Statement of Louis Saccoccio

Executive Director

National Health Care Anti-Fraud Association

"Can New Technology and Private Sector Business Practices Cut Waste and Fraud in Medicare and Medicaid?"

Before the

U.S. Senate Committee on

Homeland Security & Governmental Affairs

Subcommittee on Federal Financial Management, Government Information, Federal Services, & International Security

July 12, 2011

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

Good afternoon, Chairman Carper, Ranking Member Brown and other distinguished Members of the Subcommittee. I am Louis Saccoccio, Executive Director of the National Health Care Anti-Fraud Association (NHCAA).

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 85 of the nation's most prominent private health insurers, along with more than 85 federal, state and local government 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. The magnitude of this mission remains the same regardless of whether a patient has private health coverage as an individual or through an employer, or is covered by a public program such as Medicare, Medicaid, or TRICARE.

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 25-plus years of experience focusing on this single issue. Health care fraud is a serious and costly problem that affects every patient and every taxpayer in America. The financial losses due to health care fraud are estimated to range from $75 billion to a staggering $250 billion a year. These financial losses are compounded by numerous instances of patient harm—unfortunate and insidious side effects of health care fraud.

Health care fraud is an exceptionally complex crime that manifests in countless ways. There are many variables at play. Considering that billions of medical claims are generated in the United States every year, the sheer volume of health care claims makes fraud detection a challenge. Medicare alone pays 4.4 million claims per day to 1.5 million providers nationwide. Anyone in the system can conceivably commit fraud, and those committing fraud have the full range of medical conditions and treatments and the entire population of patients on which to base false claims. 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. Clearly, health care fraud can be a challenging crime to prevent and detect. The perpetrators of this crime have proven themselves to be creative, nimble and aggressive. Therefore, investing in and employing the most effective fraud prevention and detection techniques is critical to achieving success.

Beyond the monetary losses, health care fraud is a crime that directly affects the quality of health care delivery. Patients are physically and emotionally harmed by health care fraud. 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, dangerous and invasive medical procedures simply because of greed. Consequently, fighting health care fraud is not only a financial necessity; it is a patient safety imperative. Anti-fraud efforts identify and prevent unnecessary and potentially harmful medical care and procedures.

Additionally, anti-fraud efforts identify dangerous prescription drug abuse by patients, overprescribing by some physicians, and involvement by some pharmacists who are complicit in the scheme. Prescription drug abuse is a growing problem. Addicts will go “doctor shopping” in order to get multiple prescriptions from several physicians and will then fill them at different pharmacies. Often, it’s the insurer who is best able to connect the dots and identify overprescribing by physicians and prescription drug abuse by patients. NHCAA also sees promise in state prescription drug monitoring programs as a means to not only identify fraud but

to protect patients. Encouraging state investments in these monitoring programs through incentives is a worthwhile consideration, as is examining interoperability among state programs. Useful insights about drug diversion and other pharmacy-related fraud trends could likely be identified if the ability to compare or consider monitoring program data across multiple states were formalized.

Health care anti-fraud efforts also identify and help prevent medical identity theft. Using a person's name or other identifying information without that person's knowledge or consent to obtain medical services, or to submit false insurance claims for payment, constitutes medical identity theft. It can result in erroneous information being added to a person's medical record or the creation of a fictitious medical record in the victim's name. These victims could receive the wrong (and potentially harmful) medical treatment, find that their health insurance benefits have been exhausted, become uninsurable for life insurance coverage, or have their ability to obtain employment impacted. Untangling the web of deceit spun by perpetrators of medical identity theft can be a grueling and stressful endeavor, and the effects of this crime can plague a victim's medical and financial status for years to come. And medical identity theft is not a crime limited to patients—with increasing regularity, health care providers are finding themselves victims of identity theft too, often resulting in serious damage to their professional reputations.

My testimony today will focus on three issues which NHCAA believes are critical to successfully combat health care fraud. The first 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. The second is the critical role of data consolidation and data analytics in being able to prevent precious health care dollars from being lost to fraud. Finally, I will address the value of new anti-fraud tools provided by recent legislation, including the Affordable Care Act (ACA) and the Small Business Jobs and Credit Act of 2010, and the need to build upon these new tools to ensure continued and consequential private and public investment in anti-fraud efforts.

I. 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.

Health care fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare migrate over to private insurers, and schemes perpetrated against private insurers make their way into government programs. Additionally, many private insurers are Medicare Parts C and D contractors or provide Medicaid coverage in the states, making clear the intrinsic connection between private and public interests.

NHCAA has stood as an example of the power of a private-public partnership against health care fraud since its founding, and we believe that health care fraud should be addressed with private-public solutions. Government entities, tasked with fighting fraud and safeguarding our health system, and private insurers, responsible for protecting their beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest. Our experience has taught us that investigative information sharing works in combating health care fraud, and NHCAA dedicates itself to providing venues in which the sharing of relevant information can take place.

For example, NHCAA hosts several anti-fraud information-sharing meetings each year in which private health plans and representatives of the FBI, the Investigations Division of HHS-OIG, State Medicaid Fraud Control Units, TRICARE, and other federal and state agencies come together to share information about emergent fraud schemes and trends. Moreover, NHCAA's Request for Investigation Assistance (RIA) process allows government agents to easily query private health insurers regarding their financial exposure in active health care fraud cases. For the past decade, NHCAA has conducted a biennial survey of its private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units. In the most recent survey report (with data collected in 2009), 100% of respondents reported that they responded to NHCAA Requests for Investigation Assistance from

law enforcement. Earlier this year, an FBI special agent who had submitted an RIA provided NHCAA feedback regarding the value of the process, stating that an estimated $1.5 million in additional fraud dollars were identified as a result. The special agent rated the RIA process as "Excellent."

In addition to the NHCAA-sponsored information-sharing forums, many U.S. Attorney Offices sponsor health care fraud task forces that hold routine meetings. In the same survey mentioned above, 89 percent of NHCAA private insurer members stated that they have shared case information at law enforcement-sponsored health care fraud task force meetings.[1] It is clear that private insurers regularly share information with law enforcement, which in turn aids ongoing investigations.

The Department of Justice (DOJ) has 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" recognizes the importance of a coordinated program, bringing together both the public and private sectors in the organized fight against health care fraud.[2] Likewise, CMS has recognized the value of greater information sharing. During a September 22, 2010 Congressional subcommittee hearing, Peter Budetti, M.D., J.D., Deputy Administrator and Director of the Center for Program Integrity, stated: "Sharing information and performance metrics broadly and engaging internal and external stakeholders involves establishing new partnerships with government and private sector groups. Because the public and private sectors have common challenges in fighting fraud and keeping fraudulent providers at bay, it makes sense that we should join together in seeking common solutions."

In Philadelphia this past June, the Department of Health and Human Services (HHS) and the Department of Justice (DOJ) co-hosted their sixth regional Health Care Fraud Prevention

[1] NHCAA Anti-Fraud Management Survey for Calendar Year 2009, National Health Care Anti-Fraud Association, June 2010.
[2] See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

Summit. The importance and promise of partnership in fighting health care fraud emerged as a major theme of the event. Attorney General Eric Holder offered keynote remarks highlighting the value of information sharing and collaboration in tackling health care fraud: "When it comes to addressing a challenge as urgent, as complex, and as widespread as health care fraud, we need an innovative, proactive, and collaborative approach…There's no question that we need strong public-private partnerships."[3] Further asserting his commitment to this idea, Attorney General Holder said, "[The DOJ] will continue to engage key stakeholders in the private sector in our anti-fraud efforts…As we move forward, we will seek out guidance from representatives of the insurance industry and in the health care-provider community."

Likewise, in her keynote remarks, HHS Secretary Kathleen Sebelius described the Summit as "an important opportunity to build partnerships between public and private stakeholders who are invested in our fight against health care fraud. We have already begun to develop the relationships that can form the foundation for long-term cooperation."[4]

The Summit agenda was designed to showcase private-public partnerships against fraud that have yielded success. For example, one panel discussion was based on the *United States of America v. Stephen J. Schneider, D.O and Linda K. Schneider, L.P.N.* case, the prosecution of which was honored with the NHCAA 2010 Investigation of the Year Award. This four-year investigation into the operation of a pain management clinic in a small community south of Wichita, Kansas involved extensive over-prescribing of controlled substances, resulting in more than 100 drug overdoses, with the deaths of at least 68 persons linked to the case. The far-reaching investigative team included federal, state and private-sector representatives, offering a perfect illustration of the efficacy of private-public partnership.

Another example that illustrates the power of cooperative efforts against health care fraud can be found in South Florida, viewed by many as the epicenter for emerging fraud schemes. Here, "phantom" health care providers, which do not exist except on paper, yet manage to defraud

[3] See http://www.justice.gov/iso/opa/ag/speeches/2011/ag-speech-110617.html
[4] See http://www.hhs.gov/secretary/about/speeches/sp20110617.html

public and private programs of millions of dollars, had become an acute problem over the last several years.

One effort by HHS-OIG in 2007 to validate durable medical equipment, prosthetics, orthotics, and supply (DMEPOS) providers under Medicare revealed that nearly one third – 491 – of the 1,581 DME providers in three South Florida counties simply did not exist.[5] These phantom providers had collected hundreds of millions of dollars from Medicare, Medicaid and other public programs. As a result of this type of wide-spread fraud, the Department of Justice organized its first Health Care Fraud Strike Force in Miami-Dade County.[6]

While the government-led Strike Force was investigating, significant intelligence about these phantom providers was also being developed by private health insurers, much of it driven by information provided by beneficiaries – individuals who received Explanation of Benefit forms for services they had not received. Once information began to be shared between the public and private sectors, NHCAA member company investigators were able to review beneficiary information to determine that the same Social Security numbers were being used repeatedly by these phantom providers. A search of claim histories showed short, intense billing cycles by these providers, billing numerous services within a week or two. When investigators tried to contact these alleged providers by telephone, they typically found disconnected numbers or full voicemail boxes. Messages that were left by investigators were never returned.

In response to the challenge of phantom providers and other health care fraud schemes in South Florida, including fraud schemes involving infusion therapy and home health care, NHCAA formed a South Florida Work Group. In meetings held in 2009 and 2010, this NHCAA work group brought together representatives of private insurers, FBI headquarters and 10 FBI field divisions, the Centers for Medicare and Medicaid Services (CMS), the Department of Health and Human Services Office of Inspector General (HHS-OIG), the Justice Department, the Miami U.S. Attorney's Office, the Office of Personnel Management Office of Inspector General (OPM-

[5] See http://oig.hhs.gov/publications/docs/press/2007/PRSouthFlorida.pdf.
[6] See http://www.stopmedicarefraud.gov/heatsuccess/heat_taskforce_miami.pdf.

OIG), the Department of Defense (DOD) TRICARE, and local law enforcement to address the health care fraud schemes emerging from South Florida. The details of these schemes, the investigatory tactics, and the results of recent prosecutions were discussed with the dual goals of preventing additional losses in South Florida and preventing the schemes from spreading and taking hold in other parts of the nation.

Despite how information sharing has progressed between the private and public payers of health care, on occasion some federal and state agents have been under the misapprehension that they do not have the authority to share information about health care fraud with private insurers, creating an unnecessary yet significant obstacle in coordinated fraud fighting efforts. It would greatly enhance the fight against health care fraud if federal and state agencies clearly communicate with their agents the guidelines for sharing information with private insurers, emphasizing that information sharing for the purposes of preventing, detecting and investigating health care fraud is authorized, encouraged and consistent with applicable legal principles. NHCAA is working closely with the HHS-OIG, CMS, and DOJ to identify the barriers, both actual and perceived, to more effective anti-fraud information sharing with the goal of increasing the effectiveness of this critical tool in the fight against health care fraud.

We understand that Senate Bill 1251, the anti-fraud measure recently introduced by Senators Carper and Coburn, includes several provisions that promote expanded data sharing. The bill describes a plan to permit Medicare program safeguard contractors (PSCs) and "other oversight contractors" such as Zone Program Integrity Contractors (ZPICs), Recovery Audit Contractors (RACs) and the special investigations units of Medicare contractors access to relevant government data as a means to improve fraud fighting. The legislation also includes a provision to expand access to the integrated data repository (IDR) established under the Affordable Care Act to "relevant State agencies," including state Medicaid plans, CHIP plans and Medicaid Fraud Control Units.

Sharing information and data with contractors of federal health programs and with state health programs is crucial to the success of anti-fraud efforts. Consistent with this concept, we also

would urge that, as CMS and the HHS-OIG move forward with data consolidation and analytics, the information developed from Medicare and Medicaid data on emerging fraud schemes and trends and their geographic locations be shared with private insurers to ensure the most effective and comprehensive focusing of anti-fraud resources, and to enhance the private-public partnership against health care fraud.

II. Data aggregation and analysis are essential tools in health care fraud detection and prevention.

The numbers are staggering: The U.S. health care system spends $2.5 trillion dollars and generates billions of claims a year from hundreds of thousands of health care service and product providers. The vast majority of these providers of 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 claims for potential fraud, each payer is limited to the claims it receives and adjudicates. There is no single repository of health care claims similar to what exists for property and casualty insurance claims.[7] The complexity and size of the health care system, along with understandable concerns for patient privacy, probably make such a database impracticable. This fact further emphasizes the importance of anti-fraud information sharing among all payers of health care.

Nevertheless, data consolidation is possible at some level. NHCAA is encouraged by the expanded data matching provisions provided for in Section 6402(a) of the Affordable Care Act. This section mandates an expanded "Integrated Data Repository" at CMS that will incorporate data from all federal health care programs. The law stipulates that inclusion of Medicare data into the Integrated Data Repository "shall be a priority," and data from the other federal programs shall be included "as appropriate." As a result, this provision establishes the *ability* to create an "all claims" database, albeit limited to government programs, with the purpose of

[7] See https://claimsearch.iso.com

conducting law enforcement and oversight activities. This is a major step in the right direction for analyzing claims data in a way that will stem potential losses and identify emerging schemes at the earliest possible time.

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. Clearly, the only way to detect emerging fraud patterns and schemes in a timely manner is to aggregate claims data as much as practicable, then apply cutting-edge technology to the data to detect risks and emerging fraud trends. 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.

In recognition of this fact, some commercial health insurers have begun to utilize, or are in the process of evaluating the use of, predictive analytics, applying them to fraud prevention efforts on the front end, prior to medical claims being paid. This is similar to the technology that credit card companies and financial institutions use to detect and prevent fraud. It works by searching vast amounts of data and applying risk-scoring and building models based on patterns that emerge from that data. At the June Fraud Prevention Summit in Philadelphia, Jeff Brewer of technology company FICO participated in a panel that discussed the use of technology and data sharing among private and public payers. FICO, an NHCAA member, has extensive experience in applying predictive modeling techniques to the financial services industry and is now applying these technologies to health care, with clients such as Highmark Blue Cross Blue Shield in Pennsylvania. Mr. Brewer explained that within a payer organization, there are many stakeholders and real-time data analytics solutions really must work as "enterprise-wide systems." In estimating the promise that data analytics holds for health care, he stated, "FICO technology works in real-time—by milliseconds—for your credit card. We hope to get health care there. The technology is there."

The federal government has also recognized the value of data analysis as a key aspect of its inter-agency HEAT initiative. The Health Care Fraud Prevention and Enforcement Action Team (HEAT) counts among its goals improved data sharing—including access to real-time data—to

detect fraud patterns, and strengthened partnerships between the public and private health sectors. The Medicare Strike Force model employed by the HEAT program combines all Medicare paid claims into a single, searchable database, identifying potential fraud more quickly and effectively. There are currently Strike Force teams operating in nine metro centers across the country. The Strike Forces' use of improved real time data access and analysis has resulted in more than 520 successful prosecutions and 465 indictments involving charges filed against 829 defendants over the last four years.[8]

Congress has demonstrated its commitment to combating fraud by applying predictive modeling techniques to health care anti-fraud efforts through the Small Business Jobs and Credit Act of 2010. The Act includes language that establishes predictive analytics technologies requirements for the Medicare fee-for-service program, directing the HHS Secretary to use predictive modeling and other analytics technologies to identify improper claims for reimbursement and prevent their payment. Last month, Secretary Sebelius announced that Northrop Grumman, together with National Government Services and Federal Network Systems, a Verizon company, had been selected to implement the predictive modeling and analytic technology requirements under the Small Business Jobs and Credit Act, beginning July 1.

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 its manifestation. We are particularly anxious to learn about the results of the predictive modeling project for Medicare fee-for-service now underway at HHS. Clearly one of Medicare's strengths in terms of fraud detection is the enormous amount of data the program generates and collects. Applying predictive modeling to that data could yield very powerful, game-changing results.

[8] These statistics are for the period of May 7, 2007 through September 30, 2010 as reported in the HCFAC Report for Fiscal Year 2010, http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2010.pdf.

III. Investment in innovative health care fraud prevention, detection and investigation tools and programs is vital and should be encouraged.

There is no doubt that good work has been done in the fight against health care fraud. When it was established under HIPAA, the National Health Care Fraud & Abuse Control Program (HCFAC) was intended to be "a far-reaching program to combat fraud and abuse in health care, including both public and private health plans."[9] Now, 14 years later, the documented success of the HCFAC affirms the wisdom of making that investment. Published in January 2011, the HCFAC report for Fiscal Year 2010 shows a return on investment (ROI) of $4.90 for every $1 spent since the program began. The three-year average ROI for Fiscal Years 2008-2010 is considerable at $6.80 to $1. According to the report, the HCFAC account has returned more than $18 billion to the Medicare Trust Fund since the program's inception. Similar to the HCFAC program findings, NHCAA's private-sector members consistently yield solid returns for their anti-fraud investments. It should be noted that, given the wide range in terms of size and scope of business of NHCAA's private insurer members, the ROI for anti-fraud activities varies from company to company.

More recent programmatic anti-fraud initiatives—including the HEAT program, the Medicare Strike Forces, as well as National and Regional Health Care Fraud Prevention Summits co-hosted by Secretary Sebelius and Attorney General Holder—have also demonstrated success and promise, employing collaborative approaches to prevent and identify health care fraud, and educating providers and beneficiaries about the problem of fraud. Moreover, the numerous anti-fraud tools enabled by the Affordable Care Act (ACA) are very good news for patients and taxpayers alike. For instance, the new screening requirements for providers participating in Medicare, Medicaid and the Children's Health Insurance Program (CHIP) are a big step in the direction of preventing fraud before it occurs by helping to deny access to these programs by

[9] See http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2010.pdf, The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2010, page 3.

potential fraudsters. Based on the potential risk of fraud by categories of provider, the three levels of provider screening spelled out in the final rule will serve to protect our nation's health care investment.

The ACA also authorizes the Secretary to impose a temporary moratorium (6 months) on the enrollment of new providers of services and suppliers under Medicare, Medicaid and CHIP when necessary to prevent or combat fraud, waste or abuse. Notably, the final rule allows for moratoria in cases where CMS identifies a particular provider or supplier type and/or a particular geographic area as having a significant potential for fraud, waste or abuse. This is particularly important because health care fraud often manifests much like a fad would—it surfaces in one place or among one group, takes hold and proliferates. It is important to be able to suppress it when and where it appears in order to limit its reach.

Additionally, the ACA creates the ability of the Secretary to suspend payments to a specific provider "pending an investigation of a credible allegation of fraud." Several changes were also made to the Medicaid Integrity Program, including new provisions regarding exclusions from the Medicaid program. For instance, a provider's participation will be terminated under Medicaid if it has been terminated under Medicare or another state plan.

Among the many new anti-fraud provisions included as part of the ACA, additional funding for anti-fraud efforts was a noteworthy inclusion. The ACA allows for an additional $350 million to be appropriated to the fraud fighting cause between 2011 and 2020. NHCAA is confident that Congress and the public will be pleased with the results of this appropriation, as there is proven value in making anti-fraud investments.

The President's proposed budget for Fiscal Year 2012 is further acknowledgment that anti-fraud resources are sound investments. The budget proposes a $270 million increase for discretionary funding for Health Care Fraud & Abuse Control, and we applaud this commitment. The proposed increase is needed to fund the expansion of the strike forces and to advance the goal of shifting from the "pay and chase" fraud fighting concept to one that employs technology to

prevent and detect fraud prior to claims being paid. The return on investment for anti-fraud initiatives is significant, and therefore the increase in funding for these initiatives would be consistent with Congress' focus on reducing government spending.

These recent federal anti-fraud programs and initiatives, along with the substantial increase of funding and new anti-fraud tools enabled by the ACA, are very positive steps, particularly for government health programs. However, we question the regulatory decision to categorize anti-fraud activities undertaken by private insurers as simple "cost containment" in the medical loss ratio (MLR) interim final rules issued earlier this year. We believe this decision runs counter to the direction taken by the ACA. Consistent with the necessary priority given to anti-fraud efforts in the federal health care programs, private health plans should be given every incentive to invest in the technology and resources necessary to fight fraud and protect patients—particularly when the need to shift away from the "pay and chase" model is now. NHCAA is concerned that accounting for anti-fraud investments as "administrative" without acknowledging the quality-affirming aspects of this work will serve as a disincentive to private insurers to invest in fraud prevention. And we know that the nature of health care fraud demands constant reevaluation of methods and means and continual investment to stay ahead of the curve.

Public awareness and participation in the fight against health care fraud is also crucial to its success. We are encouraged to note that Senate Bill 1251 would change the beneficiary incentive program established under HIPAA to allow for monetary rewards to be paid prior to the full recovery of an overpayment. It also instructs the Secretary to use the Senior Medicare Patrols (SMPs) to conduct a "public awareness and education campaign" to encourage more participation in the incentive program. In 2010, NHCAA was proud to name the Senior Medicare Patrol program as the recipient of our Excellence in Public Awareness Award. This award is bestowed annually upon an organization or individuals who have done the most in the past year to raise public awareness about the problem of fraud in our nation's health care system. The SMP program is tireless in its commitment to fighting fraud in the Medicare system and would be an excellent partner for a campaign to promote the beneficiary incentive program.

Conclusion

Health care fraud costs taxpayers billions of dollars every year and often harms patients. Fighting it requires focused attention and a commitment to innovative solutions. NHCAA believes that a comprehensive approach to fighting fraud must include all payers, public and private. Additionally, multiple tools and methods must be applied. The anti-fraud efforts of organizations—private insurers and public payers alike—need to be flexible and multifaceted.

The schemes devised by perpetrators of health care fraud take many forms, and these perpetrators are opportunistic. Consequently, we must stay vigilant and work to anticipate and identify the risks, and develop strategies to meet these risks. Right now, harnessing the enormous quantities of data produced by our health care system in order to identify and predict fraud holds great promise. As Secretary Sebelius stated during the June Fraud Prevention Summit in Philadelphia, "We know that in order to stop health care fraud we also have to develop new methods and technologies to stay ahead of criminals and identify their patterns of behavior early." NHCAA encourages continued investment in exploring and implementing data consolidation and data analytical techniques.

NHCAA is encouraged by the renewed federal emphasis given to fighting health care fraud. This hearing is an excellent example, as are the statutes, regulations and policies from the past several years that have enabled greater fraud fighting success. NHCAA knows continued investment and innovation are critical, and as greater attention is given to eradicating fraud within our government health care programs, we urge decision makers to also recognize and encourage the important role that private insurers play in helping to minimize the fraud in our nation's health care system.

Thank you for allowing me to speak to you today. I would be happy to answer any questions that you may have.