyze the data that you have.

Mrs. NOEM. How many merchants did you say use Visa or process Visa?

And then do you flag these merchants for certain activities that you would deem to be worthy of watching?

Mr. NELSEN. So we have tens of millions of merchants that use and accept Visa around the world. What we do is we track both fraudulent transactions for our issuing banks. For the merchant tracking, what we typically try to do is look and see patterns of unusual behavior that helps us determine was this merchant breached. Did a data compromise occur at that merchant?

And if we have enough analysis to help prove that there is, then we would initiate what we call a forensics investigation with that merchant to help determine did a breach really occur.

Mrs. NOEM. Ms. Frizzera, you, in your experience because you are so closely tied and have been with CMS, do you think the same technology that Visa is utilizing could be utilized by CMS and be affordable as well to implement and continuously upgrade and invest in the technology?

Ms. FRIZZERA. Yes. I will say the question has been asked 100 times over the past 15 years that I have been involved in some of

these discussions, and I think the point earlier today was it is different. You know, buying a TV is very different than a medical service, and I think the problem that CMS has is the underlying documentation that goes with the claim makes it very hard just to use the claim.

So how do you take that medical documentation and make that part of a record that everyone can use? And I think that Kirk's point earlier, you know, then people just figure out a way to get around the system.

So I think it is hard. They have tried a lot to really figure out how to use the system, but that underlying documentation that supports the claim has always been the problem in trying to really identify fraud outside of just numbers and volume of movement.

Mrs. NOEM. So you do not think there is a way to really scam the claims and use that information in a quick process that would identify it as potentially fraudulent or improper?

Ms. FRIZZERA. No. So you can scan a claim. You can put a claim in a system, and you can run claims against other claims. The claim itself is not really the fraudulent activity. The fraudulent activity is what happened under the claim.

Mrs. NOEM. There should be indicators on that claim though, should there not?

Ms. FRIZZERA. Well, there are some, but again, it is not a claim by claim. It is not like let me scan and look at this claim. It is taking that data together and saying how does that fit in the pattern of other providers and how does it fit into the pattern of that particular provider.

And what we have not been able to do today that I think we can is other information about that provider. So as people talked earlier about commercial payers, you know, there is a lot of other information other than the Medicare fee for service claim which is what we hang all this on, and that is part of the issue with fraud detection. Using the Medicare fee for service claim has its own limitations.

If you can broaden it past the claim to what other payers are saying, so for example, if there is a provider that is excluded from a commercial payer, why does not Medicare automatically exclude them? Right?

So that sounds like an easy question, but Medicare has its own rules. Medicare cannot really say, "Well, I am going to forget my rules." It is statutory. It is regulatory. They just cannot say, "I am going to forget my rules and I am just going to apply these rules."

It takes time. It takes process. So a lot of it is the process that is in place that will not let them move very nimbly to make some of those changes.

Mrs. NOEM. I am out of time. Thank you very much.

Chairman ROSKAM. Mr. Holding.

Mr. HOLDING. Thank you, Mr. Chairman.

I am going to continue on with my line of inquiry on coordination. So, Ms. Frizzera and Mr. Ogrosky, you have both been in the executive branch. Give me some of your thoughts about the barriers to interagency coordination in the executive branch, starting with ladies first.

Ms. FRIZZERA. Well, I will just start with our differences when we were doing this together. So there is a very big tension between a claim or behavior that you know is not acceptable and the time it takes for Justice to do something with the claim, right?

So part of it is that gap between where do you draw the line between, okay, this is good. We are just going to stop paying the claims, and we are going to get overpayments versus saying, "I do not know. This is probably really fraud, and let us send it to the investigators."

And it is not easy. They cannot do that in a short period of time, but with no criteria in between, it is very difficult to figure out where do you draw the line. It may be fraud, but it is not worth it for us to wait time for the Department of Justice and OIG to do their investigations.

So I think it is hard. I think the other honest answer to that is territory. Right? Everybody wants credit for what happens, and it is very difficult when you do not have a system where everybody gets credit for what has happened. Everybody wants their own credit.

So I think, you know, there is a lot of that. The system does not encourage interagency cooperation. It encourages agencies to have their own metrics and their own, you know, rewards for doing a good job.

Mr. HOLDING. But how do you change that?

Ms. FRIZZERA. So, you know, I guess the way I was thinking about it, and I was just thinking about it this morning, think of an ACO for Fraud, right? So all of you guys are responsible for fraud. You all have to figure out how to meet X measure and you all get rewarded and you all get penalized if that does not happen.

So that sounds pretty grand, but if you thought about that again, you know, just think about it that way, not CMS should do, DOJ should do, OIG should do, IRS should do, right? It is really that combination of how do we just make them all responsible?

They have to share the responsibility, the risks and the rewards in doing that.

Mr. HOLDING. So if there was some standard which you could hold it to and say, "All right. You have got to get your fraud rate down or your mis-payment rate down to under five percent, and you figure out how to do it," do you think that would be the stimulating quest?

Ms. FRIZZERA. Yes, and it would be multiple agencies responsible for that. So it is not just CMS all by itself or OIG by itself or DOJ by itself.

Now, I would say that is easy for me to sit here and say, but you know, the times we tried it before, it is hard.

Mr. HOLDING. We have to start somewhere.

Ms. FRIZZERA. It is hard, but that would be one way to think of a new way of doing it in a more coordinated penalties and rewards.

Mr. HOLDING. Right. Mr. Ogrosky.

Mr. OGROSKY. Let me approach it this way and get into the alphabet soup just a little bit. You have MACs paying claims. You have ZPICs determining that the MAC payment is appropriate or not appropriate.

Then you have referrals from the ZPICs that go to the OIG. Then you have the OIG coordinating with the FBI. Then you have the FBI bringing a case to DOJ, and DOJ is then going back to CMS and saying, "Give me the baseline data so I can determine whether a crime has been committed or not."

Mr. HOLDING. Right. Do you happen to know the current placement of Medicare fraud in the priorities established by the Attorney General shipped out to the U.S. Attorneys?

Mr. OGROSKY. I do not. I can tell you that what is interesting to me when I look at the DOJ reports is still almost a third of the entire criminal enforcement of health care fraud happens in Miami-Dade County, two-thirds in the rest of the country, and in the rest of the country there are many districts that do not do much health care fraud at all.

One of the things that Lou and I would disagree on is he said health care fraud does not discriminate among payers. I think, in fact, it does. It goes where the money is, and that is the trust basis system of Medicare. I think private payers have done a much better job of preventing fraud.

Mr. HOLDING. Do we know the fraud rate or the mis-payment rate for providers, this 12.7 percent Medicare? Do we have a private provider that we can compare apples to apples with?

Mr. SACCOCCIO. No. I mean as far as an error rate, I do not think. I have never heard them keep track of it that way again, the distinction between fraud and erroneous payments.

And fraud itself, as Dr. Agrawal said, because of its nature, it is very hard to say what the percentage is. There are percentages that range from three to ten percent of all health care spending in the country that could range anywhere from $70 billion up over $200 billion a year that is lost to fraud, and then what do you consider fraud; what do you consider abuse, you know, depending on the definitions?

On the private side, I have not seen any numbers with respect to erroneous payments as they are defined in Medicare.

Mr. OGROSKY. So private payers have done some things that Medicare simply has not done, like preauthorization for in-patient hospital admissions. I cannot think of any instance in my almost 20 years of doing this where a private payer has spent billions of dollars for a drug to treat HIV that was facially unneeded.

I have not seen any instance where private payers pay for hundreds of millions of dollars of prosthetic limbs that are not needed. So they do a better job when claims come in.

Now, of course, private payers spend a much higher percentage on admin., but you really asked about the coordination, and I think Ms. Frizzera really did a service in answering that by saying the incentives within all of these agencies, it needs to be collaborative and cooperative with a goal in mind of eradicating fraud and doing that means on the front end, the victim, the trustee that administers that fund has control of that process, and that is where it starts.

And law enforcement should be an afterthought in terms of, I mean, it costs money to put people in jail. It costs money to bring cases. These claims should not have been paid to begin with. So

that coordination needs to work across government to bring all that together.

Mr. HOLDING. Thank you.

Thank you, Mr. Chairman.

Chairman ROSKAM. Mr. Smith.

Mr. SMITH OF MISSOURI. Thank you, Mr. Chairman.

I asked the first panel about the FPS and the Zone Program integrity contractors, the contractors hired to investigate fraud. I want to ask you about the relationship between the ZPICs and the Medicare administrative contractors known as MACs.

My understanding is that ZPICs root out fraud and MACs review claims from providers and sign the checks.

Ms. Frizzera, is there any incentive for the MACs to ensure that the claims they are paying are not fraudulent?

Ms. FRIZZERA. Well, there is incentive because they want to pay good claims, but it is not their responsibility.

And, you know, just a little bit of history. So MACs used to do all of this work at some point in time, and then we reengineered the MAC process. Legislation was passed that said we had to look at them differently, and we basically broke up the MAC so that they no longer do all of those services.

So they used to do beneficiary services. They did a lot of the fraud detection. They did all of the claims processing. CMS broke that apart and divided that up so that they would specialize in fraud, waste and abuse detection and paying claims and beneficiary contact.

So they have an incentive in the sense that they obviously want to pay good claims, and some of them do have some programs where they actually do some claim review. They will look at the claims and then also notice that there is some aberrant behavior.

But the ZPICs are ultimately responsible for taking that data and putting it into some tiering process and sending that to the ZPICs for processing.

Mr. SMITH OF MISSOURI. Is there a way for the system to work better?

Ms. FRIZZERA. So I would offer a suggestion really to be to look at all of the Medicare contractors and what do they do and how much money do they spend on what they do, and I would go back to Mr. Marchant's earlier comment. RACs, ZPICs, MACs, there are a lot of acronyms and a lot of people trying to do fraud, waste and abuse.

We have sort of bifurcated it from, you know, fraud, waste and abuse, and it really is all one. It is all one system. You heard today the difficulty of defining the differences between the two. I mean, they have different results. Fraud results in people going to jail, but all of those other activities result in abuse and waste of the system.

And I think that is where there should be much more coordination in that arena in the waste and abuse and among and between the contractors, and maybe even, you know, some redirection of how that contracting process works and who even does it.

Mr. SMITH OF MISSOURI. Do the MACs use FPS' prepayment edits to stop payments before they go out?

Ms. FRIZZERA. I do not know that. Do you?

I do not think it does, but I do not know that for sure.

Mr. SMITH OF MISSOURI. Okay. Mr. Nelsen, I asked the first panel about how they evaluated the outcome of leads generated by their predictive analytic system. Does Visa have metrics to determine performance?

Mr. NELSEN. Yes. We create different models for different segments. So we have models for e-commerce fraud, for credit, for debit, and so for each model that we create we have a performance metric that we share with our issuing banks, and they can then use that performance metric to determine what degree of false positive do they want to accept from the approve or decline perspective.

So every time we create a model, we have those performance projections that we publish.

Mr. SMITH OF MISSOURI. So you all do have track of false positives?

Mr. NELSEN. Yes, absolutely.

Mr. SMITH OF MISSOURI. All right. Thank you, Mr. Chairman.

Chairman ROSKAM. Mrs. Black.

Mrs. BLACK. Thank you, Mr. Chairman.

Very interesting subject matter, and I am just trying to put it all together. I actually tried to diagram all of this, and I have got the FBI, the OIG, the CMS, the DOJ, the ZPICs, the MACs, the RACs. When you start looking at what the cost of operating all of these various divisions, I know that the security piece that folks like Visa use has got to be expensive. I know Mr. Nelsen talked about how it is a great percentage of their budget.

But it seems to me that that would certainly be a savings in the long run when you look at the cost of all of these because it is a "pay and chase," and getting any of that money back is very difficult to do.

So, Mr. Ogrosky, I think one of the things that you said that you thought when you looked at the private sector insurance companies was the preauthorization piece. Do you, Ms. Frizzera and Mr. Ogrosky, believe that that is something that we possibly should be looking at on the Medicare side, is the preauthorizations as opposed to the "pay and chase"?

Ms. Frizzera, how about you first and then Mr. Ogrosky?

Ms. FRIZZERA. So I will say every time we try to do that physicians go crazy, or hospitals, whoever the provider is. So you definitely delay the payment when you put a process in like that, and the complaint is you are hurting the good guys for the bad guys so that the majority of us are doing the right thing, but we have a delayed payment because, you know, we have to allow you to prevent the bad guys.

So you know, I think there are policy issues that come out of these claimed processings. So a lot of times you will see, well, this is not right, but when you really look at what is happening, it is a bad policy, and the policy needs to be changed and adjusted to stop the waste and abuse project.

I do not know that I would say that the preauthorization for hospital admission is workable in a system like CMS when you have so many beneficiaries, and quite honestly so much pressure on CMS to pay timely claims, and when providers do not get paid,

that is a pretty big problem and it becomes everybody's problem here. It becomes everybody's problem at CMS.

So anything that delays that payment probably will cause a lot of problems. However, I do think there is an additional piece that CMS could do which is really revising policies when they see things happening that are creating waste and abuse.

Mrs. BLACK. Because it is working in the private sector, and people do get paid timely in the private sector. So I would like to explore that a little bit more about why that does not work in the public sector.

Ms. FRIZZERA. Yes. So I would just add one quick comment in defense of CMS. The private payers do not have the same pressures that CMS has in paying providers publicly. Right? It is a very public program. So anything that we do not do, anything that CMS would not do becomes a big public problem.

Private payers really do not have that same responsibility to publicly announce that they are stopping payment. So I think the public perception is one of the issues around CMS that makes it a little bit harder for them to do some things that maybe commercial payers can.

Mrs. BLACK. Mr. Ogrosky, you mentioned it. So let me turn to you.

Mr. OGROSKY. So I am by no stretch of the imagination an expert in how to run an insurance company, which is what CMS is. Private insurance companies have put in checks and balances over the years that do things like preadmission, preauthorization.

When you have 50 million people, the bulk of whom are over 65, the rates of hospital admission are very different. That is a different thing.

The administrative cost that private insurance companies run compared to the administrative cost that CMS runs is a lot different also. So there are different factors here that go into it.

My thinking is Medicare has been since the 1960s to today a trust based system, and that trust is earned by the majority of providers in the community. They file legitimate claims. They work hard.

We are talking about finding ways to close those loopholes or minimize that margin, whether it is five percent or ten percent, to eliminate that, and some of the ways of thinking about it are if we cannot get rid of the outright criminal fraud, you know, then spending our time second guessing a doctor's decision on whether someone needed to be in this status seems to me to be a real waste of resources.

So I do not know the right way to design it. I do know that on the other question that was asked about the structure of the system, there are a lot of components that are expensive, but you know, everyone needs to figure out how to work together, and there are some government agencies that work great together.

Mrs. BLACK. I cannot see how much time I have left, Mr. Chairman. Am I still——

Chairman ROSKAM. Seconds.

Mrs. BLACK. Oh, seconds. Well, I was going to go to the historical patterns and try to figure out how do you get these historical patterns to be able to determine when there is a possibility of a

fraud or the improper use of a certain procedure or a device, so to speak. Someone has legs but they get a prosthetic.

Mr. OGROSKY. So historical patterns, if you look at fraud cases over the last 20 years, they are replicating fraud patterns. You see most criminals are not highly sophisticated. They copy what they see in the community.

So basic community policing knows that low barrier to entry companies, whether they are DME, home health care, some pharmacies, companies where you do not need a medical degree, you do not need a high school degree; you can go in and get a provider number; those low barrier entry companies are the ones that tend to have patterns of repeating fraud.

And if you look at the data from each community and you do not compare it to the averages across the country but you compare it to the mean for Medicare beneficiaries, you can very quickly see DME, ambulance, home health. These things just pop off a page, and they are repetitive.

And as much as we would try at DOJ to tackle and reduce those rates, and we were able to see it in the claims data, as soon as the DME would drop, the home health would go up. So the criminals are on the move.

Mrs. BLACK. Thank you, Mr. Chairman.

Chairman ROSKAM. Thank you.

Let me just ask a few closing questions, and I will sort of gallop through these kind of quickly, but they are important, I think, for the record and to bring this discussion to fruition.

Mr. Nelsen, there has been a lot of discussion about paying and the delay of payments and so forth. How does Visa mitigate? You know, you have got an unhappy merchant who is part of your system and you want to keep satisfied, but how do you all mitigate that relationship if the argument is, "Hey, look. You have got an unhappy provider here," and so forth?

Can you walk us through that parallel and just give us some insight?

Mr. NELSEN. Yes, that is a good question. So it is a little bit different for Visa because our relationship is with the acquiring bank. So each merchant has an acquiring bank, and so we would go after the acquiring bank if there is a fraud case, for example. So it is up to the acquiring bank to actually go to each individual merchant to collect the funds.

So for our perspective, it is a little bit easier in terms of how we manage and monitor the system.

Chairman ROSKAM. How long does that process usually take?

Mr. NELSEN. It depends. It depends kind of by geography. It can be fairly quick, a couple of days. It could be a couple of weeks as well.

Chairman ROSKAM. Are you able to discern between a fraudulent claim, a false claim, and an error?

Mr. NELSEN. That is a little bit more on the issuing side. Since we have zero liability, some consumers will take advantage of that and they will claim it is fraud, but it may actually be the genuine consumer. So the issuing banks deal with that to some degree. We call it first party fraud, and they will have to do some due diligence

to say did this person really do this or not, and that is going to be up to each individual bank to determine was it really fraud or not.

But the banks will use our tools to help assess that. So if it is within a pattern and the risk scores are low, the bank can use that to help determine, hey, this is actually maybe the genuine consumer.

Chairman ROSKAM. So a question for Mr. Nelsen and Mr. Ogrosky.

Can you help us discern this concept that has been floating out there today? CMS asserted earlier, hey, there are all of these other data points and that makes our life more complicated. Is there not an argument that says: no, no, no. If you have more data points it is actually more helpful?

Who is right? What is up with that?

Mr. OGROSKY. So I will answer it from my perspective, looking at the data and analyzing claims data, and I like claims data. I do not need an electronic health record to be able to spot patterns and trends.

Basic data points on a health care claim, you cannot look at just one claim standing alone. You look at the providers in a community and you look at all of their claims, and what I see in claims forms are really some basic things that are very helpful.

Does the diagnosis match the service?

Is the doctor alive?

Is the zip——

Chairman ROSKAM. Crazy, that. Wow.

Mr. OGROSKY. Is the zip code within the same region as the provider? Like is the patient's home address near the provider?

Chairman ROSKAM. Now, just for my benefit, is that billing information? So walk me through. You have got an underlying medical record, right? That is not what you are really talking about.

Mr. OGROSKY. No, I am talking about——

Chairman ROSKAM. You are talking about claims.

Mr. OGROSKY [continuing]. The 1500 form. It used to be the HCFA 1500 form.

Chairman ROSKAM. And that is all you have got to look at? That is what you are saying?

Mr. OGROSKY. That is what I have always used. You have the name of the beneficiary. You have their Medicare number, which is the Social Security number. You have their home address, where they live. You have the name of the provider. You have the doctor, the ordering physician, and you have the service or the item.

So you have all of this information. Now, if I wanted to know, and I have seen cases where the provider is in, let us say, Miami and is servicing patients from all over the country. Well, how would that be possible?

Well, it is theoretically possible. They could have all traveled to Miami, but then you look at the next thing. Does the diagnosis match the treatment? And then I would consult with a nurse and say, "Gee, you know, they have ordered all braces for people diagnosed with arthritis. Do you brace an arthritic joint?"

And the nurse would say, "No, you do not brace an arthritic joint. You flex an arthritic joint."

So there is enough information for me to be able to look at that claim form and flag it as an aberrational claim form.

Now, once it is flagged as an aberrational claim form does not mean that the provider has committed fraud. There could be a specialist out there that has a unique treatment. But then what you do is you refer it and a ZPIC or someone goes out to see does this company actually exist.

And what I would find when we would send people out from OIG or from some of these agencies, they would show up at the provider and it would not exist.

Chairman ROSKAM. So can I put you in the Peter Roskam camp of more data is better?

Mr. OGROSKY. I think so.

Chairman ROSKAM. Okay.

Mr. OGROSKY. I think there are many choices.

Chairman ROSKAM. Stop talking. Perfect.

[Laughter.]

Chairman ROSKAM. That is right where I want you.

Mr. Nelsen, what do you think?

Mr. NELSEN. I would agree more data is generally better. I think one of the challenges though is organizationally a lot of times data is siloed within different databases. So in order to really use it——

Chairman ROSKAM. That is a serious point.

Mr. NELSEN [continuing]. You have to develop and engineer the systems that can get access to the data in real time to either build the models or analyze the activity.

Chairman ROSKAM. Yes.

Mr. NELSEN. But if you can use the data, then it is valuable.

Chairman ROSKAM. Okay. So just last little line of inquiry. Ms. Frizzera, should CMS be able to discern between improper payments and fraud?

You heard me. I was surprised.

Ms. FRIZZERA. Yes. Well, I will say they should. They should, and I think the distinction really is they can distinguish it, but people continue to put it in the same bucket. Right? So everybody calls it fraud. It really is not. I mean you can redefine fraud differently.

Fraud is defined as people illegally using the system, and fraud in the way it has been interpreted and used are the really bad guys just really scamming the system.

Improper payments, maybe not. Maybe they are just scamming the system a little bit. It is just improper.

So I think it is the definition that makes that very hard, and when people talk about fraud, they include all of that, and it is not the same. Fraud is really, you know, when you have the Strike teams and you see the data about real fraud. They put people in jail. That is fraud. That is very different than the waste and abuse, and improper payments are in that bucket.

So I think the difficulty is people tend to put it all into one bucket, but I think if you defined fraud as people who go to jail, they can give you those differences. I think the definition is just very unclear today when you ask the question.

Chairman ROSKAM. So let me just wrap up. I know I speak on behalf of the Ranking Member and every Member here. It has been

really helpful for us to get your perspective. Your time is valuable, and you have been generous with your time today, and we really, really appreciate it.

One point, and that is the general concern about slowing down of payments, and there is clearly a sensitivity to that. But if you look at the reality and kind of the broader picture, we have a sort of Damocles over our head, and the sort of Damocles is an SGR that will come to an end, which what does that mean? That means a 22 percent payment cut for providers which is unpleasant and miserable. That is not slow. That is never coming.

Now, you know and I know it is going to get fixed, but I think we need to think more broadly in the totality of there is plenty of money for us to deal with this system. There is plenty of money to make sure that seniors are cared for and to Mr. Lewis' point that nobody is left on the side here.

But we absolutely need to be much, much smarter about how we do this, and I know that this Subcommittee and the Members who are on it on a bipartisan basis are passionate about this.

I will make one other point. A lot of times we conflate, and this is a point that you made Ms. Frizzera. You conflate these concepts of waste, fraud and abuse, and they become almost a phrase that we chuck out. And the more I have thought about this responsibility that I have now, I begin to think of them in different ways.

Abuse is what we heard last month at this Committee. The IRS had been abusing people with civil forfeiture. That is the misuse of government power, poorly place on someone that is used to a bad end. That is civil forfeiture that was abusive.

Fraud is that hustler, that manipulator, somebody that comes and gains a personal gain, a pecuniary gain, but it's ill-gotten.

And waste is something different. Waste is, you know, ordering the pencils and paying too much for them or leaving the lights on or being stupid and gratuitous while it is easy to spend other people's money.

And that sort of construct has been helpful for me to think about the responsibility of this Subcommittee. But here is what I know. I know that we have got to do better. I know that on a bipartisan basis with the help of all of the Members of this Subcommittee we will do better, and your insight today, all four of you, is very, very helpful, and I know I speak for every Member in thanking you.

Thank you. The hearing is adjourned.

[Whereupon, at 12:34 p.m., the Subcommittee was adjourned.]

[Member Submission for the Record follows:]

George Holding, letter

W&M Oversight Hearing on Medicare Fraud
March 24, 2015
Statement for the Record
Congressman George Holding

Thank you Mr. Chairman, for your leadership in exploring the use of data analysis to identify emerging trends that will help to eliminate Medicare fraud. I think it is fair to say that all Members of Congress would like to identify and prosecute fraudulent providers in the Medicare program. I support the development and use of tools that target these bad actors and ensure that they do not continue to garner any benefit from the program. I believe that it is important to use every tool available in the marketplace today to achieve this goal, and I am looking forward to learning about these tools from each witness today.

[Public Submission for the Record follows:]

Federation of State Medical Boards, letter

Federation of STATE MEDICAL BOARDS

March 24, 2015

The Honorable Peter Roskam
United States House of Representatives
2246 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Lewis
United States House of Representatives
343 Cannon House Office Building
Washington, D.C. 20515

Dear Chairman Roskam, Ranking Member Lewis, and Members of the Ways and Means Subcommittee on Oversight:

On behalf of the Federation of State Medical Boards (FSMB), I am pleased to submit the following letter for the record in accordance with today's hearing on the federal government's use of data analysis – namely the Centers for Medicare and Medicaid Services' Fraud Prevention System (FPS) – to combat Medicare fraud. The FSMB strongly supports your mission to improve program integrity and provider screening procedures in order to tackle waste, fraud, and abuse in the Medicare and Medicaid system.

The FSMB is committed to partnering with and supporting federal health and law enforcement agencies to combat fraud and abuse, particularly the Centers for Medicare and Medicaid Services (CMS), the Department of Health and Human Services Inspector General (HHS OIG), and the Department of Justice (DOJ). In this capacity, the FSMB welcomes the opportunity to provide assistance with physician licensure and disciplinary data monitoring.

About the FSMB

Founded in 1912, the FSMB is the national non-profit organization representing the 70 state medical and osteopathic boards of the United States and its territories. With offices in Texas and Washington, D.C., the FSMB serves as the collective voice for state boards and supports them in protecting the public health and safety.

Improve Provider Screening and Monitoring

It is estimated that approximately $60 billion is lost annually as a result of waste, fraud, and abuse in Medicare and Medicaid. In recent years, CMS has taken proactive steps to address this matter, and has sought to replace the "pay and chase" model with the utilization of new technologies and databases to conduct predictive analytics and improve provider screening procedures.

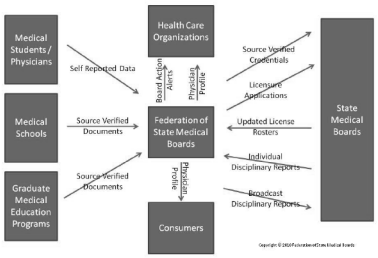
The FSMB applauds these efforts, and strongly believes that CMS' predictive capabilities would benefit from consultation with state boards' physician licensure and disciplinary data. For this reason, in 2011, the FSMB endorsed Chairman Roskam's legislation, *H.R. 3399, The Medicare and Medicaid Fighting Fraud and Abuse to Save Taxpayers' Dollars Act (The Medicare and Medicaid FAST Act)*, which recognized the inherent value of state medical licensing data, and its ability to improve program integrity and help identify fraudulent providers. With nearly a quarter of physicians holding more than one state medical license, it is imperative that all state licenses be screened and monitored simultaneously for fraudulent activity.

The FSMB Physician Data Center

The FSMB retains a central repository of physician licensure and disciplinary data. The FSMB was the first organization to publish and distribute the names of the nation's disciplined physicians. That information is now disseminated electronically via the Federation's Physician Data Center (PDC), a repository of board action and licensure data on U.S. physicians that contains thousands of disciplinary actions dating back to the 1960s. The PDC receives regular updates from medical and osteopathic boards upon taking disciplinary actions against physicians and physician assistants, which would negate the need for CMS to contact each individual board.

Within the Physician Data Center, the FSMB maintains a central repository of formal actions taken against physicians and physician assistants by state licensing and disciplinary boards, the Department of Defense, the U.S. Department of Health and Human Services, and a growing number of international regulatory organizations, including Canada, England, Australia and New Zealand. The FSMB's data flow chart is presented below.

FSMB Data Overview



As the preeminent resource for board action information, the Physician Data Center is routinely consulted not only by licensing and disciplinary boards, but also by military, governmental and private agencies and organizations involved in the employment and/or regulation of physicians.

To be included, an action must be a matter of public record or be legally releasable to state medical boards or other entities with recognized authority to review physician credentials. Among the actions included are revocations, probations, suspensions, and other regulatory actions, such as license denials and reinstatements, consent orders, and Medicare exclusions. Certain actions reported to and released by the Physician Data Center are not disciplinary or otherwise prejudicial in nature. Such actions are reported to ensure records are complete and to assist in preventing misrepresentation or the use of lost or stolen credentials by unauthorized persons.

The FSMB has established comprehensive quality assurance procedures to enhance the accuracy and integrity of its information. All data is extracted from multiple data sets and is cross-checked and matched for accuracy with updates being provided on a regular basis. Disciplinary sanctions and other board actions are reported to the FSMB by state medical and osteopathic boards and other regulatory entities on a regular basis. These reported actions are verified in writing and accompanied by supporting documentation, such as copies of board orders, findings of fact, conclusions of law, final decrees and stipulations.

The PDC offers two services for its customers: physician profile reports and disciplinary alerts; both services are recognized as primary source equivalent by the National Committee for Quality Assurance (NCQA) and the Joint Commission on Accreditation of Healthcare.

- **Physician Profile Reports** are queries identifying actions reported on specific individuals. The service provides information pertaining to any actions contained in the PDC and also provides a historical view of disciplinary actions taken by reporting entities.
- **Disciplinary Alerts** are provided via a continuous monitoring service that can alert CMS and OIG to recently adjudicated cases. CMS would provide a list of practitioners that would then be uploaded to be screened against reporting entities on an ongoing basis. A Daily Disciplinary Alert Report would be provided to CMS to notify them that enrollees have had actions taken in other states, allowing for nationwide tracking and monitoring.

PDC users are categorized by customer type, including: credential verification organizations (CVOs), government entities (U.S. Department of Veterans Affairs), hospitals, insurance carriers, physician associations, medical groups, medical societies (American Board of Medical Specialties (ABMS) specialty boards), medical licensing authorities (state medical boards; international regulatory authorities), managed care organizations and placement services (locum tenens). For 2014, nearly 230,000 queries were processed for commercial customers and nearly 80,000 queries were performed on behalf of state medical boards.

Proposed Utilization of Physician Licensure and Disciplinary Data

The FSMB would be able to provide a solution that supports the CMS Provider Enrollment, Chain, and Ownership System (PECOS) and assist in verifying licensure status for CMS eligible providers and monitor that status for those physicians on an ongoing basis. In order to meet this requirement, FSMB recommends adding Medicare and Medicaid providers into the Federation's Disciplinary Alert Service (DAS). As with all technical implementations, the final solution would require detailed coordination between the FSMB and CMS. We envision a process to work similar to the following scenario.

The first step of this process would be the submission of a provider list to FSMB from CMS and its Center for Program Integrity (CPI). The FSMB would then validate this list against its current provider directory and send an acknowledgement of a matching record that includes the current status of each provider's medical license. All data would be exchanged in an agreed upon data record format.

After the initial load of this provider listing, any change in the status of a physician's license, due to an action taken by a medical or osteopathic board, would be immediately reported to CMS/CPI. This will assist CMS in identifying high-risk providers, and those suspected of fraud and abuse.

The FSMB would also be able to assist the OIG in meeting its needs to identify providers fraudulently submitting claims without a valid license. Given that the OIG requires copies of board orders that have resulted in the suspension or revocation of a physician's license by state boards when actions occur, the OIG would benefit considerably from streamlining its processes and receiving board orders as they occur and from a single source. The FSMB has the capability to provide the OIG with board orders daily and a weekly summary report that will allow the OIG to reconcile board orders received.

Following a contractual agreement, the FSMB Physician Data Center would be able to provide and update the databases of CMS, OIG, and DOJ with data matching capabilities for all disciplinary actions taken by state medical boards in any given time frame, allowing the agencies to track and monitor nationwide those physicians suspected of fraud, illegal prescribing practices, or other offenses. Moreover, the FSMB's data monitoring capabilities would assist CMS and OIG with preemptively identifying claims that are being submitted by providers whose licenses have been revoked, suspended or restricted in some other manner that would make them ineligible to submit valid claims for service reimbursement.

Conclusion

The FSMB offers its strong support to the U.S. Congress and the appropriate federal agencies as they seek to devise and implement new mechanisms to combat waste, fraud, and abuse in Medicare and Medicaid. The FSMB would be pleased to meet with you to discuss our capabilities to assist with improving program integrity and provider screening procedures. We thank you for your bi-partisan leadership on this important issue, and look forward to working with you, Congress, and the Administration.

Sincerely,

Humayun Chaudhry, DO, MACP
President and Chief Executive Officer
Federation of State Medical Boards

○