Senate Bill 13-137 Request for Information Evaluation

Issued: October 21, 2013

Background:

Colorado Senate Bill 13-137, Act Concerning System Improvements to Prevent Fraud in the Medicaid Program, was signed by the Governor on May 24, 2013. It stated the intent of the Legislature to "implement waste, fraud, and abuse detection, prevention, and recovery solutions to improve program integrity in the State's Medicaid Program and create efficiency and cost savings through a shift from a retrospective 'pay and chase' model to a prospective prepayment model."

On June 18, 2013, the Department of Health Care Policy and Financing (Department) initiated a Request for Information (RFI). Responses were due on July 22, 2013. The Department received seventeen (17) responses from vendors.

Relevant Information:

- The Department has reviewed the responses and utilized information provided from the RFI to develop some requirements in our Request for Proposals (RFP) for the Business Intelligence and Data Management Services (BIDM), which is a piece of the Department's reprocurement of the MMIS. The BIDM RFP includes a requirement for a Predictive Analytics Tool, that utilizes advanced analytic methods and models to identify and assign a risk score for aberrant behavior in provider claims billing which may be fraudulent or are overpayments, identify aberrant or fraudulent patterns to find unknown or unusual behavior and anomalies, perform relational analytics, utilize social network analyses to identify possible associates, detect and visually represent interrelationships between providers and clients, utilize linked information to predict relationships that have a high probability of fraud, and identify potential program vulnerabilities. The tool would utilize data available through the BIDM (claims data) and would require the contractor to access external data sources over time as information from those systems becomes available to the Department.

- The estimated fiscal impact to implement the components in the RFI can be upwards of $7-$10 million (based on estimates from other states) with significant ongoing costs, including increased staffing for the Department. Based on the review of the RFI responses, the Department expects that staffing will need to be increased 1) to develop the modeling to utilize the software proposed in the RFI and 2) to review and analyze leads generated by the software that are identified as potential fraud, waste, and abuse.

- Some of the RFI responses include reviewing claims prior to payment. Pre-payment review cannot delay payments due to timely payment requirements by the federal government. Additional Department or contractor staff would also be needed to effectively utilize pre-

payment review tools to identify improper payments prior to payments being made while meeting federal requirements. Because of this, the Department is moving cautiously before implementing tools that impact providers on a pre-payment basis.

- Dollars collected from pre-payment reviews may also lower recoveries the Department already catches doing post-payment reviews. Through existing efforts, the Department recovered approximately $71,915,000 in fraud, waste, and abuse efforts from providers last fiscal year.
    - o The $71,915,039.77 above includes the following: All Program Integrity section recoveries including global settlements, Recovery Audit Contractor and Contingency based recoveries, Benefits Coordination section's recoveries (except for estate and trusts), nursing facility recoveries, bankruptcies, collections, client fraud collections, and Xerox/Provider Third Party Liability recoveries.

- The Department acknowledges that more can be done in the prevention and collection of fraud, waste, and abuse in Medicaid and we are working to increase our efforts. Any large implementation of a new system or the components provided by vendors in the RFI that are not be included in our BIDM RFP will need to follow the traditional budget process.

- With the addition of predictive analytics in the BIDM RFP and gleaning what we can from the RFI process, the Department is confident that recoveries from fraud, waste, and abuse will grow at a faster rate than caseload growth.

Next Steps:

- The Department proposes to host a Vendor Fair in Mid-January 2014 through Mid-February 2014 (dates to be confirmed once a location has been determined). This Vendor Fair will allow vendors to demonstrate products and discuss their solutions with the Department. All vendors who submitted responses and those on our distribution list will be provided an opportunity to present their products and solutions to the Department.
    - o The Department will notify all vendors who submitted responses and those on our distribution list by Monday, November 25, 2013 of the official dates and available time slots related to the Vendor Fair so travel and accommodations can be scheduled appropriately.
    - o Vendors wishing to contact the Department regarding the Vendor Fair or joining the distribution list may contact us at RFPQuestions@hcpf.state.co.us
    - o The Department will discourage staff from attending meetings with individual vendors outside of the Vendor Fair to maintain the integrity of the process and any future RFPs related to this topic.

- The Department will request additional information from vendors, requesting ideas and solutions that could be packaged within specific budgetary ranges. For example, what products and services could the Department purchase for an initial $3 million investment, with $500,000 ongoing costs as opposed to an initial investment of $5 million, with $750,000

ongoing costs? Vendors will be encouraged to present solutions to these options at the Vendor Fair and in written proposals, which the Department plans to keep confidential to protect vendors' pricing information.

- Following the Vendor Fair, The Department will develop options for the Governor's Office and the General Assembly to consider. If funding is made available, the Department expects that a formal RFP related to this topic would be released in FY 2014-15, with work commencing during FY 2015-16. The implementation of products and services would need to correspond to the implementation of the new MMIS and BIDM, which are expected to be operational during FY 2016-17.

Summarization of the RFI Responses:

A summarization of the RFI responses are provided below. The criteria provided in the RFI can be found in Attachment A. A summary of each vendor's response by criteria is provided in Attachment B. A more detailed summary of each vendor's response can be found in Attachment C.

Criteria #1 – Experience utilizing predictive modeling: According to the responses, many vendors use some type of rating method to determine the likelihood of fraud, waste, and/or abuse. These methods mainly include using numbers (e.g., 1-100) or percentages (e.g., 0.1-100%). Generally, the higher the number or percentage the more likely an issue of fraud, waste, and/or abuse exists. Network management, financial management, profiling technology, and predictive models are examples of other solutions that vendors offered to the Department. A good portion of vendors responded that their tools were used worldwide; however, very few specifically revealed business or entity names. Of those who did reveal names, approximately two or three mentioned providing predictive modeling services to Medicaid and none of them mentioned the length of time they provided those services to other entities.

Criteria #2 – Detailed description of vendors' predictive analytic tools: A common theme throughout vendor responses in the predictive analytics process is to gather aggregate data from multiple sources then integrate the data into a global database that can be queried in various ways. Most of the responses stated that some type of database development would be required which many of the vendors said they would build and maintain. A significant portion of the vendors would require the Department to provide claims data. The majority of the vendors' methods are directed at pre-payment and post-payment reviews.

Criteria #3 – Empirical details related to the performance of vendors' tools or methodologies: Vendors responses varied widely regarding the type of entities using their tools and in what capacity. Responses included vendors who have worked with or are working with such entities as: UK Defense and Intelligence community, Centers for Medicare and Medicaid Services, Medicare, physicians' offices, state human service departments, Navy Ballistic Missile Program, and PayPal to name a few. Only one or two entities mentioned specifically working with Medicaid on a predictive analytic tool. A significant number of vendors' opted not to provide performance measurement information due to contractual obligations or lack of information due

to implementation being so recent. Vendor responses were very diverse when addressing payment prevention of provider claims. Many said they could prevent payment if transactions could be flagged and manually reviewed by a supervisor or designated personnel. Very few vendors addressed whether they could stay within the federal governments' prompt payment requirement.

Criteria #4 – Detailed description of provider and recipient data verification: Vendor techniques and functionality varied widely in this area. Most of the responses stated that for provider/recipient verification, some type of database development would be required for which many vendors said they would build and maintain. A Commercial off the Shelf (COTS) solution for provider validation was mentioned by more than one vendor. Most, if not all, vendors outlined an easy-to-use visualization/search tool, many of which were web-based.

Criteria #5 – Empirical details related to the performance of provider/recipient verification and screening solutions:

a) **The number and type of entities utilizing the technology solutions. Separately identify any health care entities or Medicaid programs.** Many vendors responded to this request by giving the type of entities using their solutions but did not specify names (e.g., commercial health care payers, state Medicaid programs, Medicare Administrative Contractor, federal, state, and local governments). The vendors that did specify this information revealed entities such as: Department of Justice, Department of Labor, Internal Revenue Service, Her Majesty's Revenue and Customs, Australian Tax Office. The majority of the vendors did not specify working with Medicaid specifically.

b) **The number of potential issues identified separately for providers and recipients.** Some vendors stated that they did not perform recovery audit, investigations, or collection activities. Other vendors stated that they were either engaged in pre-contract analysis, producing reports that would release confidence scores for accuracy, or declined releasing this information for fear that fraudsters would use it to aid in their attempts. Vendors that did respond stated that issues had been identified in claims being billed by sanctioned providers, deceased owners' National Provider Identification numbers being used, recipients who receive benefits in multiple states, recipients who sell their prescription drugs for cash.

c) **The number of those identified providers on which the issue was verified and action was taken by you or the entity. Separately identify the same for recipients.** Many vendors did not address this portion of the request stating that they preferred not to reveal this information out of respect for their clients, or that they didn't know because they only provided data and did not perform recovery, investigative or collection activities. Other vendors outlined provider sanctions, licensure and board disciplinary actions being taken.

d) **The number and total amount of inappropriate payments which were prevented by your solution. Describe what action was needed by you or the entity to prevent payment.** Vendors' responses to this request varied widely. Some stated that the

information was sensitive and could not be divulged, while others stated they identified findings that resulted in cost avoidance or cost savings. Various vendors identified combined inappropriate payments ranging from $80,000 to $2.1 billion.

Criteria #6 – How methodologies and technology tools will be easily integrated into the Medical Management Information System (MMIS): The majority of vendors feel their analytical tool could be easily integrated into the MMIS through a direct interface that will feed data from the vendors' database to MMIS. Many of the vendors claim that the referenced integration would not interfere with MMIS performance.

Criteria #7 – Explain your investigation services that the Department does not currently possess: Vendor fraud detection and investigation services varied widely in this area, so a true summary could not be developed. In order to get the clear picture of what is available, it is suggested that the reader review the more detailed response provided in Attachment B and Attachment C.

Criteria #8 – Detailed explanation of the extent to which you will seek clinical and technical expertise from Colorado providers: Many of vendors' responses indicated they were more than willing to work with the provider community while developing tools and technologies. Most vendors seem to be familiar with educating providers through Webinars or providing educational resources through a web portal.

Criteria #9 – Resources and capabilities needed by a Medicaid program to investigate potential fraud: Many vendors did not provide information on staffing requirements, however, a few said that predicting staffing would depend on claims volume, past cases used for predictive modeling, and analyst productivity; others said they would provide their own staff; and some said they preferred not to disclose that information before the Request For Proposal process due to Colorado Open Records Act and proprietary pricing information. Some vendors outlined such services as prepay and post-pay analytics, audit, and investigative services, development of unique solutions tailored to particular client needs, case management services, enrollment, and reenrollment activities. Others stated that they only provided data services and did not perform recovery audit, investigations or collection activities.

Criteria #10 – Cost/price itemization that will allow the Department the ability to understand the costs of purchasing implementing and maintaining an updated product, system and service: Many providers did not disclose cost/pricing information due to non-disclosure clauses in their contracts or needing more information about the Department's specific requirements. The few vendors that did disclose prices quoted between $75,000 and $9 million annually.

To obtain the full response submitted by a specific or all vendors, please send an email request to RFPQuestions@hcpf.state.co.us and the request will be considered an official Colorado Open Records Request (CORA) for information.

Attachment A

The Department of Health Care Policy and Financing (Department) initiated a Request for Information (RFI) to solicit the following information/capabilities from the vendor community:

1) Vendors' experience and expertise with utilizing a predictive modeling and analytics tool, knowledge of provider and recipient data verification and screening technology, what fraud investigation services are available that HCPF does not currently possess or perform, database creation or integration of data, and education and outreach.

2) Comprehensive and detailed description of vendors' predictive modeling and analytics tools or methodologies to improve waste, fraud, and abuse detection, prevention and recovery in the Colorado Medical Assistance Program.

3) Empirical details related to the performance of vendors' tools or methodologies over the last twelve (12) months, such as: the number of entities who utilized the tools or methodologies, any Medicaid programs using the tools or methodologies, total number of claims/encounters identified and total payment recovered, specify whether the tool will prevent any claims identified as wasteful from being paid.

4) Comprehensive and detailed description of vendors' provider and recipient data verification and screening technology solutions and how the solutions are used for the purposes of automating reviews and identifying and preventing inappropriate payments.

5) The performance of vendors' provider and recipient data verification and screening solutions such as the number and type of entities utilizing their technology, potential issues identified separately for providers and recipients, actions taken on any issues, the number and total amount of inappropriate payments that were prevented by the vendors' solutions.

6) How providers' tools, methodologies and technology will be easily integrated into a Medicaid Management Information System (MMIS).

7) Details explaining vendor's fraud investigation services that HCPF does not currently possess or that HCPF is not currently performing.

8) Details of the extent to which vendors will seek clinical and technical expertise from Colorado providers concerning the design and implementation for the tools and technologies described in their responses to improve Colorado Medicaid's fraud detection system.

9) Outline of resources and capabilities needed by HCPF to investigate potential fraud and recover inappropriate payments. Specify the resources needed for prepayment use and post-payment use.

10) Cost/price itemization that will allow HCPF the ability to understand the detailed costs of purchasing, implementing, operating, maintaining, and updating vendors' product. Separate the cost/pricing by pre-payment implementation and post-payment implementation.

ATTACHMENT B
SUMMARY BY CRITERIA

VENDOR NAME	**Criteria #1: Provide a brief description of vendor's organization. Provide detailed information of your experience with utilizing and expertise with predictive modeling and analytics, provider and recipient data verification and screening technology solutions, fraud investigation services that the Department does not currently possess.**	**Criteria #2: detailed description of vendors' predictive modeling and analytics tools or other methodologies to improve waste, fraud, and abuse detection, prevention and recovery in the Colorado Medical Assistance Program.**

Vendor #1: CERNER (KANSAS CITY, MISSOURI)	**Criteria #1:** Cerner is the leading U.S. supplier of health care information technology solutions that optimize clinical and financial outcomes. Cerner Corporation uses a suite of math models to detect fraud waste and abuse. Cerner Math's models include Benford's Law that operates on the theory that amounts will start with the digit 1 more often than the digit 9. Benford's Law provides a mathematical formula that describes the percentages. The digit 1 should show up about 30 percent of the time, while the digit 9 should occur less than 5 percent of the time. In medical claims, the distributions of digits deviate from Benford's Law due to payor constraints and charge master rates, but nonetheless the digit distributions can accurately detect outliers and fraudulent transactions, through the use of Kolmogorov-Smirnov and related tests. Cerner systems are used by everyone from individual consumers, to single-doctor practices, hospitals, employers, and entire countries.	**Criteria #2**: Cerner Math's fraud detection and fraud predictions and pre-payment prevention models run in a Cloud-based computing environment. The data are extracted, translated, and loaded continuously into the cloud and thus do not require separate data-transport and duplication that occur in SAS or other traditional statistical packages.

| **Vendor #2: DUN & BRADSTREET (SHORT HILLS, NJ)** | **Criteria #1**: D&B (NYSE:DNB) is the world's leading source of commercial information and insight on businesses, enabling companies and government entities to decide with confidence for over 172 years. D&B's global commercial database contains more than 130 million business records and is perpetually maintained and enhanced by D&B's proprietary DUNSRight™ Quality Process. For over 30 years D&B has supported and assisted Federal, State, and Local government departments and agencies in the mission of Data Management, Financial Oversight, Fraud Detection, Homeland Security, Acquisition Management, Law Enforcement/Intelligence and Regulatory Compliance. D&B is uniquely positioned to support several listed goals of the Department to identify Medicaid Fraud prior to adjudication. Specifically, D&B is focused on providing data, services and technology solutions in support of the Department's efforts by: Matching Department enrolled Provider files to D&B match reference file for accurate identification of a Provider entity for discovery, reporting, Federal debarment and potential fraud; Providing accurate, complete and timely 3rd party business information in support of analyzing and identifying suspicious misrepresentation patterns of Providers enrolled, registering as a Provider, and/or filing real-time claims; Tracking and managing daily business changes experienced by the Provider network and to provide proactive warning of potential fraudulent or misrepresentation behavior. | **Criteria #2**: DUNSRight™ is Dun &Bradstreet's (D&B) proprietary process for collecting and enhancing data. Global Data Collection aggregates data from hundreds of sources to provide superior business information. Sources of information that may be pertinent to the Department include coverage of all U.S. courthouses for suit, lien and judgment information as well as Excluded Parties List System (EPLS), a web-based system that identifies parties excluded from receiving Federal contracts and subcontracts, and Federal financial and non-financial assistance and benefits. The key to the DUNSRight™ process is the D-U-N-S® Number- D&B's unique, nine-digit, location specific identifier which D&B assigns as a means of identifying and tracking companies globally throughout their lifecycle. Once assigned, a D-U-N-S® Number is neither reused nor assigned to another business. The D-U-N-S® Number is recognized globally and within trade associations. The mandatory data elements required are Internal ID, Business Name, Address, City, State, Zip and Telephone. Entity Matching is D&B's method for integrating the data collected into their global business database. This process allows for and corrects variations in spelling (e.g. IBM vs. International Business machines), formats trade names and addresses, and associates data from disparate sources (e.g. a state business license, a Federal 10k filing, and a Yellow Pages listing) with the appropriate D&B record. With this, D&B is then able to produce a single, accurate picture of each business. |

| **Vendor #3: DETICA CORPORATION (BOSTON, MASSACHUSETTS)** | **Criteria #1:** Detica is the global leader in providing advanced fraud detection technology; combining the latest in big data analytics with link and social network visualization to identify wasteful and abusive claims, providers, and recipients in both real-time and post-pay settings. Detica's proprietary tool NetReveal identifies fraud by harnessing its proven technology to ingest data from multiple sources to uncover hidden networks and relationships, otherwise undetectable in the raw data. NetReveal automatically joins and risk scores data from a wide range of sources, including, but not limited to, claims, managed care encounter data, provider registrations (in-state and NPPES) and exclusion lists, such as the Office of the Inspector General's (OIG) List of Excluded Individuals/Entities and State Exclusion and Sanction lists. In a pre-payment setting, NetReveal then incorporates these social networks and historical behavior profiles into real time predictive models that identify and suspend the riskiest and highest value claims for further investigation. | **Criteria #2:** The NetReveal solution uses a combination of predictive modeling techniques and social network analysis (SNA) to identify potentially abusive or fraudulent claims before a payment is made. Prior to claims processing, NetReveal automatically links together data from a number of sources, such as the NPI, state exclusion lists, the OIG exclusion list, state corporate records, MCO encounter data, historical claims data, and many other sources to identify behavioral patterns among providers and recipients, or "social networks." During claims processing, NetReveal uses this network intelligence, in addition to all data available in the claim fields, to risk-assess the claims in real time for fraudulent activity. Potentially improper claims are automatically suspended and routed for investigation. NetReveal could also be used in a post-payment setting should MassHealth elect to do so in the future. a) Regardless of the complexities and structure of the information, the sources often involve data from traditional RDBMS data sources from within the State's domain and other sources outside of the State's purview. DRC would recommend that the project to improve Medicaid fraud detection require that the system integrator be responsible to build and initially maintain the Predictive Modeling Solutions database(s). The state would provide historical claim, provider and recipient information as well as arrange for information from external sources to be made available. |

| Vendor #4: DYNAMICS RESEARCH CORPORATION (ANDOVER, MASSACHUSETTS) | Criteria #1: DRC is a leading provider of information technology (IT) services and solutions for government customers. We have a 58-year history of excellent service and satisfied customers. DRC has approximately 1200 employees and is a publicly held corporation (NASDAQ: DRCO) headquartered in Andover, Massachusetts. DRC serves Department of Defense, Federal Civilian Agencies and State & Local government. We provide solutions and professional services in 5 areas: Information Technology, Training and Performance Support, Business Transformation, Management Services and Engineering and Science. DRC has been providing services to the State of Colorado since 1997, when we began a project to design, develop and implement Colorado Trails, the Child Welfare case management system which is still being used today. DRC operates the IT infrastructure used to deliver applications such as CBMS, CHATS and Trails to all 64 of Colorado's counties. Over our tenure in Colorado have provided services as a valued partner to several state agencies and the Governor's Office of Information Technology. a) DRC is providing information from our Predictive Modeling Initiative project in support of the Massachusetts Executive Office for Health and Human Services. | Criteria #2: DRC presents the Detica NetReveal® suite of products for predictive analytics. NetReveal® is a suite of generic products which are configured to detect particular types of fraud within an industry such as the Healthcare. Our solution in Massachusetts integrates BAE Systems' Detica NetReveal® Healthcare solution with the Commonwealth's MMIS in real time. The solution is designed to either mark the claim for normal payment processing, deny the claim with appropriate reason attached to the claim, or suspend the payment and refer the claim (alerts) for further investigation. Initially, the plan is to flag (suspend payments) for 100 potential fraud, waste or abuse claims per day for the newly created investigative staff (currently 5 individuals). a) DRC would recommend that the project to improve Medicaid fraud detection require that the system integrator be responsible to build and initially maintain the Predictive Modeling Solutions database(s). The state would provide historical claim, provider and recipient information as well as arrange for information from external sources to be made available. In many cases the initial deployment will involve less than 10 data sources (sometimes less than 5) and over a 2-3 year period the number of data sources will scale up as the models evolve. b) A predictive model is designed to identify recipient and provider behavior characteristics likely to influence or suggest future behavior. In predictive modeling, data is collected for relevant characteristics, a statistical model is formulated, predictions are made and the model is validated or revised as additional information becomes available. The model may employ a scoring formula that evaluates claims at the time of processing and before payment. If a claim appears to be high-risk or out of the ordinary, the claim will be flagged for further scrutiny. c) In the most conservative implementation, a predictive modeling solution will complement existing rules and edits by identifying new, emerging and unknown patterns of aberrant behavior and preventing fraud and abuse before payment. Colorado can expect many of the high-scoring providers (in which a high score is "bad") scored high because of overutilization, mistakes or duplicate services. Understanding patterns of billing errors and overutilization can be very useful for providers who are going to have to reduce costs and increase the quality of outcomes in order to get paid the "incentives" being offered by new payment models. |

| Vendor #5: EMDEON (LINCOLNSHIRE, IL) | **Criteria #1**: As leaders in the Program Integrity market, Emdeon and FICO collectively have nearly 50 years of experience in detecting and combating fraud, waste and abuse in healthcare. By teaming our resources, we offer the Department a predictive analytics solution that is unique in depth and breadth of experience in program integrity predictive analytics. a) Emdeon has teamed with FICO, the predictive analytics organization which serves as the backbone of the credit card fraud detection industry, to develop and deploy a solution unparalleled in the health care industry. This powerful solution uses a combination of patented profiling technology, predictive models, statistical analysis and rules to achieve a level of detection accuracy that is unmatched. As stated previously, the analytics models are seeded with close to one billion claims from Emdeon, enhancing the power of the data to learn and detect aberrancy. By pairing FICO's analytics models with Emdeon's proprietary analytics and claims data and experience, the team has created an unparalleled predictive analytics engine that is able to dig deeper into the data to find more potential savings. While each claim runs through the Emdeon/FICO tool is scored for the likelihood of fraud, waste, and abuse at both the claim line and provider levels, it uses much more than the information contained on the claim itself. For example, a claim may be analyzed based on:
• Current and historical data about the patient.
• Current and historical data about other patients receiving similar services.
• Data about the provider(s) associated with the claim, including their history of providing care across their patient population. | **Criteria #2**: De-identified data from many payers is analyzed using multiple statistical models to identify those providers that have the highest likelihood of abusive or fraudulent behavior. This more complete view allows for more rapid identification of cases that might be of interest to those in the field of law enforcement. Analytical models detect improbable or highly-suspect scenarios by analyzing the provider's billing practices across multiple payers. Emdeon's data assets allow the most complete view of a provider's billing practice available in the industry today. A dedicated team of healthcare research and analysis professionals focuses on developing and refining these models. Two examples of the many models currently implemented against the multi-payer data are the Time Study Model and Patient Cost Distribution Model:
• The Time Study Model identifies providers billing for improbable days (>24 hours/day). • The Patient Cost Distribution Model identifies providers whose patients are significantly more expensive than the patients in their defined peer groups. a) Vendor did not address this portion of the information request. b) As a data-driven analytic solution, IFM relies on the data itself to determine the degree of aberrancy of a scored claim or provider. The data-driven approach utilized by IFM reaches deep and wide, leveraging related data from the entire network of the Departments' recipients, paid claims and healthcare providers, enabling the detection of both known and emerging fraud types, including complex and subtle fraud trends that may be difficult to express in rules-based logic. c) Functionality listed in Section 2.1.1.1-2.1.1.1.5: Refer to vendor's response |

Vendor #6: GRANT THORNTON (ALEXANDRIA, VA)	**Criteria #1**: Founded in Chicago in 1924, Grant Thornton is one of the largest accounting and management consulting organizations in the world. Grant Thornton is renowned for its distinctive client service and rigorous analytical capacity. To most optimally support the DHCPF's need for advanced analytics focused on fraud prevention and detection, Grant Thornton can utilize our partnership with Performant Financial Corporation (Performant), a firm that has the depth of subject matter understanding, enabling technology platforms, and unique experience in the deployment of advanced analytic technologies to address program integrity issues at their core. Currently, Performant provides services to a large national health plan where it, hosts a national data warehouse for purposes of overpayment identification, fraud detection, pharmacy inventory tracking, and other payment integrity initiatives. The target data sources include Claims, Membership, Pharmacy, Encounter, Accounts Payable, Payroll and more. In total, Performant receives data extracts from over 65 unique health plan data sources. Performant's data engineering team has extensive experience working with these dynamics and the Insight™ platform is uniquely capable of supporting extracts from any host system while requiring no file conversion burden to the client.	**Criteria #2**: The Grant Thornton Enterprise Integrity Solution (EIS) is an ongoing partnership between Grant Thornton and Performant to provide superior results in the prevention of healthcare fraud. Performant's data mining technology is built for processing extremely large volumes of data. Therefore, unlike many other models, the quantity of data analyzed is not limited to a defined subset. For example, an analysis for duplicate claims will be reviewed against the full history of data on an ongoing basis, and not simply one week's or one day's claims. Additionally, the EIS applies a multi-faceted approach including but not limited to up-to-date detection models. Rapid identification of new trends and behavior/identity changes. One example is a sudden change in a given provider's billing pattern that is inconsistent with those of his/her peer group. Another example is a billing entity that suddenly disappears from one place and reappears in another – which is often what happens in "hit and run" schemes. A third is the geographic spread or migration of questionable activity from its origin to surrounding and/ or distant counties. Performant's proprietary technology platform, Insight™, performs analyses of claim services related to counter fraud efforts, including the detection and verification of suspected FWA. Insight™ rapidly sorts through large quantities of data, runs statistical models and optimizes recovery opportunities. The technology has been deployed in a variety of complex and highly regulated environments for more than 20 years and has built-in security and compliance measures that have been evaluated and found to exceed public- and private-sector standards.

| **Vendor #7: HEALTH MANAGEMENT SYSTEMS (IRVING, TEXAS)** | **Criteria #1**: Founded in 1974, HMS provides expertise in healthcare policy; fraud, waste, and abuse (FWA); program analysis; data analytics; coordination of benefits (COB); and recovery to more than 130 managed care organizations (MCOs) and state and federal government agencies. Over the years, we have expanded our scope of services and added to our list of clients to include child support agencies, Veterans Administration facilities, and the Centers for Medicare & Medicaid Services (CMS). For applications and references, see Exhibit 1-2 of vendor's response. | **Criteria #2**: No additional hardware is required; all hardware, software, and databases are managed and maintained by HMS. a) HMS focuses on developing practical predictive models that produce actionable results. In this respect, HMS has a significant advantage that software vendors do not. Not only do we have extensive clinical expertise to aid in the development, review, and training of our predictive models, but we are also engaged nationally in the clinical review and audit of claims and providers targeted by our models. We thoroughly test our models and identify data attributes that work and those that produce false positives. Our predictive models run across the analytical planes identified by CMS as part of a fully functional fraud detection solution. We use statistical models to model normal behavior and identify outlier or nonnormal behavior for investigation. These models include historical analysis of claims data to identify potential issues and anomalies, and apply this knowledge actively to future claims data to predict potential issues with provider, member and claim data. HMS implements multiple sets of advanced analysis that are available on-demand through the online portal. These routines and analysis are automated and are regularly run across provider and member history; however, to make the information more actionable, HMS has chosen the online portal as the method to push data to our clients. These analysis routines include: provider peer analysis; anomaly routines; provider scoring; Provider validation/screening; member validation/eligibility review; utilization analysis. HMS implements multiple sets of advanced statistical analysis that are available on-demand through the online portal. These routines and analysis are automated and are regularly run across provider and member history |

| **Vendor #8:** **LEXISNEXIS** **(DALLAS, TEXAS)** | **Criteria #1**: For over 40 years, LexisNexis has been a trusted source and leading provider of decision-making information that help Human Services Agencies such as the Department. LexisNexis is the premier provider of decision-making intelligence solutions to businesses and government. Through numerous successful implementations, LexisNexis has developed significant expertise in providing identity-driven fraud detection and recovery solutions to Social Services Agencies, with solutions deployed in New York, California, Massachusetts, Texas, Georgia, Florida and across the United States. a) An example of a reference relevant to the Department's requirements is New York State Department of Health (State Medicaid Agency): LexisNexis have been providing advanced data analytics software tools to support the State of New York's effort to combat fraud, waste and abuse in the State's $45 billion Medicaid program. The LexisNexis solution started with the build and successful deployment of a cloud-based database that contained every New York State Medicaid claim (almost ten terabytes of data). Florida Department of Children and Family Services (DCF): With approximately 5.5M Beneficiary applications annually. Florida Department of Children and Family Services (DCF): With approximately 5.5M Beneficiary applications annually, DCF needed a solution to prevent fraud, waste, and abuse, and increase operational efficiencies without creating unreasonable barriers to access for true applicants in need. | **Criteria #2**: a) Provider Management - Leveraging our vast public records repository, LexisNexis offers comprehensive Provider Management solutions for enrollment and monitoring of Provider networks. In compliance with CMS regulations, LexisNexis Provider Management Solutions provide the Department confidence Providers participating in Medicaid are eligible to do so, and constantly monitors for, and alerts to, any changes in Provider status. b) LexisNexis/SourceHOV offers a unique, tightly integrated program integrity COTS/SaaS solution. This unique COTS/SaaS solution, includes prepay, post-pay, predictive analytics, coupled with a fully integrated recovery, augmented by certified fraud examiners, over 350 medical coders/reviewers, and combined with a funds management team. Nearly all of the aforementioned solution elements may be utilized as individual modules to augment existing program integrity capabilities or deployed alongside the existing program integrity process as an autonomous operation. This holistic approach starts with a provider and recipient assessment that when combined with the data analytics findings help identify and prioritize investigative matters. The process includes a comprehensive link-analysis of providers, recipients, and operational characteristics. This adds to the most comprehensive picture of your participants and their practices. c) The LexisNexis advanced suite of health care anti-fraud, waste and abuse products are propelled by several diverse, enabling technologies including our rules-based inference engine, our predictive modeling engines and our vast public records data store. Each has been designed to work specifically within a pre-payment and post-payment environment. |

| Vendor #9:
McKESSON
CORPORATION
(SAN FRANCISCO,
CA) | **Criteria #1**: McKesson Corporation is the nation's oldest and largest healthcare company. McKesson has been in continuous operations for 180 years (since 1833) and is headquartered in San Francisco, CA. Our network management and financial management tools help payers opti-mize business performance to operationalize today's complex volume-based and value-based payment models. Our FWA solutions are delivered by this business unit. Our decision management solutions — including InterQual — help connect payers and providers to align decision-making, improve outcomes and reduce unnecessary utilization. Our RelayHealth financial solutions streamline and optimize billing communication between providers, patients and payers to help optimize the revenue cycle management process. | **Criteria #2**: To meet the Department's advanced predictive modeling and analytics needs, we are proposing our InvestiClaim predictive analytics solution. Our complete InvestiClaim solution combines predictive analytics with the intelligent, proprietary pre-pay clinical rules and a full-service consultative approach to help identify both suspected and unknown billing aberrancies. You will be able to use the prospective analysis aspect of InvestiClaim to deny claim lines that are identified as exhibiting aberrant patterns before payment goes out the door. This enables an immediate ROI since claims can be pended or denied prior to payment. Also, as the pre-pay clinical editing rules are added, the pre-pay ROI will increase. Claim review occurs after adjudication and presents the most aberrant claims to the analyst or examiner, gives them a complete set of reasons for the aberrance, and provides views of the pattern along multiple dimensions, including member, provider, service and dates of service. This enables the claims auditor or examiner to make a rapid decision to pay, deny, pend for further review, or seek a recovery. InvestiClaim uses Windows Server 2008. The core application components are installed as Windows Services. The GUI is hosted in IIS. The database is Oracle 11g R1. During the solution design process, we will evaluate your requirements and at the conclusion, we will be in a position to provide database specifications. In an installed implementation, the application and data reside in your data center. In an Application Service Provider (ASP) implementation, the application and data reside in our ISO 27001 certified data center. The advantage of this approach is that McKesson purchases and maintains the hardware. There is minimal need for your IT resources. |

| Vendor #10: NORTHROP GRUMMAN (McLEAN, VA) | **Criteria #1:** Northrop Grumman Corporation is a leading global security company that provides innovative systems, products and solutions to government and commercial customers worldwide. We are a nationally recognized tier-one systems integrator with $34 billion in annual revenues and a workforce of 75,000 persons. The Information Systems sector, which is responsible for the contents of this RFI response, is a $7.9 billion business employing more than 22,000 professionals in 50 states and 25 countries. It is made up of four divisions: Defense Systems, Federal and Defense Technologies Division, Cyber System Division, and Intelligence Systems Division. a) For CMS Northrop Grumman successfully launched the Fraud Pevention System on time by July 1, 2011, less than 60 days from the contract award date. FPS supports the Center for Program Integrity (CPI) in providing a combination of advanced analytic techniques, and prepayment and case management systems for the prevention and detection of fraud, waste, abuse, and other improper payments under the Medicare and Medicaid programs. | **Criteria #2:** Northrop Grumman uses a variety of predictive modeling techniques and analytical tools to detect fraud, waste, and abuse. Our FPS for CMS runs numerous rules-based, anomaly-based, predictive models, and social network models to perform both pre-payment and post-payment claim analysis. a) Our solution has an existing data management capabilities based on an open source, big data management platform that Northrop Grumman uses in civil, intelligence, and defense sectors to protect our Nation from the threats. The data management platform runs on an array of low-cost commodity hardware that can either be hosted in Colorado data center, a Northrop Grumman data center, or a third party data center. The hardware can be sized based on the Department's requirements relative to the billions of transactions managed by system in full-scale production at CMS. b) Northrop Grumman uses a variety of statistical method and techniques (e.g., decision trees, Bayesian models, linear discriminants, genetic algorithms, neural networks, and network analysis) that are directed at provider and recipient fraud. c) Our solution prioritizes cases and assigns risk scores to drive certain actions. For example, a high score may result in a denial of the claim, while a lower score may require more research. Building models to predict fraud, waste, and abuse requires historical information and instances in which fraud, waste, and abuse is known to have occurred. The model is trained and validated using these previously investigated claims or providers where we know that the claim or provider either was doing something wrong or they were not. The Department should select a system that has flexibility to manage multiple workflows between the MMIS system and the fraud prevention system. The system should have the ability to flag a claim for review, message the event to the MMIS system, and queue the claim for further analysis. |

Vendor #11: OPERA SOLUTIONS, LLC (JERSEY CITY, NJ)	**Criteria #1**: Opera Solutions was founded in 2004 with a notion that the world's flow of information then starting to intensify — was going to be the oil of the 21st century. Today, Big Data has exploded and Opera numbers 660+ people, with offices in New York, Boston, San Diego, London, New Delhi, and Shanghai. We have massed the largest community of scientists in the private sector (220+ across 20 disciplines) and have Netflix Prize and the Heritage Health Prize both which measured machine learning capabilities. a) Opera Solutions offers a leading medical fraud solution, which consists of three key components namely: fraud detection algorithms, case management software and the Vektor technology stack.	**Criteria #2**: a - c) Opera Solutions will implement their sophisticated algorithm toolset developed to identify and combat FWA. The algorithms include pattern detection, anomaly detection, supervised predictive modeling, and network analysis with interactive visualization. Instead of basic rule based approaches, our algorithm toolset is built around a patent pending claims outlier detection solution, which includes a set of machine learning and pattern recognition algorithms to automatically capture the complex relationship among diagnosis, procedures, and patient profile in claims data. b) We will utilize our industry leading expertise in big data predictive analytics and extensive experience in developing healthcare predictive modeling solutions to provide a comprehensive FWA Platform. We work in various industries handling enormous amounts of data with and currently scoring more that 2M+ transactions on weekly basis for leading healthcare client.

| Vendor #12: OPTUM GOVERNMENT SOLUTIONS (ERIE, CO) | **Criteria #1**: Optum Government Solutions, Inc., and our affiliated Optum-branded companies, collectively referred to as Optum throughout our response, is a health services company dedicated to making the health system work better for everyone. With a combined Optum-wide workforce of more than 30,000 people, we deliver integrated, intelligent solutions that work to modernize the health system, improve overall population health and build and enable sustainable health care communities. Optum is heavily experienced in working with Medicaid data. We excel at building and administering data warehouses containing Medicaid claims, provider, member, and reference data. We are experts in Extract, Transform, and Load (ETL) processes and have the capability to accept extracts in a mutually agreed upon electronic format used for analysis and review activities. Optum has extensive experience deploying and integrating our predictive modeling analytics, improper payment recovery services, and other program integrity solutions for our clients. With respect to the Department's RFI, our recommended solutions not currently deployed within Colorado include: Predictive Analytics and Case Tracking that work across the entire claims spectrum from prepayment all the way through post-payment; Provider and Recipient Screening and Verification Services. We also apply our robust set of Medicaid-specific tools to leverage external data for eligibility screening and apply analytics to identify provider and/or recipient collusion. a) Because Optum believes that the request for references requests the disclosure of certain information that is not commercially available, that such contents include trade secret or other commercial information about how Optum would perform the services contemplated in the RFI, Optum is unable to provide a response to the Department's specific request for references at this time. | **Criteria #2**: Optum believes that the Department would benefit from a fraud and abuse solution that subjects claim, provider, and recipient data to additional scrutiny--over and above typical Medicaid Management Information System (MMIS) prepayment checks such as clinical editing. To be implemented effectively, such a system requires prepayment claims to be assigned numeric risk scores that enable customized prioritization of results so that appropriate clinical, coding, or investigative staff are able to perform an effective review of suspended claims to make payment determinations, target provider education efforts, and identify instances of potential recipient fraud. The solution should also address the full spectrum of fraud, waste, and abuse from coding errors to aggressive revenue maximization to collusive fraud schemes. To separate the true signals of improper billing from the other patterns inherent in Medicaid data, models need to be constructed around that data rather than designed for another industry (e.g., marketing or financial services) and moved into a health and human services setting. Thus the Optum Prepayment Review Solution (OPRS) makes extensive use of retrospective claims analysis to customize and train predictive models and analytics designed for Medicaid programs. This customization and training process can be part of or supported through a data warehouse such as the Department's proposed BIDM. The greatest risks to the success of a predictive modeling solution are threefold: that the solution will produce an unacceptable rate of false positives and provider abrasion, that it can only identify effectively a small portion of fraudulent, abusive, or wasteful billing, or that the solution's results are not transparent and/or interfaces not intuitive enough to gain trust and wide acceptance from users. The OPRS scoring engine requires a database of post-payment claims data and key external reference data sets in order to effectively identify suspect claims pre-payment. This database also contains pre-payment claims and analytics results referenced by the case management system and the Business Intelligence environment. The OPRS reporting system will use pre-payment and post-payment claims data, as well as analytics results and review determinations, from this database to measure savings, ROI, and the performance of system components. OPRS analytical models are highly dynamic and are built to rapidly adapt to new data. They also include a variety of detection mechanisms designed to target specific provider and recipient patterns. |

| **Vendor #13:** **PALANTIR** **TECHNOLOGIES** **INC.** **(PALO ALTO, CA)** | **Criteria #1**: Palantir Technologies was founded in 2004 by a handful of PayPal alumni and Stanford University computer scientists. Our headquarters are in downtown Palo Alto, California, with offices around the globe. Our company is dedicated to providing next-generation software in support of critical missions. Palantir's software represents the intersection of data, technology, and human expertise. Our platform sits above traditional data systems, enabling people to ask the questions they need answered in a language they understand. Palantir is based on the simple idea that the human mind is the most effective tool to identify patterns in information, while computers are the most effective tool to manage enormous amounts of data. As a platform company, we ship open, extensible, scalable software platforms that can be deployed immediately against the entire class of problems facing an organization in any industry. a) Dozens of government and commercial organizations around the world have turned to Palantir to address their most challenging data-related problems. Our engagement model is to deploy our software at an enterprise, iterate on a solution, and deliver substantive results in weeks, not months. By following this model, we have helped organizations achieve outcomes that were previously thought to be impossible. Born in Silicon Valley, battle-tested in the field and the commercial marketplace, our platforms are revolutionizing the way data is analyzed across a diverse range of enterprises. For more information, please visit www.palantir.com. Some of the projects and customers where we have implemented Palantir on an expedited timeline are as follows: NY Office of Medicaid Inspector General; US Center for Disease Control; and US Army and Marine Corp. | **Criteria #2**: a) Palantir has been successfully deployed against threats ranging from Medicaid fraud to contracting fraud to financial fraud. Based on these experiences, we have learned that algorithms alone do not provide the best means of detecting the patterns, trends, and anomalies that lie hidden in massive data sets. We have developed an approach to human-computer symbiosis that combines the computational power of machines with the best of human reasoning and creativity, enabling computer-assisted, human-driven analysis of data at massive scale. Palantir Hercules is our core technology for human-driven, adaptive predictive modeling and analytics. Hercules relies on adaptable, analyst-defined algorithms that traverse data integrated in Palantir and create clusters that reveal previously unknown entities, events, and connections. An analyst begins by constructing a query based on criteria such as behavioral patterns, sets of characteristics, or known entities of interest. Hercules then algorithmically combs through all data sets integrated in Palantir to create clusters of entities that match the criteria. b) The resulting clusters are ranked by relevance and presented to the user along with other visualizations such as risk scores, pie charts, and heat maps. An analyst can then drill down on specific entities for deeper contextual investigation. Organizations can easily modify Hercules' algorithms to test hypotheses and ensure that search strategies evolve with the analyst's intuition. Hercules' flexibility can be leveraged against both provider fraud and recipient fraud and can algorithmically explore billing and utilization patterns, such as excessive services, duplicate claims, and unbundling. |

| Vendor #14: SAS (CARY, NC) | Criteria #1: Headquartered in Cary, North Carolina, SAS is the largest privately held software company in the world with record 2012 revenue of $2.87 billion. We have been in the business for 37 years and our longevity is a testament to our superior software and customer service. SAS and the U.S. Department of Health and Human Services (DHHS) have an enterprise license agreement which covers every operating division, as well as contractors, and CDC grantees and there are currently roughly 10,000 SAS users throughout DHHS. Since 1976, SAS experts have integrated data, ensured its quality, and, frequently, employed a master data management strategy. We have hundreds of employees dedicated to gathering and organizing every type of data source. We understand that organizing and structuring data prior to any analytic effort is paramount to mitigating project risk. SAS is recognized by analyst Gartner, Inc. in the Leaders Quadrant in the "Magic Quadrant for Business Intelligence and Analytics Platforms, 2012." SAS/Dataflux is in the Leaders Quadrant in the "Magic Quadrant for Data Quality Tools 2012" and in the "Magic Quadrant for Data Integration Tools 2012." SAS is an industry leader (recognized by industry analysts as a key market player) in the entire fraud prevention field, spending nearly three quarters of a billion dollars annually in research and development. The continued introduction of advanced analytical techniques, such as link analysis (also known as social network analysis), into the SAS Fraud Framework is further confirmation of SAS' commitment to leadership in the fraud space. Additionally, SAS has created a global Fraud and Financial Crimes Practice, with domain expertise specifically in health care fraud. | Criteria #2: The SAS Fraud Framework for Government supports the entire end-to-end fraud detection process, including data integration, analysis, alert generation, investigation and ultimate disposition—be it an audit, recovery action, criminal prosecution or decision to take no action. The solution includes SAS Social Network Analysis to detect and visualize both top-down and bottom-up hidden and risky fraud rings and collusive networks to ensure they are visible to investigators. Rather than relying on a single detection technique, the solution combines heuristic rules to find known fraud patterns, anomaly detection to surface unknown yet unusual behavior, and predictive models to allow the system to leverage attributes of past fraud cases to identify future cases of fraud within the Department's data. And finally, the solution incorporates sophisticated link analysis and social networking capabilities to detect hidden relationships between entities. a) Whether implemented on-site in Colorado, or through SAS hosting services, the SAS Fraud Framework does not require development of a new database. The solution leverages but does not provide proprietary databases. We can work with any database solution already existing within your environment. b) While one agency may address the provider side and another may address the recipient, SAS can address both sides in one integrated solution. One key differentiator of the SAS Fraud Framework that drives incremental detection earlier with reduced false positive referrals is the SAS hybrid approach to analytics. It utilizes sophisticated scoring and ranking to surface the most relevant referrals for investigation. c) Predictive models are a core of our Hybrid approach, in which data from known fraudulent behavior from past cases within providers, recipients and networks is used to derive formulas that identify key variables and associated weightings to score claims, providers, and recipients for the probability of fraud. Anomaly detection uses distributional analysis and analyzes variables to identify which claims and provider practice patterns are extreme outliers relative to the rest of their respective distribution. The SAS Fraud Framework is built from the ground up to support workflows and various "streams" of treatment as required by organizations. With past implementations, this has included automating actions related to alerts. Those automated actions may include denial of a claim based on certain parameters and scores, pending a payment until an alert is reviewed and adjudicated/resolved, or other forms of contact with the entity. |

| **Vendor #15:** **TERADATA** **GOVERNMENT** **SOLUTIONS** **(ANNAPOLIS, MD)** | **Criteria #1**: Teradata Corporation (NYSE: TDC, www.teradata.com) is the world's largest company focused on analytic data solutions through integrated data warehousing, big data analytics, and business applications. Teradata was founded in 1979 and is corporately headquartered in Dayton, Ohio, with additional major U.S. offices in Atlanta, Georgia; Rancho Bernardo (San Diego), California; Indianapolis, Indiana; and Raleigh, North Carolina. Teradata employs more than 10,250 professionals in almost 70 countries worldwide who are dedicated to analytical solutions. The Teradata Workload-Specific Platform Family offers our customers options that take full advantage of all the power of Teradata systems anywhere in the enterprise – as an active data warehouse, enterprise data warehouse, entry-level data warehouse appliance, special-purpose data mart or sandbox environment. Our platform family ranges from symmetrical multi-processing (SMP) to massively parallel processing (MPP), and is recognized for high performance, scalability, and easy supportability. Teradata platforms are known for the processing speed, the amount of data that can be queried and the number and complexity of queries that can be run. a) Vendor's response does not specifically address this portion of the request. | **Criteria #2**: For predictive analytics, the Teradata team will utilize the Teradata Health & Human Services LDM (H&HS-LDM) to jump-start the project. The H&HS-LDM extends the underlying tenants of the Medicaid IT Architecture and Teradata Healthcare Framework. It supports an unlimited number and depth of hierarchies and relationships to reflect a complete view of an individual with the programs, services, providers, claims, agreements, financials, clinical encounters, and contracts that support them. a -c) Vendor's response did not specifically addresss these portions of the request. |

| **Vendor #16:** **TRUVEN HEALTH** **ANALYTICS** **(BALTIMORE, MD)** | **Criteria #1**: Truven Health has been a leader in Medicaid program integrity analytics since the 1980s when we delivered our first Surveillance and Utilization Review (SUR) system. We have been a federal Medicaid Integrity Contractor (MIC) since the inception of the program in 2006 and a federal Medicare Zone Program Integrity sub-contractor for analytics since the program was authorized in 1996. Our work with the Zone Program Integrity Contractors (ZPICs), a federal government project, requires us to combine Medicare and Medicaid claims data to deliver provider profiling and advanced fraud detection algorithms and models across both Medicare and Medicaid. We have extensive domain knowledge of fraud, waste, abuse, and overpayment detection and investigation business processes. Throughout our history, we have had a special focus on program integrity and analytics that control healthcare fraud, waste, and abuse within state Medicaid systems, the federal government, and health plans. Our products and services have assisted Medicaid agencies and the federal government in identifying tens of millions of dollars in healthcare fraud, waste, and abuse. Experiences in the government sector have provided us a robust framework that is used by commercial plans and managed care organizations to stop abusive billing practices. a) we currently provide payment integrity support to 24 states directly and indirectly to 14 more states through our Federal-level contracts. Truven Health has been a leader in Medicaid program integrity analytics since the 1980s when we delivered our first Surveillance and Utilization Review (SUR) system. | **Criteria #2**: Due to the complexity of detecting and eliminating healthcare fraud, waste, abuse, and overpayment, a multi-faceted approach is required. This approach must combine multiple data systems, methodologies, areas of expertise, processes, education techniques, program design approaches, and policy improvements. In tune with these needs, Truven Health has developed a solution suite that incorporates the key components required to support a comprehensive fraud, waste, abuse, and overpayment prevention program. First, we work with you to review specific areas of focus and define a tailored payment integrity strategy that best addresses your organizations' individual needs. Then, we collaboratively identify the level of solutions and services needed to achieve your desired results. This may result in a comprehensive set of payment integrity tools and services, or it may consist of a targeted strategy to fill existing program gaps. a) One proposed solution for Colorado is a software as a service (SaaS) model where Truven Health would build and maintain a database and provide access to the results. All that is required from a customer is an encrypted data feed into our data center to assess claims, providers or beneficiaries in a real-time, near real-time or batch environment. b) As mentioned previously, we utilize a variety of methods and techniques to detect fraud, waste, and abuse. We have patent pending predictive models that assess the full claims distribution – NOT just the most extreme or expensive identified by "canned" outlier models offered by others. These models have less than 15% false positive rate and are 40%+ more accurate than outlier models. In addition to our proprietary predictive models, we also apply proven analytic methodologies for fraud and abuse detection. c) Truven Health utilizes predictive models to identify when a claim, provider, beneficiary or individual behavior goes from "normal" to "out of character" behavior commonly associated with fraud and abuse. Our solution provides a foundation for more cost efficient methods of interacting with a provider, such as establishing educational work streams or queues that automatically route claims requiring closer scrutiny without disrupting clean claims processing. There are a number of approaches available in our proposed solution that support refinement and enhancement of the predictive analytics technologies, and these will be detailed in any proposal submitted as a result of an RFP. |

Vendor #17: VERIZON BUSINESS NETWORK SERVICES, INC.	**Criteria #1**: Our Team provides a complete solution for comprehensive fraud detection, including near real-time data analysis, a repository for business intelligence and data mining, predictive modeling, risk scoring, case management and dashboards. These systems have been deployed and improved for more than 20 years and are used both internally and externally by our customers. They in fact are "Made in Colorado," with our engineering team based in Colorado Springs and our fraud operations center in Highlands Ranch. Verizon delivers these same services with other partners to the Centers for Medicare and Medicaid Services (CMS) National Fraud Prevention Program through the use of our VFM solution. Verizon implemented this solution in a 60-day time period for the largest government health program in the nation. The system processes nearly 5 million claims per day. In the first year alone, the results include the prevention of more than $115 million in suspected fraud while generating a 3 to 1 return on investment. Over 1,000 investigations have been supported through the findings of the system.	**Criteria #2**: a) The solution can process healthcare claims, provider and recipient transaction data in near real-time and applies domain-specific, predictive models, configurable edit rules, artificial intelligence algorithms and risk scores to identify inappropriate patterns and outliers. Verizon will load the necessary data from the Department into the data warehouse as part of our standard implementation services. The solution incorporates standard data load file formats based on HIPAA ANSI transaction formats. Proprietary data load formats can also be supported through our Integration Mapping and Translation tools. Additional national and external data sources can be incorporated based on the needs of the Department. Verizon currently subscribes to a large number of national b) Key strengths and features of the system include: Data reduction architecture; predictive modeling; proven fraud models; resks scores and alert creations; fraud case management module; comprehensive date warehouse with analytic data mining tools; data integration tools. c) Verizon has identified a number of specific patterns that represent suspect activity as noted above. However, as previously stated, patterns evolve as perpetrators determine the most effective to game the system. For this reason, it is critical that a fraud management solution be configurable and quickly adjusted to identify and respond to new egregious behaviors. The following list provides examples of the hundreds of possibilities that are quickly configurable within Verizon's solution.

VENDOR NAME	**Criteria #3: Provide empirical details related to the performance of vendors' tools or methodologies over the last twelve (12) months.**	**Criteria #4: Provide a comprehensive and detailed description of vendors' provider and recipient data verification and screening technology solutions and how the solutions are used for the purposes of automating reviews and identifying and preventing inappropriate payments.**
Vendor #1: CERNER (KANSAS CITY, MISSOURI)	**Criteria #3**: The types of entities using Cerner Math's Bendford-type models have been ambulatory physician-office and clinic claims. In the past, Cerner has performed such model-based tests in nightly 'batches' of transactions. Cerner did not address 3a, 3b or 3d of the request. In our project with State of Tennessee, a set of 574,940 claims yielded 58,113 instances of fraud or abuse, comprised of 52,032 cases of fraud by recipient consumers and 6,081 cases of fraud and abuse by providers/pharmacies. Flagged transactions were not paid, pending supervised human review.	**Criteria #4:** Vendor did not specifically respond to provider/recipient data verification. a) HCPF data requirements would be two years of Colorado's Medicaid Claims data. Cerner would build, maintain and host the database as part of the solution. b) The User Interface visualization tool may be customized to meet the Colorado Medicaid's unique needs. c) Vendor did not specifically address this portion of the request. d) Cerner Math uses Bayesian models for representing the dyadic relationship between providers and beneficiaries. Co-clustering enables us to group providers and beneficiaries simultaneously, that is, the clustering is interdependent. The objective of this approach is to identify potentially fraudulent associations among the two or more parties for further investigation.
Vendor #2: DUN & BRADSTREET (SHORT HILLS, NJ	**Criteria #3**: a and b) D&B is in active discussions, engagement and in some instances performing pre contract analysis and pilot demonstrations with a number of large, medium and smaller state Medicaid Program Integrity offices from the West Coast, Central US, and East Coast. c) Since we have not engaged with a State Medicaid Program Integrity office for a full suite of Medicaid Fraud solution set for a year or more, these statistics are not available. In situations where we have limited scope engagements under contract in the HHS area, we do not have sufficient statistics to answer this question. d) In this particular scenario, D&B would provide the third party data assets as well as technology to integrate with another vendor analytics solution to address the goals of this approach. D&B data will not provide a "silver bullet" to "automatically" verify a claim for fraud, waste and abuse. Nor do we believe another vendor analytics system will be able to provide this "silver bullet" automatically. D&B data, along with a top analytics solution, however, will be able to quickly identify claims that fall within risk thresholds that have been established for review by an analyst/investigator prior to adjudication.	**Criteria #4**: a) D&B data assets for businesses (Providers) and consumers (Recipients) would be leveraged by the Department. We would work closely with the Department, analytics/solution vendors, and/or system integrators to bring the overall solution to fruition. b) The User Interface (UI) may be customized to meet the Colorado Medicaid's unique needs. At a high level, the UI is comprised of dashboards, graphs and trend reports. Access may be controlled at a role-based level, ensuring that correct users have appropriate access to the content. c) For the purposes of an RFI, Cerner Math, Inc. and Cerner Corporation do not feel that the disclosure of proprietary and confidential information in the form of demonstrations is prudent at this time. d) 2.1.1.2.1 In this scenario, D&B provides data assets such as a company's Financial Stress Score (financial viability within the next year), Commercial Credit Score (how prompt they are in fulfilling credit obligations), and trade activity (amount of goods and services a company is buying to conduct general business) that when combined with current and historical Provider claims—as well as other D&B and Department data elements—can immediately risk rank Providers to consider prior to payment/adjudication. 2.1.1.2.2 Vendor did not address this portion of the request.

Vendor #3: DETICA CORPORATION (BOSTON, MASSACHUSETTS)	**Criteria #3:** NetReveal currently processes all Medicaid claims, except dental and pharmaceutical, for the Commonwealth of Massachusetts. Up to two hundred thousand claims are risk-assessed in real time each day and over one million claims are processed weekly in batch to update the social networks. Investigators are currently receiving alerts, however, due to the sensitive nature of the investigations, Detica is unable to provide specifics on claims that have resulted in fraud, waste, and/or abuse. We would be happy to provide a private demonstration customized with respect to Colorado's needs to illustrate Detica's capabilities.	**Criteria #4:** NetReveal uses the same platform for recipient data verification and screening as for our predictive modeling solution. We would therefore use a single storage database for all sources. a) Detica provides a database, normally Oracle, as part of the deployment. The database can be maintained by the state or by Detica, as agreed upon during the design phase of the implementation. b) Alert Manager provides a comprehensive and highly configurable alert management and workflow environment for analysts and investigators. It provides functionality, including claims, provider and recipient information, score summaries, detailed score descriptions, disposition notation, alert history, and access to Visualizer, the network visualization and navigation tool. c) NetReveal Scenario Manager is a GUI driven scoring module that can risk-assess claims in real time or post-pay. This next generation product allows for easy configuring of new rules or models as well as the quick changing of thresholds. Scenario Manager allows the Department to break out of the mold of quarterly code releases by making every change a simple configuration change, where the only factors in how fast a change can be rolled out to production are the business processes associated with model change controls and the subsequent testing to ensure a change was made correctly. d) The NetReveal solution for healthcare includes powerful methods for the identification of collusion between the parties involved in claims. NetReveal also contains extensive scoring and behavioral analysis mechanisms for the detection of ineligible recipients.

| **Vendor #4:** **DYNAMICS RESEARCH CORPORATION (ANDOVER, MASSACHUSETTS)** | **Criteria #3:** a) For this RFI response, DRC provides information on the use of the NetReveal® predictive analytics tool suite from Detica which is employed in support of a Medicaid program in the Commonwealth of Massachusetts. This product suite is used in the commercial insurance and tax industries and has just gone into production the end of May for the EOHHS project so we do not yet have 12 months of statistics available for this project. b) The MA EOHHS implementation of NetReveal® supports provider and recipeint pre-payment Medicaid claim review to prevent improper payments, and detect potential fraud and abuse. The solution utilizes the agency's historic data, combined with external databases in order to identify improper claims before payment. c) EOHHS went live with the new predictive modeling environment at the end of May 2013. As of yet, EOHHS is not denying payments as they establish and work with the newly created pre-pay fraud detection system so meaningful statistics are not yet available. d) In the Massachusetts's Predictive Modeling Solution, NetReveal® is configured to monitor individual claim line items in order to detect possible fraudulent activity and inappropriate or improper billing in real-time. It enhances detection scenarios by building profiles for providers and recipients and scoring them compared to peer groups and social networks. Profiles are updated in real-time by claims data to trigger alerts. When a claim line alerts, a real-time message from NetReveal® to MMIS causes the MMIS to suspend the claim associated with the claim line until an investigator can resolve the alert. | **Criteria #4:** The NetReveal® solution works under the assumption that proper eligibility determination for providers and recipients are completed by the agency's system in accordance with the proper rules, regulations and policies that govern this process. NetReveal® works in close alignment with this data, and can incorporate additional internal and external data record combinations in order to detect and report individual scenarios where prior determined eligibility should be reviewed based on conflicting data found in these data sources. a) An Oracle database is created from the various data sources used to create the predictive models. b) NetReveal Visualizer™ is a powerful visualization tool allowing investigators to view complex data and identify associations that are not explicit in the underlying data, highlighting patterns of fraud or other behaviour of interest. It provides in-depth viewing of all data produced by NetReveal Builder™, including source documents, entities and generated networks. c) Once a claim has been scored and an alert has been created for this claim, NetReveal Alert Manager™ provides a comprehensive and highly configurable case management and workflow environment. Analysts and investigators use Alert Manager™ to manage queues of case work from the initial detection through to resolution and closure. The output of the predictive model is a rating for each claim with a 'score' – higher scores relate to higher probabilities of an improper claim. A score is accompanied by a risk category – red, yellow, green. A claim rated as 'green' will be automatically approved; while claims rated as 'yellow' or 'red' will be referred for investigation. d) 2.1.1.2.1 In many cases, an investigator will be able to make a decision based on the information provided by NetReveal®. They would then record whether to approve the claim for payment or for denial. In some instances, the investigator may wish to see more information about the recipient or provider in order to make a better-informed decision. This can be done by using the link analysis visualization. 2.1.1.2.2 Our incorporation of additional data sources (e.g. SSA Death Master, Corporate Records, etc.) will facilitate detection of data scenarios that may bring established recipient claims into question based on additional information that was not available or disclosed during the MMIS claim edits. The NetReveal® solution utilizes a series of publically available data sources, but is also able to incorporate any additional proprietary or subscribed data sources to which that that agency has access. |

Vendor #5: EMDEON (LINCOLNSHIRE, IL)	**Criteria #3**: a) FICO IFM is currently used by seven commercial health care payers, by two state Medicaid programs, and by one Medicare Administrative Contractor. Additionally, IFM has been used in the past by other commercial payers and state Medicaid programs. b) Emdeon's process for prospective claim review is complete and thorough, both clinical and investigational. Depending on the type of edit/flag/aberrance, the investigation can take a number of different approaches (see Figure 8 of vendor's response to Criteria #3). c) IFM claim scoring typically results in 1% of all scored claims scoring above a review threshold. That is, 1% of all scored claims are typically aberrant enough to warrant manual review using the IFM UI's Review component. Of those high scoring claims, 1 in 4 to 1 in 5 are typically found by the payer or their payment integrity intermediary to involve fraud, waste or abuse. d) IFM's "Action" functionality is designed for claim decisions by the Department reviewer within the claim review screen, with the corresponding decision – Pay, Pend, Deny, Forward (for additional review) in accordance with the Departments' decisioning workflow - sent via an automated advice file to the MMIS system.	**Criteria #4**: Emdeon proposes use of a Commercial Off The Shelf (COTS) solution for Provider Data Validation which is powered by Enclarity ProviderPoint. Emdeon's Provider Data Validation is a proven, powerful, hosted information solution that delivers. Emdeon delivers the highest quality information by tapping the best data sources, assembling the right information via our innovative AcuSync® process, and systematically verifying the results. The result is a storehouse of correct, current and comprehensive information that Emdeon calls its Master Provider Referential Database. a and b) Vendor did not address this portion of the information request. c) IFM's automatic generation of claim and provider scores and reason codes and reports and analyses that explain the aberrancy of high scoring claims and providers is designed to solve two of the leading challenges for payment integrity programs: Which adjudicated claims should we review, and why should those claims be reviewed? And IFM's web-based user interface is specifically designed for ease of use and interpretability of claim and provider scoring outcomes, enabling rapid, effective decisions of high scoring (aberrant) claims and providers. d) IFM includes a Link Analysis component that, integrated with the IFM Detection component's claim and provider scoring, identifies associations between providers, practitioners and beneficiaries that indicate rings of collusive fraudulent activity. IFM automatically calculates claim and provider scores based on FICO's time-tested IFM claim and provider predictive analytics, which consist of hundreds of direct and derived mathematical variables that are designed to deliver an "expert" point of view on aberrancy across all of the Departments' claims, recipients, providers, and procedures. By doing this work automatically for the Department, the Departments' reviewers and investigators can devote their time to the most aberrant claims and providers to the greatest and most rapid effect.

Vendor #6: GRANT THORNTON (ALEXANDRIA, VA)	**Criteria #3**: See chart starting on page 14 of vendor's response.	**Criteria #4**: Vendor did not specifically address the base question. a) Vendor did not address this request. b) The final analytic environment consists of components that are available through Performant's online browser-based tool and other delivery tools which include full claims detail, analytic detail files, claims from multiple sources to support cross-file analysis, summary data files, reference data sets. c) All test results support review through a combination of scoring, supporting details that provides an additional levels of information, charts, graphs that further support the understanding and assessment of results. d) The application of EIS Identifies associations between providers, practitioners, and beneficiaries that indicate rings of collusion. Preps and matches of data, where records across areas are rationalized and integrated.

Vendor #7: HEALTH MANAGEMENT SYSTEMS (IRVING, TEXAS)	**Criteria #3**: Our FWA services are engaged to submit referrals or to provide identification, investigation, and monitoring services on behalf of the entity via post-payment services. Automated analysis services include an array of compliance, coding, billing, and automated FWA logic that can be applied without additional resources to review data (excluding what is required as part of implementation). These services can be applied pre-payment or post-payment according to the contract and scope of the project. Used on a pre-payment basis, automated analysis can effectively prevent payment of provider claims for reimbursement that are not compliant, violate billing and coding areas, or indicate potential FWA by leveraging documented, regulatory-based logic and a flexible SaaS model. HMS identifies claims for potential overpayment and validates the integrity of the overpayment through a review of medical records. These services can be used pre- or post-payment. Vendor did not address Part 3C of the RFI.	**Criteria #4**: No single data source is both comprehensive and current, but HMS's approach to recipient verification is both comprehensive and current. To be comprehensive, HMS will access Internal Revenue Service information on behalf of the State to process its quarterly wage file and perform a real-time query to a private source of payroll information to validate current employment status. Similarly, we could perform a DMV match to verify a recipient's residency and confirm that he/she has not moved to another state. a) HMS can validate provider information against exclusion lists to identify and flag providers and their claims with identified demographic data. HMS works with data partners to validate and maintain the necessary databases to facilitate these integrity checks; the database would not require the dedication of any Colorado resources. b) HMS has implemented a series of eligibility integrity rules within IntegriMatch, some at the case/household level (e.g., income and asset) and others at the individual level (e.g., citizenship, and Social Security Number [SSN] validity). Depending on how we deliver this information, we can graphically make these rules come alive with a green "thumbs-up" if a rule is passed, with a "question mark" if there is missing information, and with a red "thumbs-down if a rule fails. Our rules can be invoked whenever data changes, whether from an applicant attestation, a data match, a query, or an applicant or caseworker change. c) HMS works closely with clients to ensure the transparency of our results. All results are available after analysis; with our SaaS solution, HMS returns results through an automated file uploaded via secure FTP.

Vendor #8: **LEXISNEXIS** **(DALLAS, TEXAS)**	**Criteria #3**: a) LexisNexis has over 40 years of experience in fraud and abuse prevention and detection, risk assessment, and analytics, over 14 years of experience specific to Healthcare. Through the identification, retrieval, storage, analysis and delivery of data, our robust product offering supports anti-fraud efforts across all major lines of business in the health insurance industry Commercial HMO, Medicaid Managed Care, and Medicare. We have also provided services directly to the Centers for Medicare and Medicaid Services (CMS). b) Our solutions have been implemented over 100 times across similar and differing health plans with covered lives ranging from 25,000 to 10 Million. Every claim line and type (Professional, Hospital, DME) is broken down to the claim line level and auto –evaluated by our solution. Our solution creates hundreds of millions of dollars in findings, yet our false positive rate is less than 1%. Because we utilize multiple methodologies on the data, when our solution identifies a problem, it is a problem. c) Our recovery platform are in use by more than 500 entities in the medical field and we have recovered over $1.7 billion dollars. d) The LexisNexis claim analysis solutions both prevent reimbursement of claims identified as having a high potential for fraud, waste and abuse, as well as passing through claims that are valid.	**Criteria #4**: LexisNexis Provider Integrity Scan™ solution leverages advanced data technology to assist the Department in verifying and monitoring health care provider licensing and credentials, and detecting and preventing fraudulent or criminal provider activity. Provider Integrity Scan automates a variety of provider verification searches and ongoing monitoring options, and provides a wide range of high risk indicators. a) The proposed COTS/ hosted (SaaS) solution would utilize two databases. The Department would not be responsible for the setup or operation of either of these databases. b) LexisNexis Relavint for Social Network Analysis (SNA) tool provides innovative visual displays of key information and relationships: between individuals and their relatives, associates, addresses, vehicles, property and corporations. c) As the claims are reviewed and prioritized using the Composite Lead Indicator (CLI) probability number, each case produced uses that CLI and will be prioritized based on that number. From there a human review is recommended and our staff can augment your staff and perform a number of the primary tasks prior to the final decisions being made on the claims in question. d) Social Network Analysis (SNA) - LexisNexis takes provider, practitioner, and beneficiary linking to the next level by offering enterprise Social Network Analysis. LexisNexis provides a robust, identity-driven, provider and recipient data verification and screening solution that first confirms the identity of the individual, then establishes the level of risk of FWA based on public records attributes, and finally monitors the status of the individual for any changes.

Vendor #9: McKESSON CORPORATION (SAN FRANCISCO, CA)	**Criteria #3**: a) The Total Payment platform, including the rules engine used by InvestiClaim, is currently being used by more than 35 clients with 105 Million covered lives. McKesson has partnered with FICO [formerly known as Fair Isaac Corporation (www.fico.com)] to bring their expertise in fighting fraud and abuse in the financial services industry into the healthcare industry. b) Our InvestiClaim clients have selected the modules that are most appropriate for their business needs, pre-payment and/or post-payment. Our breath of FWA options have been described in our response to Question 2 in this section. c) McKesson respects and values the relationships we have established with our clients. Out of consideration for our clients, it is our policy not to provide actual client results. Please refer to our response to Question 5b in this section. We have provided claim- and provider- analytics examples of savings and upcoding for Medicaid and commercial payers. d) InvestiClaim analytics can score claims in the following ways: Prepayment - allows you to identify, and therefore stop, the "symptoms" - that is, specific instances of fraud and abuse. Postpayment - allows you to diagnose and address root causes of fraud and abuse, such as pattern of fraudulent behaviors.	**Criteria #4**: McKesson's solution does not use publicly available records to automate reviews and identify and prevent inappropriate payments. However, the solution can leverage data from multiple sources to generate scores on individual claims and providers. a) InvestiClaim interfaces with claims processing systems and requires specific data about claims, providers and members. It leverages data from multiple sources to generate scores on individual claims and providers. McKesson would build and tune the initial database with input from the State. Once deployed, the database is self tuning requiring minimal manual maintenance. b) For individual claim review, the InvestiClaim claim work queues allows the Department to define precisely the type of claims which need to be reviewed, and who will review them. Any claim data element (e.g. procedure code, dollar amounts, dates, reason code, provider TIN, member ID) can be used to define which claims are to be queued. c) Once claims or provider of interest are identified and prioritized, InvestiClaim allows users to review the links between the suspect and other entities within the InvestiClaim data. InvestiClaim's Link Analysis module complements claims and provider scoring provided in InvestiClaim, adding another dimension of analysis. While claims models analyze claims data for risk, and provider models analyze providers' billing or care patterns looking for aberrant behavior to the peer group, InvestiClaim's link analysis technology analyzes networks, looking for relationships among organizations, individuals and transactions. With InvestiClaim's linking and discovery techniques, you can search across a variety of attributes – such as locations, service providers, telephone number, names, and identifiers (License, NPI, DEA Numbers) – to uncover hidden relationships behind criminal fraud rings. d) Vendor did not address part d of the request.

Vendor #10: NORTHROP GRUMMAN (McLEAN, VA)	**Criteria #3:** Our contractual obligations to CMS prohibit us from sharing performance metrics. However, we can offer the following information that CMS has publicly released on the effectiveness of the Medicare FPS that Northrop Grumman operates. Since June30, 2011, the FPS has run predictive algorithms and other sophisticated analytics nationwide against all Medicare fee-for-service (FFS) claims prior to payment. For the first time in the history of the program, CMS is systematically applying advanced analytics against Medicare FFS claims on a streaming, nationwide basis. a) The FPS system runs multiple models using a variety of commercial off-the-shelf (COTS) fraud detection products and open sources technologies. b) Techniques can be used in a pre-pay and post-pay implementation. c) Northrop Grumman processes an average of 4.5 million new claims a day and searches through billions of historical claims on a daily basis to identity patterns of fraud and abuse. The total number of claims identified and their associated payments are proprietary to CMS. d) Northrop Grumman's solution does support automatic denial of claims. While it is up to the State to determine the aggressiveness of their pre-payment approach, the use of more simplistic rule-based techniques limits the likelihood of false positives affecting legitimate payments to providers.	**Criteria #4:** Our solution can ingest and use provider and recipient data from verification and screening solutions and/or other publicly available records. a) Our existing data management platform has the capability to integrate multiple structured, semi-structured, or unstructured datasets into the solution. We would work with State personnel to examine the viability and effectiveness of integrating other datasets into a comprehensive fraud detection solution. b) The ability to view complex patterns and relationships is critical to both model development and case investigation. In support of model development, the Department should select a solution that supports the ability to derive analytical insights from large amounts of data exploratory visual analysis tools. c) The solution Northrop Grumman provided to CMS presents a rank ordered of list of entities of interest. Each entity has one or more alerts that can be analyzed for further analysis. The investigator can drill down into the claim line details that were associated with the alert. The Department should select a system that supports the ability to easily adjust rank order scoring and model specific parameters based on information entered by the investigators. d) Colorado should establish an automated identity verification system through which the State can verify and validate identities and validity of claims submitted; The use of advanced social network analysis tools is critical to identifying associations between providers, practitioners, and beneficiaries to indicate rings of collusive activity. The Northrop Grumman solution is configurable to support rules-based models that will alert on indications of improper eligibility, such as but not limited to death, out-of-state residency, inappropriate asset ownership or incarceration.

Vendor #11: OPERA SOLUTIONS, LLC (JERSEY CITY, NJ)	**Criteria #3**: a) Opera Solutions was selected competitively to provide advanced analytics to enhance operational controls and prevent fraud in the HIX Operations managed by CMS' Center for Consumer Information and Insurance Oversight (CCIIO). b) The current revenue integrity system is used both in pre-payment as well as post-payment. The impact in the pre-payment scenario is much higher as it allows end user to make changes not only on higher value charges but also for low value anomalies. The post-payment scenario allows analysts to look back at historical claims and make changes to high value charges if they were not attended to in the pre-payment scenario. This dual approach ensures that no anomalous claim slips through the system. c) Opera's current system handles more than 30-50K claims per day and holds back only a limited quantity. A second round of scoring captures any missed anomalous claims and are reviewed in the post-payment process and limits the exposure. This overall process runs in parallel with the existing system and does not affect the regular processing of claims. d) Our system currently screen's 100% of the claims and identifies potential fraud cases. Depending on the analyst workforce available, a group of high scoring claims are picked out of the regular process and held back for auditing. The rest of the claims are passed into the routine claim processing.	**Criteria #4**: Vendor did not address the base request. a, c and d) Vendor did not provide a response to this request. b) critical component of workflow management tool is to provide easy powerful reporting and visualization capabilities. Opera's FWA solution will permit users to study the predictive model results interactively. In addition to demonstrating the tables of numbers and scores, as the main point of access to the predictive modeling solution, the reporting module will enable the Analyst to explore fraud model outputs in multiple ways, using tabular results, summary charts, and more detailed graphs depicting topics such as cluster, cohort memberships, and links among entities. The interactive and easy-to-use visualization and workflow management tool provides the analyst with investigative freedom to review the claim and support data.

Vendor #12: OPTUM GOVERNMENT SOLUTIONS (ERIE, CO)	**Criteria #3**: a) A predecessor version of OPRS has been detecting fraud and abuse pre-payment for numerous Commercial, Medicare Part C, and Medicaid MCO health plans since 2009. Additionally, the recipient fraud analytical features in Optum's FADS system are being used in a number of Medicaid FFS programs. The other fraud and abuse components of the FADS system (described in detail in Response 1) are in wide use for Medicaid programs and Optum's Medicaid predictive models and analytics are being used successfully for post-payment recovery in other State health and human services organizations. b) Optum has deployed for our pre-payment review clients a comprehensive suite of predictive models and analytics to profile providers and to identify individual claims that should be reviewed before payment is made. These analytics capabilities are paired with highly effective pre-payment claims review, payment system vulnerability remediation, and post-payment recovery activities. c) As an example of the reach of Optum's pre-payment analytics, one of our predictive models for professional services scores over one million claim lines per day for one large client and suspends about 0.17% of them for pre-payment review by Optum staff. Of the claims suspended for review, about 73% of them result in an overpayment or non-compliance determination and are denied, resulting in savings of 1.5% of total professional services expenditures. d) Optum's pre-payment solutions automatically suspend suspect claims for further review.	**Criteria #4**: Optum screens new providers as they enter health care programs to assess their eligibility to bill for services and to provide an initial estimate of fraud and abuse risk based on their licensing, past behavioral identifiers including board sanctions and previous billing to other healthcare programs, and connections to other providers and participants who have billed Medicaid or other health care programs. After providers have begun billing for services, Optum's social network and other analytics leverage claims and external datasets to continually assess the appropriateness of provider billing and participation. a) Optum's provider and recipient screening capabilities require a database, which can be shared with Optum's predictive modeling solution. The database would also contains historical claims data on which Optum's screening analytics would be run in order to identify billing and utilization patterns that may indicate provider or recipient eligibility concerns. b) Optum can employ a variety of data visualization tools for provider and recipient screening including heat maps, network graphics, and geospatial analysis mapping. c) One of Optum's keys to success for program integrity is to make analytical results as transparent as possible regarding why provider, recipient, or claim information should be reviewed. d) A key component of Optum's provider and recipient screening approach is our leading-edge social network analytics that have been designed from the ground up to identify inappropriate relationships between health care providers, program recipients, and other related entities. Employing this approach allows the identification of inappropriate individual connections between participants (for example, a provider who refers patients to a given surgery center at an unusually high rate) and also unusual networks of participants and connections. In the latter network scenario, individual connections often appear innocuous unless viewed in the wider network context.

| Vendor #13: PALANTIR TECHNOLOGIES INC. (PALO ALTO, CA) | **Criteria #3**: a) Palantir was originally developed from a system used successfully at PayPal to identify fraud among millions of financial transactions. One of the largest health insurance providers in the United States uses Palantir to identify and combat healthcare fraud. The health insurer turned to Palantir to supply a counter-fraud solution that provides a complete picture of healthcare resource utilization for over 12 million members. b)   In 2011 , we partnered with New York State Office of the Medicaid Inspector General (NYS OMIG) to detect, investigate, and analyze Medicaid fraud in the State of New York. The goal of the project was to discover previously unknown networks of prescription drug fraud and investigate those networks using a variety of relevant data sources. Within two weeks of contract signing, we installed and configured Palantir Gotham to search, discover, and analyze patterns of fraud among prescription drug prescribers and users. We then integrated a number of different data sources, including pharmacy lists, provider lists, Medicaid claims data, and exclusion lists. With all data integrated into one secure environment, we performed a wide range of analyses and investigations, including: Outlier analysis on doctors and pharmacies with unusual billing patterns; cluster analysis on Medicaid providers exhibiting unusual behavior; predictive analysis on prescribers and providers, including the generation of risk score components and the implementation of predictive models; deep-dive investigations on prescribers and providers flagged for further analysis. c and d) Vendor did not specifically address this portion of these requests. | **Criteria #4**: Vendor did not address the base request. a) Vendor did not address this request. b) Palantir's data integration technologies enable organizations to access all of their data from a single workspace, regardless of size or format. To extract the most value from data sources that were never architected to exist in the same platform, an organization must develop a robust and flexible data model that can be adapted to accommodate additional data sources and analytical workflows. Palantir solves this problem with Dynamic Ontology, which lets organizations customize and change their data model even after deployment. Palantir's comprehensive suite of search capabilities allows users to search their entire enterprise knowledge base from a single intuitive interface. c) Many of the analytical instruments double as visualization tools, allowing users to explore data dynamically on a graph, map, or timeline. Furthermore, all analyses can be shared or converted into reports with just a few clicks, underscoring Palantir's collaborative nature. d) Vendor did not specifically address this portion of the request. |

| Vendor #14: SAS (CARY, NC) | **Criteria #3**: a) There are 65 entities currently utilizing and implementing the methodologies and solutions described in this RFI response. They range from Medicaid agencies to Medicaid Managed Care organizations, private health payers, insurance companies. Trillions of dollars of transactions are scored and ranked for potential fraud, waste or abuse annually. b) Within the public and private healthcare payer space (e.g., Medicaid, Medicaid Managed Care Entities Medicare, Blue Plans, etc.) our solution is utilized across a broad range of issues and areas, including: recipient eligibility; ongoing recipient monitoring; provider claim review; fraud associated with identity theft. c) As a software company that does not provide direct recovery audit, investigative or collection services, we do not have the details to answer this question. Please see select examples and details in RFI Responses 1 and 5. d) Many of our customers have not chosen to automatically prevent payment of provider claims for reimbursement, rather surfacing those with the highest risk and severity for review and intervention. However, both within the healthcare and insurance space for medical providers and within our broader customer base for the SAS Fraud Framework (e.g. tax refunds), some customers have chosen to implement with automated responses that hold payments until such time as a full review or other intervention can be taken. Others have combined that automated hold on reimbursement along with other automated actions, such as requests for additional documentation. The latter approach often has resulted in claims for reimbursement being withdrawn, or a fake entity simply "disappearing". | **Criteria #4**: SAS utilizes an analytically driven approach to risk score each enrollee as to the likelihood that they are actually ineligible. The following are capabilities of the SAS solution: profiling data across multiple dimensions such as beneficiary, households, providers, provider networks, and geographic areas. a) Whether implemented on-site in Colorado, or through SAS hosting services, the SAS Fraud Framework does not require development of a new database. The solution leverages but does not provide proprietary databases. We can work with any database solution already existing within your environment. b) Social Network Analysis helps investigators detect and prevent organized fraud. The Social Network Analysis (SNA) interface allows for easy viewing of an entire network of connections. Represented recipients, providers, pharmacies and data points are each represented by a graphical "node." c) The solution's alert queue ranks providers, recipients or networks by severity, or the likelihood that fraud or abuse is occurring. Scores provided are developed through the hybrid methodology. d) Our Social Network Analysis functionality that links providers, practitioners and beneficiaries and scores their behavior directly exists to identify collusive behavior. Recipient attributes often successfully identify not only improper eligibility of a recipient, but also identity theft being utilized in conjunction with a false provider billing mill. |

| **Vendor #15: TERADATA GOVERNMENT SOLUTIONS (ANNAPOLIS, MD)** | **Criteria #3**: The tools and methodologies referenced throughout this document are used with great success at the following public and private healthcare industry clients. a) CMS, a Teradata customer since 2005, handles the administration of the Medicare and Medicaid programs which amount to $800 billion (21% of Federal Budget) in combined funding for its 100 million beneficiaries/recipients. Today, the State of Michigan is saving 1 million dollars per day —approximately 41,667 dollars per hour or 700 dollars per minute. 10,000 users in five major departments—the two most prominent being the Department of Community Health and the Department of Human Services. b) The EDW The system has also been used to identify high-risk children for influenza vaccinations. During the 2006-2007 flu season, Michigan identified 59,000 children on Medicaid who were at risk of flu complications. Using this information, the Department of Community Health sent messages to physicians as they accessed medical records for these children, encouraging them to administer a flu shot. c) For privacy reasons, we cannot divulge the name of this customer. However, Teradata has supported this client since 1991. The Teradata system allows over 100 power users to perform advanced analytics while also supporting the ability to load over 400,000 claims each day. d) Vendor's response did not specifically addresses these portions of the request. | **Criteria #4**: Teradata partners with a number of widely known and well-respected visualization tool providers in order to satisfy the technical and business needs of our customers. These partnerships include Aster (a division of Teradata), SAS, Revolution Analytics, Tableau, MicroStrategy, Cognos, IBM/SPSS, and KXEN. a, c, and d) Vendor's response did not specifically addresses these portions of the request. b) Each of the above-referenced companies has enhanced interoperability with the Teradata database in order to support efficient in-database processing of complex operations on large datasets. This allows in-memory and permanent storage processing on the client platform to be dedicated to efficiently processing only the data needed for visualizations. These visualizations are multi-dimensional and may include, depending on product, model accuracy and misclassification graphs, model ROC curves and lift charts, scatterplots and trend lines, histograms and bar charts, pie charts, heat maps, and path analyses, amongst others. |

| **Vendor #16:** **TRUVEN HEALTH ANALYTICS (BALTIMORE, MD)** | **Criteria #3**: a) Over the past 12 months, we implemented our various tools for several state Medicaid Programs, for a dozen healthcare entities including health plans and ACOs, more than a dozen large employers, and developed FWA methodologies and algorithms to detect FWA on behalf of CMS covering more than 20 state Medicaid programs, and for other federal agencies such as Veterans Affairs. b) Vendor's response did not specifically address this request. c) Truven Health partners with a number of companies to provide the best solutions to meet their ROI and reduced fraud, waste, and abuse goals. One such company that Truven Health has worked closely with is XLHealth, a Medicare Advantage Health Plan Provider, that provides complete coverage for hospital, professional, prescription drug, and care management services. The patient population it supports is comprised of the elderly, chronically ill, and underserved. This population is also at the highest risk for fraud, waste, and abuse. d) detail how this is accomplished. Our proposed solution employs an environment that allows for automatic prevention of the payment of suspect or high-risk claims. The solution can be configured to route the suspect claims to any number of custom-defined work queues for further action. | **Criteria #4**: Our solution meets all of the requirements of ACA 6028 for provider surveillance and is also used for beneficiary surveillance. Information utilized in the screenings includes personal identifiers, names, addresses, ownership of healthcare facilities and practices, sanctions, licensure action, assets and other information that may be used to identify providers and beneficiaries who should not participate in federally funded programs. a) As mentioned previously, one proposed solution for Colorado is a software as a service (SAAS) model where Truven Health will build and maintain a database and provide access to the results. Colorado would provide an encrypted data feed into our data center and we would assess claims, provider information or beneficiary data in a real-time, near real-time, or batch environment. b) Our visualization tools display in several forms including graphical, maps, link analysis, scorecards, dashboards and reports to identify providers and claims that require further scrutiny. Additionally, our results can be moved into standard COTS software for further display and manipulation. c) The outcomes of our solution suite display results as a risk score graph, such that the most likely outliers, ie, the persons or entities most interesting from a fraud, waste, and abuse perspective, appear at the top of the report. Investigators and analysts can then select as many or as few as they have bandwidth to handle, and achieve maximum ROI for their effort. d) Our extensive use of public records to identify links amongst individuals and entities allows for a comprehensive analysis that highlights incidents of fraud, waste, and abuse by providers and recipients. Use of link analysis points to collusive relationships between providers, and between providers and recipients. The many sources of data that we use for our analysis, including individual and entity identifiers, such as SSN, EIN and NPI, addresses, family and friends, court records, ownership information, and others, allow us to paint a comprehensive picture of providers and beneficiaries and their relationship. |

Vendor #17: **VERIZON** **BUSINESS** **NETWORK** **SERVICES, INC.**	**Criteria #3**: Verizon has identified a number of specific patterns that represent suspect activity as noted above. It is critical that a fraud management solution be configurable and quickly adjusted to identify and respond to new egregious behaviors. a) The extended Verizon team provides consulting services to: a Medicaid Integrity Contractor; a Medicare Administrative Contractor; academic medical centers such as Johns Hopkins and the University of Medicine and Dentistry of New Jersey. b) In healthcare, the Verizon Fraud Management solution is being used to detect provider and recipient claims fraud, profiling of providers and detection of collusion across providers. All of these activities are being performed today in production in a pre-payment environment. We have completed other proof of concept projects with various Medicaid/Medicare programs in a post-payment environment and identified hundreds of millions of dollars in potential savings. c) Verizon client-specific results information is generally protected under non-disclosure. However, listed below are the highlights from the Centers for Medicare and Medicaid Services (CMS)' Report to Congress Fraud Prevention System (FPS) First Implementation Year 2012: Prevented or identified an estimated $115.4 million in payments; generated leads for 536 new investigations by CMS's program integrity contractors; augmented information for 511 pre-existing investigation.	**Criteria #4**: a) The Verizon solution provides a comprehensive fully integrated data warehouse/database that incorporates all of the necessary Medicaid claims, encounters, recipient, and provider file data structures to support fraud prevention, detection and data mining. No additional database would need to be built. Verizon will load the necessary data from the Department into the data warehouse as part of our standard implementation services. The solution incorporates standard data load file formats based on HIPAA ANSI transaction formats. Proprietary data load formats can also be supported through our Integration Mapping and Translation tools. Additional national and external data sources can be incorporated based on the needs of the Department. b) Verizon utilizes a wide range of visualization tools and techniques to support its data analytics and predictive modeling solution. See page 18 for illustration of the capabilities available with the Verizon Solution. c) The Verizon solution delivers a web-based, easy to use graphical user interface that is intuitive to users. All information is presented in a highly readable format. The system supports a wide variety of views including by case, patient, provider, location, patients to providers, providers to patients, charting/graphic, link analysis and geo-mapping views, among many others. d) The Verizon solution incorporates link analysis methodologies that show the relationships between providers, practitioners and beneficiaries. Through incorporating data from other Colorado Departments and external subscription sources, the Verizon solution is able to validate and correlate various sources into the fraud detection and screening algorithms to improve results. For example provider/recipient date of death or incarceration status can be quickly determined and flagged on any transaction and an alert can be generated to the appropriate user or system.

VENDOR NAME	Criteria #5: The performance of vendors' provider and recipient data verification and screening solutions described in response 4 over the past (12) months.	Criteria #6: Describe how vendors' tools, methodologies and technology will be easily integrated into a Medicaid Management Information System (MMIS).
Vendor #1: CERNER (KANSAS CITY, MISSOURI)	Criteria #5: a) Cerner Math's technology solutions have been applied to ambulatory physician offices, state Medicaid systems, and clinical claims. b) In our project with State of Tennessee, a set of 574,940 claims yielded 58,113 instances of fraud or abuse, comprised of 52,032 cases of fraud by recipient consumers and 6,081 cases of fraud and abuse by providers and pharmacies. Flagged transactions were not paid, pending supervised human review. Cerner did not address 5c and 5d of the request.	Criteria #6: Depending on the State's preferred implementation Cerner may integrate into the MMIS in a variety of ways. Data feeds from the Cerner maintained database may be considered, or web service calls via APIs. Cerner may also deliver single-sign-on technology allowing the MMIS user to launch and use the Cerner application within their normal MMIS workflow, allowing for time savings and convenience.
Vendor #2: DUN & BRADSTREET (SHORT HILLS, NJ	Criteria #5: a, b, c and d) D&B is in active discussions, engagement and in some instances performing pre contract analysis and pilot demonstrations with a number of large, medium and smaller state Medicaid Program Integrity offices from the West Coast, Central US, and East Coast.	Criteria #6: There are many ways to approach this objective. D&B data assets could be leveraged and integrated with an analytics solution of the Department's choosing to produce the desired pre-payment adjudication and the analytics system integrated with the Department's MMIS and/or other system of record solutions. In a HHS enterprise model, D&B data assets can be leveraged along the complete decision support continuum: identify resolution for an Enterprise Data Warehouse, manage risk / potential fraudulent activity of other businesses operating in the HHS environment (i.e., licensed daycare providers), manage the risk of vendor suppliers, as well as many other use cases for decision support.
Vendor #3: DETICA CORPORATION (BOSTON, MASSACHUSETTS)	Criteria #5: NetReveal has been implemented in a number of governmental agencies, including the Commonwealth of Massachusetts' Executive Office of Health and Human Services and Her Majesty's Revenue and Customs (HMRC), the UK tax agency.	Criteria #6: NetReveal can integrate with MMIS in a variety of ways, and the best way to suit the Department's specific requirements and operation context would be agreed during the analysis and design phase between Detica, the Department, and the Department's MMIS vendor. Net Reveal is built on Java Enterprise Edition (JEE) architecture which allows it to neatly interface via web-services or most other industry stand interfacing methods.

Vendor #4: **DYNAMICS RESEARCH CORPORATION (ANDOVER, MASSACHUSETTS)**	**Criteria #5**: At this time, NetReveal® is not being used by EOHHS for provider and recipient data verification or screening. a) The solution is implemented by many of the world's top fraud experts with specializations in insurance, banking, tax and healthcare fraud. These experts pool their knowledge to stay a step ahead of fraudsters. The DRC/Detica team also has a large staff of technical experts with backgrounds in statistics, math, and computer engineering. b) The DRC Team worked with the business experts in Massachusetts to develop detection scenarios that will help the agency identify possible misuse, abuse, and fraudulent business practices. These detection scenarios are made possible by bringing together independent data sources which are used to produce real-life social network visualizations of entities, actions, and intelligence. These social networks enables investigators to connect and understand relationships between recipients and providers that are otherwise hidden from a normal MMIS claim processing perspective. c and d) EOHHS has just implemented the NetReveal® solution and is working to build processes and procedures for the investigative team with regards to potential issues that the system has identified.	**Criteria #6**: Based on our understanding of the Colorado MMIS system, we understand the following integration points with the MMIS: — Historical and Batch Data Feeds – In order to undertake a predictive modeling solution, Colorado can anticipate the necessity to provide periodic updated data with information on registered providers and registered recipients. This information will most likely be provided as batch flat files for ingestion by the modeling solutions. — Claims Processing – In order to receive a risk assessment for each claim from the predictive modeling solution, Colorado can anticipate a real time interface between MMIS and the modeling solution. The MMIS system will pass each new claim to NetReveal® via a real time interface such as Web Services. The modeling solution will then process the claim and send a response back to MMIS as either to pay or suspend payment. — Investigative Staff User Portal – Investigative user will interface to the modeling solution and the claim alerts provided. They also will need an interface into the MMIS system to aid in their investigation. Claim investigation results – When an investigator reviews a claim and determines it to be valid, Alert Manager will notify the MMIS, which must then process the claim for payment. Since the solution is highly scalable, to provide the effort and cost to integrate MMIS with our solution would require joint design sessions and be part of the project to establish the predictive modeling solution for fraud, waste and abuse detection.

Vendor #5: EMDEON (LINCOLNSHIRE, IL)	**Criteria #5**: The Provider Data Validation System automatically generates confidence scores to quantify matching confidence. Team Emdeon has developed an algorithm that ties confidence scores to each element from each source in our Master Provider Referential Database that reflect the confidence of accuracy. For this reason, we score the DEA number high (authority source for this element) and the rest of the elements lower. We will also score your input to enable business rules to automate updates where appropriate (for example, replace a USPS undeliverable with a phone-validated address). a) IFM is currently used by seven commercial health care payers, by two state Medicaid programs, and by one Medicare Administrative Contractor. b) IFM's "hit rate" for high scoring providers is 1 in 2. That is, 50% of the high scoring providers are typically found to have been paid money that they should, due to fraud, waste or abuse, return to the payer. c) The number of high scoring providers which have been identified by IFM, and the resulting action taken to address provider and recipient behavior, varies by payer according to the capacity of the payer or their payment integrity intermediary to review the providers and recipients. Typically, the payers hold these results as confidential. d) In order to prevent payment, IFM should be integrated into the payer's payment process, post-adjudication, pre-payment, including integration of IFM advice files which pend suspicious claims and then which execute the payer's claim review decisions that are captured in the IFM UI's Review component.	**Criteria #6**: Emdeon's Program Integrity Suite of solutions can be customized to integrate into the Departments' current strategies and system requirements. As a flexible and modular suite of solutions, offered in a SaaS model, it is adaptable to changing environments. This means there is little, if any, need for the investment in software, hardware, or ongoing system maintenance by the Department. In order to implement a pre-payment, prospective program integrity suite of solutions, claims would have to be sent to Emdeon for review prior to disbursement of funds to the providers. Emdeon's Program Integrity suite of services efficiently identifies fraud, waste and abuse in healthcare claims, and helps payers accurately pay only valid claims, while reducing and removing wasted healthcare dollars. Safety nets combine multiple technologies, such as rules and analytics, with expert services to provide a comprehensive solution to the growing need for more efficient program integrity management. With Emdeon, the Department can choose to utilize our solution in pre-adjudication, post-adjudication/pre-pay or a fast-cycle post-pay.

Vendor #6: GRANT THORNTON (ALEXANDRIA, VA)	**Criteria #5**: Grant Thornton and Performant have an extensive track record of providing hosted integrity services for numerous state, federal, and commercial payers' largest, most complex and compliance sensitive financial and data portfolios. As all of our solutions leverage publicly available data and involve a data visualization component, the entities listed in Section 3 also apply to this section as well. Therefore, please refer to Section 3 for specific performance and result metrics pertaining to our solution.	**Criteria #6**: Performant has extensive experience interfacing with various systems resident in state and federal governments as the system of record. Using Insight, Performant has experience loading direct extracts from the Fiscal Intermediary Shared System (FISS), Multi-Carrier System (MCS), National Claims History (NCH) system, and most other claims processing systems used in Medicare, Medicaid. Performant's IT environment is tailored to flex and scale to the high demands of Colorado Medicaid's program, and meet specific Colorado Medicaid requirements and broader agency goals. Performant has the data capacity necessary to meet and perform requirements stated in the RFI. Performant maintains system data designs in accordance with HIPAA and other security regulations and policies. Insight™ could supplement the basic MMIS for surveillance and utilization review functions and detection of fraud and abuse. Information already contained in the MMIS would provide a robust source of data. Performant's solutions are designed to integrate with existing MMIS platforms.
Vendor #7: HEALTH MANAGEMENT SYSTEMS (IRVING, TEXAS)	**Criteria #5**: a - d) HMS has been supplying health plans provider and recipient verifications since 2010. A detailed overview of our experience in this area will be available during the formal RFP process. Our findings are used by State caseworkers to make a final benefit determination. With documentation and integrity as objectives, up to 50% of all cases reviewed for redetermination have been cancelled. Based upon average expenditures, savings for these clients are estimated at more than $130 million.	**Criteria #6**: As a SaaS model, HMS's solution does not need to directly integrate with the MMIS but rather operates in parallel to provide an independent, objective analysis of FWA activity. We work with data extracts and submit our findings via return files for integration into the MMIS, Decision Support System, or other databases as requested by our client. This data extract approach allows our solution to be deployed either pre- or post-payment and allows for a faster implementation than would otherwise be possible. Our solution also eliminates hardware/software compatibility issues, reduces implementation costs, and enables better ongoing support, allowing HMS to deploy a technologically advanced solution to our clients at a lower infrastructure and resource cost.

| Vendor #8: LEXISNEXIS (DALLAS, TEXAS) | Criteria #5: Empirical data on the identification and elimination of fraud, waste and abuse is typically closely held by LexisNexis customers. Few customers wish to reveal the extent of the FWA issues, or publish details on their anti-FWA efforts that may aid fraudsters in their attempts. Further complicating this is the wide range of measurements and definitions for fraud, waste and abuse. a) Please see Response 3a. b) The number of potential issues identified for providers and recipients varies based on the risk profile and policy of each customer. For example, customers with a small investigation team request that LexisNexis provide only the highest risk "hits" on potential issues, while other customers cast a broad net looking for all available fraud, waste and abuse. c) Lexis Nexis does not track specific recovery details, since most clients track their own recoveries. However, below we have provided a couple of case examples that support our capabilities in assisting agencies detect FWA. d) Historically, LexisNexis' products have a strong return on investment, whereby many our customers experience between a 4 and 8:1 return on their investment. One of our more recent State Agencies indicated that during the limited deployment pilot, they generated over $210,000 in fraud detection cost avoidance and projects that the annual fraud detection cost avoidance over $60,000,000. | Criteria #6: . First, in the pre-pay world, we employ a "do no harm" methodology whereby claims are processed, identified as questionable, and pushed to the appropriate area for review. Once a review is complete, our solution has the ability to post a daily update file to the MMIS system. This file can be constructed and transmitted in numerous formats or methods depending upon the MMIS solution capabilities for inputting claims updates. The simplest mechanism involves posting a flat file daily to the MMIS system (via web services, SFTP, etc.). The MMIS solution processes the file and the changes (Payment Commands, Provider Suspensions/Terminations, etc.) are posted. |

Vendor #9: **McKESSON** **CORPORATION** **(SAN FRANCISCO,** **CA)**	**Criteria #5**: a) McKesson Health Solutions has been providing payer-focused solutions for more than 37 years. Our FWA solution is based on technology that has been available for 17 years. The Total Payment platform, including the rules engine used by InvestiClaim, is currently being used by more than 35 clients with 105 Million covered lives. b) McKesson respects and values the relationships we have established with our clients. Out of consideration for our clients, it is our policy not to provide actual client results. We do not track this information from clients. However, clients who have InvestiClaim Claim Analytics have reported the following to: $7M in repeated hearin tests; $922K in upcoding; $3.2M in physical therapy billing; $3M from a photo-facial billing scheme. c) McKesson respects and values the relationships we have established with our clients. Out of consideration for our clients, it is our policy not to provide actual client results. Please refer to our response to Question 5b. d) Please refer to our responses to Question 5b.	**Criteria #6**: InvestiClaim interfaces with any claims agement/adjudication system. Since the analytics run after adjudication, McKesson needs only to receive the fully adjudicated claim file in the InvestiClaim data format. The analytics will not interfere with normal claims processing/adjudication or timely payment. Further scoping would be required to fully understand the Department's MMIS integration requirements for McKesson to establish an accurate and achievable implementation timeframe including effort, time and cost.
Vendor #10: **NORTHROP** **GRUMMAN** **(McLEAN, VA)**	**Criteria #5**: a) Our example Public Records Provider (PRP), LexisNexis, stays at the forefront of industry and technology trends and events to deliver the valuable insight. They assist 70% of local government and almost 80% of federal agencies in the U.S. to safeguard citizens and reduce financial losses.b) PRPs contain records on millions of individuals, including providers and recipients. They compile the following types of data from a vast array of sources from federal, state and local level jurisdictions. c and d) Data related to the FPS is considered sensitive.	**Criteria #6**: Because Northrop Grumman uses a modern, big data management platform, time and effort to integrate data from Colorado's MMIS is much less than with traditional database management tools. We can more easily consume data and ensure that data accuracy and reliability is not compromised during the analysis processes. In addition, we will establish processes to check that the agreed-upon transaction timeframes are being met and that reference data is complete and compliant to those timeframes. This is extremely important because a conflict in the timeframes and currency of the reference and transaction data will affect the claims lifecycle. Northrop Grumman can leverage our experience and expertise that we acquired via the integration of the Nation's largest public sector fraud detection system with the Nation's largest claims processing systems.

Vendor #11: OPERA SOLUTIONS, LLC (JERSEY CITY, NJ)	**Criteria #5**: Opera's analyst centric approach allowed it to design solution around the end users. All solutions are developed while working closely with end users to understand their needs, ease of usage and providing capability to provide quick feedback into the system. Current users of our anomaly detection solution are able to review claims on daily basis and based on the documentation available. a-d) Vendor's response does not specifically address a-d of the RFI's request.	**Criteria #6**: Leveraging our Vektor™ Platform, based on Open Standards (SOAP and REST Web for SOA access and JDBC connectors for SQL databases), and designed to be able to plug in a variety of different database and middleware technologies, Opera, working with DHCPF team, will be in a position to identify appropriate interfaces and integrate with the MMIS system without any impacts to the existing processing times.
Vendor #12: OPTUM GOVERNMENT SOLUTIONS (ERIE, CO)	**Criteria #5**: a) Optum provides comprehensive provider verification and eligibility monitoring for over 30 Commercial, Medicare Part C, and Medicaid MCO health plans. b) For one Medicaid MCO payer, we identified over one thousand claims in 2012 as billed by providers subject to sanctions, licensure, and specialty board disciplinary actions. c) The over one thousand claims mentioned above were all denied for provider sanctions, licensure, or specialty board disciplinary actions. d) The costs avoided from those denied claims totaled $139,743.11 in 2012 for the Medicaid MCO client. Given that these are only denied claims, it is likely that the providers would have billed a larger number of claims if not for the earlier denials, suggesting the actual cost avoidance due to identification of these providers may be considerably higher.	**Criteria #6**: Optum has years of experience working with every major MMIS vendor (including Xerox, the current Colorado MMIS incumbent), as well as major commercial health care claims adjudication systems and has developed efficient data transfer systems to rapidly send and receive complex datasets. By leveraging its experience, Optum designed OPRS to integrate easily with any MMIS in use today. We have worked with MMIS data from the largest states in the nation, including California, Illinois, New York, and Michigan, and have extensive experience working with Xerox/ACS systems. During a project for the Department, Optum will work closely with the Department and its MMIS vendor to integrate OPRS effectively and in a manner that does not adversely impact the established claims processing timelines.
Vendor #13: PALANTIR TECHNOLOGIES INC. (PALO ALTO, CA)	**Criteria #5**: a-d) Palantir fraud detection deployments draw upon the entire integrated platform, including the predictive analytics and multi-perspective analytical capabilities described in RFI Responses 2 and 4. We included a representative summary of our experiences deploying these fraud detection capabilities in RFI Response 3.	**Criteria #6**: Palantir Gotham fulfills the Department's needs for automated compatibility and integration with MMIS. Palantir can interoperate with the Department's third-party systems, applications, and data sources through Palantir's open APIs. This will allow the Department to leverage previous investments and continue to use systems with unique functionalities or capabilities that they do not wish to deprecate. Integration with MMIS would be included in our total Fixed Firm Price. Since we do not charge for services, Palantir would undertake the integration work and ensure interoperability during installation. Once the deployment is stood up, this interoperability is automated, enabling a consistent, unified system. In addition, because Palantir Gotham is open and extensible, the Department does not risk being locked into a proprietary platform or losing access to any of its data. Palantir allows data owners to retain control over their data and creates analysis and reports in non-proprietary formats.

Vendor #14: SAS (CARY, NC)	**Criteria #5**: SAS is a technology company and does not perform recovery audits, investigations or collection activities. As such, we enable our customers to succeed with the resources available to them, by providing the best quality leads through hybrid detection and social network analysis, and reducing false positives. a) As mentioned previously, there are 65 customers implementing and utilizing the full SAS Fraud Framework. This framework is our only solution that includes Social Network Analysis, which is critical to surfacing, scoring and visualizing entire fraud networks, rather than single recipients, providers or claims. b - d) As noted previously, SAS is a technology company and does not perform recovery audits, investigations or collection activities. As such, we are not embedded within our customers' proprietary end results in a manner that would provide us this data point.	**Criteria #6**: The SAS Fraud Framework and its alert queue easily integrates with MMIS systems given our data integration/data quality capabilities. Our solution does not impact the performance of the MMIS. The effort, time and cost would be dependent on the level of integration. In addition, the data points discussed in RFI Response 10 would need to be addressed to provide more information on effort, time and cost.
Vendor #15: TERADATA GOVERNMENT SOLUTIONS (ANNAPOLIS, MD)	**Criteria #5**: a and d) CMS, a Teradata customer since 2005, handles the administration of the Medicare and Medicaid programs which amount to $800 billion (21% of Federal Budget) in combined funding for its 100 million beneficiaries/recipients. Today, the State of Michigan is saving 1 million dollars per day —approximately 41,667 dollars per hour or 700 dollars per minute. 10,000 users in five major departments—the two most prominent being the Department of Community Health and the Department of Human Services. b and c) CMS, a Teradata customer since 2005, handles the administration of the Medicare and Medicaid programs which amount to $800 billion (21% of Federal Budget) in combined funding for its 100 million beneficiaries/recipients. Today, the State of Michigan is saving 1 million dollars per day —approximately 41,667 dollars per hour or 700 dollars per minute. 10,000 users in five major departments—the two most prominent being the Department of Community Health and the Department of Human Services	**Criteria #6**: Teradata has been in the business of serving the data and data management needs of the state Medicaid, Financial and Insurance communities for more than 30 years. We have experience in the Insurance industry in the areas of Claims, Underwriting, Customer Management, Risk and Finance Management, Fraud and Abuse. We also have experience in the banking sector with more than 30 successful Basel II implementations. Teradata's fraud solution consists of both Teradata and SAS components which are fully integrated on the Teradata family of analytical platforms. For example, Highmark Inc., an independent Blue Cross Blue Shield provider in Pennsylvania, uses SAS in conjunction with Teradata to detect irregular patterns. "We also rely heavily on the use of databases implemented on Teradata servers to help us retrieve process and store data quickly and efficiently" (Shawn McNelis, Highmark's vice president to health care informatics, research and analysis.

Vendor #16: TRUVEN HEALTH ANALYTICS (BALTIMORE, MD)	**Criteria #5**: a) Truven Health has successfully deployed our provider surveillance and recipient surveillance solutions to identify and terminate from their respective programs those providers and recipients who should be terminated, resulting in millions of dollars in savings for our clients. b and c) We have noted a range of issues such as: identification of businesses where the business is sanctioned at the state or federal level but they are still in business; identification of out-of-state providers who are selling products and services in other states even though they are sanctioned in their home state; identification of businesses where the owner of the NPI is being used for payment, but the owner is deceased (often for many years). identification of businesses that look appropriate but the owners should not be participating in healthcare programs because of sanctions. providers receiving payments after their license was revoked or expired. d) The results and value of savings enjoyed by Truven Health clients varies from client to client, but all of our clients have positive ROI beyond their investment in our solutions. The ROI is often dependent on how aggressive each client is in identifying and measuring savings, but it is important to note that Truven Health works with each client to assure it is comfortable with the recommended solution prior to implementation. As cited throughout this RFI, a number of examples are given to demonstrate the impact our solutions have in benefiting our clients' business model, and we are certain that we can achieve similar results for Colorado.	**Criteria #6**: Truven Health has worked, and continues to work with more than 20 Medicaid agencies, and in each project has a direct interface with the state's MMIS for claims and reference information. The direct interface allows a more robust approach to resolving claims quickly and efficiently on both a pre and post payment basis. We have found that a direct interface with a state's MMIS is also the least costly solution to fraud, waste, and abuse analysis.
Vendor #17: VERIZON BUSINESS NETWORK SERVICES, INC.	**Criteria #5**: a-d) The Verizon solution is composed of integrated tools, processes, and professional expert services such that individual empirical performance details for the component parts/services are not defined. Rather, the results of the overall solution are measured and analyzed to represent the value and return on investment. These empirical results are documented, to the degree allowable by non-disclosure agreements, under RFI Response 3.	**Criteria #6**: Our solution can be seamlessly integrated with the Department's MMIS system and other systems with minimal impact to processing times. The time and effort required to integrate the Verizon solution depends on the complexity and number of interfaces required. One of the strong features of the solution is that a standard implementation can be accomplished in as few as three to four months, thereby delivering immediate savings. The standard solution includes a fully integrated suite of predictive modeling algorithms, risk scoring tools, a case management module, and the data warehouse component "out of the box". No special databases need to be developed. Other features of the solution can be phased in over time, which minimizes the demand on the Department's current resources and reduces up-front vendor costs.

VENDOR NAME	Criteria #7: Provide details explaining your fraud investigation services that the Department does not currently possess or that the Department is not currently performing. Emphasize services that combine retrospective claims analysis and prospective waste, fraud or abuse detection techniques. These services should include: Analysis of historical claims data, medical records, suspect provider databases, and high-risk identification lists, as well as direct recipient and provider interviews. Consider in your response that emphasis must be placed on providing education to providers and allowing them the opportunity to review and correct any problems identified prior to adjudication.	Criteria #8: Provide a detailed explanation of the extent to which vendors will seek clinical and technical expertise from Colorado providers concerning the design and implementation of the tools and technologies described in your responses to improve the Colorado Medicaid fraud detection system and the method(s) for seeking that expertise.
Vendor #1: CERNER (KANSAS CITY, MISSOURI)	**Criteria #7**: Please see responses to RFI Requests 2, 3, and 4.	**Criteria #8**: a) In the past, Cerner has developed user portals to gather information, written and published white papers on findings, and offers additional services for the Cerner solutions including training and educational resources. b) Cerner has created, for all our clients, a portal called uCern where clients can find additional information, resources and topics related to their solution set. Any client can gain access to the resources and customize the content to their specific area of interest.
Vendor #2: DUN & BRADSTREET (SHORT HILLS, NJ	**Criteria #7**: D&B's approach is to bring together a multitude of public and private data attributes to the Department's disposal, along with the capabilities for D&B to provide manual investigations into businesses that do not currently have a D-U-N-S Number ® to determine if they are a viable business in operation. It is possible for a small business (i.e., single practitioner) that is new or has not engaged in enough business activity to be identified by D&B. As discussed in the narrative above, the Federal Government uses D&B as part of the SAM program to provide third party vendor identification and validation. As part of this service, vendors cannot change and update their information directly in the SAM system; they must request any changes to D&B directly. We will in turn validate and verify such changes are accurate and complete before changing the D&B record for that business. This helps prevent business identity theft and deters fraudulent activity.	**Criteria #8**: a) If the D-U-N-S Number ® is adopted as the unique Provider identifier (similar to the Federal SAM Program), D&B would work closely with the Department and/or selected vendor/system integrator to develop a Provider education framework that would educate Providers about D&B and the process required to get a D-U-N-S Number ® if they currently do not have one or to request changes to their D&B record. b) N/A

Vendor #3: DETICA CORPORATION (BOSTON, MASSACHUSETTS)	**Criteria #7**: Detica takes a proactive approach to stopping fraud. Detica's behavioral analysis and predictive analytics prevent fraud with high certainty before it occurs, reducing the need for the Department to staff a large team of investigators. NetReveal provides all the information needed in one place for investigators to action decisions quickly, dramatically increasing efficiency and output. With NetReveal the Department will realize significant savings without needing to further enhance its current post-pay investigative tools and personnel. The NetReveal suite of products is designed to work in both pre-payment and post-payment scenarios. However, our experience has shown that pre-payment produces the highest return on investment by avoiding the costly, labor intensive investigations necessary under the pay-and-chase model.	**Criteria #8**: Detica brings depth of understanding in Medicaid fraud detection from its experience at the Centers for Medicare and Medicaid Services (CMS) and the Commonwealth of Massachusetts' Executive Office of Health and Human Services. We have developed a team of ten technical experts who have engaged with subject matter experts and gained knowledge that will be applied in the context of Colorado. Detica will also take advantage of Colorado providers' clinical and technical expertise to configure an implementation that will best suit the needs of the Department. We will work with healthcare professionals prior to the go live date to validate our models so that our team of analysts understand common provider filing mistakes and ensure these errors do not trigger unnecessary investigation. a) In cases where it is necessary to provide outreach, Detica will work with the Department to develop an effective educational program. b) Detica partnered with Her Majesty's Revenue and Customs (HMRC), the UK tax agency, to create customer relations letters that informed tax payers who had incorrectly submitted their tax forms how to resolve the issue.
Vendor #4: DYNAMICS RESEARCH CORPORATION (ANDOVER, MASSACHUSETTS)	**Criteria #7**: DRC is a systems integrator and Detica is the NetReveal® tool suite provider. Although our team has subject matter expertise in predictive analytics related to claims processing and fraud and abuse detection, we do not provide traditional fraud investigation services at this time. However, we do highly recommend that Colorado build an internal predictive analytics investigative team to learn and use the tool suite as has been accomplished by EOHHS. Although they continue to outsource their post-pay investigations and the tool suite may, at some point, be used by that team, the primary focus is making predictive analytics for Medicaid fraud and abuse detection, an in-house core competency for the Commonwealth. a) These services can be provided pre-payment and the resources necessary to accomplish the investigation is highly dependent on the state's desired rate of return on its investment.	**Criteria #8**: a) Education and outreach may be more important than technology when it comes to reducing fraud, waste and abuse – or for that matter when implementing any kind of program practice change. Because of this, DRC's approach to system implementation of any type is to involve as many parties as possible, including service providers who typically do not use the system. Incorporating a wide range of viewpoints into the design, development, and implementation phases helps build a foundation of trust and confidence. b) In our Ohio Statewide Automated Child Welfare Information System (SACWIS) project, DRC held Partnership Forums to solicit input from the 88 county child welfare agencies as to the design and construction of the new system. The partnership included key stakeholders supported by DRC personnel. The Partnership formed, built, and maintained a change management framework and sponsored/championed a change management process.

| **Vendor #5: EMDEON (LINCOLNSHIRE, IL)** | **Criteria #7**: a) Emdeon's Fraud Investigative Services combine retrospective claims analysis and prospective fraud detection techniques. We review and analyze historical claims data, medical records, suspect provider databases and high-risk identification lists while also conducting patient and provider interviews. With our audit and recovery services, we also provide both desk and onsite audit capabilities. a) All analytics can be provided on a pre-payment basis. The resources required to perform the investigations in a pre-payment mode are not substantially different from those required for post-payment reviews. Certified fraud investigators, medical personnel and SIU staff would be necessary. The exact number of personnel required will depend on: • The sensitivity threshold or risk scoring level established by the State during implementation for investigation flagging; • Any outsourced SIU resources engaged by the State for pre-investigation screening, specialty investigations, overflow investigations or other support. | **Criteria #8**: a) The IFM tool is a well-established COTS solution which does not involve the timeline or costs involved with the design of a singular solution. Involvement of Colorado providers in the technical design will be limited with any COTS offering, therefore. However, Emdeon will work with the Department to involve Colorado-based knowledge as appropriate. As the solution is neural, the data learns based upon the inputs – this means that the tools and technologies described will continue to evolve, learning and applying detections to behavior and billing patterns specific to Colorado Medicaid. Emdeon offers remote WebEx and video training for all of our solutions to assist our customers with any post-implementation training that may be necessary. Training videos and FAQs are posted to ON24/7 and can be downloaded to the user's desktop for frame-by-frame guidance. b) Emdeon holds introductory and annual intrastate outreach meetings with consumer advocacy groups that represent the constituents most impacted by Medicaid |

| **Vendor #6: GRANT THORNTON (ALEXANDRIA, VA)** | **Criteria #7**: a) Effectiveness in the pre-payment environment depends on the process as much as it does on the technology. One problem in the pre-payment environment is anticipating how to address the potential output and its impact on operating units (i.e., the potential "backlog" in claims, medical review, and utilization review) and SIUs. SIUs are often overwhelmed with low-dollar claim reviews at the expense of the bigger picture: detecting provider patterns, not just investigating individual claims. Performant's solution can integrate seamlessly with Colorado Medicaid's existing pre-payment edit checks and review processes to analyze output and detect patterns. Far beyond a traditional "edit check" system, Insight™ combines the extensive findings of peer groups, comparative benchmarks, entity baselines and pattern/deviation detections developed from the entire historical portfolio of claims data. It uses that information to provide continuous monitoring and quick identification of emerging trends in Colorado Medicaid's database. b) Additional business intelligence can be found through social media, where people often input their whereabouts and reference their actions, which allows the movement of individuals and assets to be tracked. Performant has significant operational infrastructure as well as a robust staff of certified coders, registered nurses (or RN coders) and therapists that conduct medical record reviews. Performant has an extensive history of managing recoveries of overpayments and other debts for clients (i.e., the U.S. Department of the Treasury, U.S. Department of Education). | **Criteria #8**: Performant has conducted outreach on two successive CMS Recovery Audit contracts (MSP Demonstration and Region A). This was done when Recovery Auditors were still a new concept to most providers, so the outreach process had to be developed with the objectives: (1) simplifying the Recovery Audit experience, (2) informing the audience and (3) minimizing unnecessary client and provider burden. Performant is responsible for coordinating all information with providers and other participants related to the CMS Recovery Audit program. This includes addressing all concerns, and providing relevant and timely feedback. Providers consistently give Performant high marks for communication efforts. A recent survey (AHA's March 2013 RAC TRAC), found that Performant is the most responsive to providers, with 81% of providers ranking responsiveness and overall communication as "good" or "excellent." We know well that managing the people side of change is a critical success factor. In addition, we work with our clients in a train-the-trainer capacity or a facilitative capacity to share knowledge and empower individuals to own the change and the capacity to manage it. |

Vendor #7: HEALTH MANAGEMENT SYSTEMS (IRVING, TEXAS)	**Criteria #7**: HMS can provide different levels of investigative services through our in-house SIU. These services include identifying potential investigations and conducting investigations, including a preliminary investigation, an initial comprehensive data analysis, and a more extensive analysis that involves medical record review. HMS's SIU performs three primary functions for FWA: identify FWA investigations; investigate suspect claims, providers, and members; monitor providers/members. Preliminary investigations are analysis-based inquiries conducted to determine if a reported allegation or a provider/member requires further investigation. The preliminary investigation includes a complete analysis of the provider or member claims and services for a three-year period (or a smaller time frame if data is not available for the entire three-year period). If a preliminary investigation results in a determination that a provider's or member's actions indicate FWA, Colorado can initiate an extensive investigation, an in-depth review conducted in accordance with State-specific investigation requirements to determine if FWA actually occurred.	**Criteria #8**: HMS supports a collaborative approach that welcomes input from provider groups, such as medical societies, but we ensure that their input does not serve as the primary source for initiating an investigation; thus, we help to protect the integrity of the process and Colorado's ability to present findings from our investigation in a court of law. We also facilitate forums for educating providers and offering opportunities for constructive communication to this critical stakeholder group. These initiatives vary in depth and scope in accordance with the core project and client goals. Provider Portal. The Provider Portal is an online portal that providers can access for on-demand information regarding their claim data. The portal can support regular claims adjudication (deny, adjust) claims, medical record review, and recovery projects. Webinars/in-person seminars. HMS has conducted live education sessions to support specific project initiatives, including sessions educating providers on: compliance requirements; proper billing procedures.
Vendor #8: LEXISNEXIS (DALLAS, TEXAS)	**Criteria #7**: The resources vary depending upon the volume of claims, prompt pay period, number of providers, and the number of beneficiaries covered by your program. All services can be applied in both the prepayment and post-payment aspects of your program. By utilizing the advanced scoring that the combined CLI and LexID offers, we reduce false-positives to nearly none, while ensuring we can properly assess a claim within the prompt pay window established by your program.	**Criteria #8**: a) The solution integrates with our "Reach-Out" platform that allows us to quickly identify those "good players" that have "drifted" or erroneously entered information. This platform utilizes automated response collection services via web, email, SMS, and phone to contact the party requiring educational services and ensure that the education is received and perceived. Additionally, we have numerous partners in the field of healthcare educational outreach programs that contribute to our library of learning. This library may be included with the solution or simply utilize the Reach-Out platform for addressing issues as they arise. b) The Reach-Out platform has been utilized for not only education, but also employee/customer retention, address updates, and other data verification requirements by entities both externally (with their customers) and internally. One of the largest telecom providers in the world currently utilizes our platform to respond to customer inquiries, track usage patterns that may indicate a customer is not happy and help retain them through outreach and education, and to offer updates to customers on new services and get feedback on how these new features are perceived.

Vendor #9: McKESSON CORPORATION (SAN FRANCISCO, CA)	Criteria #7: We do not currently offer fraud investigation services. Our software is designed to support client internal fraud investigation operation and reducing the need for outside services. Further analysis would be required to fully understand the Department's fraud investigation operations and the mandated Colorado Senate Bill 13-137 goals. McKesson is offering a commercial off-the-shelf (COTS) FWA software solution to the Department.	Criteria #8: As mentioned in our response to Question 7a, we are offering a COTS FWA software solution. We do not offer educational or outreach programs to providers on issues relating to coverage, coding, industry best practices and medical record keeping. InvestiClaim's predictive analytics are data driven and continually run to detect new and sophisticated forms of FWA. The analytics are continuously self-learning and self-updating, enabling you to identify newly emerging instances of FWA in real-time without the need for ongoing costly system software updates. While not specific to Colorado providers, McKesson does outreach to all significant medical specialty organizations on an ongoing basis to ensure that our rule content reflects currently accepted best medical practices.
Vendor #10: NORTHROP GRUMMAN (McLEAN, VA)	Criteria #7: Northrop Grumman provides a broad range of solutions and services to the Health industry at the State and Federal level. To date, none of our contracts has required fraud investigation solutions or systems. Our strategy to provide these solutions and services, successfully accomplished on other contracts, is to identify small businesses and/or niche providers that are leaders in this discipline. Alternatively, we consider proposing as a subcontractor to a business with expertise in fraud investigation or other specialized capabilities that are not current part of our repertoire.	Criteria #8: Algorithms used to identify fraudulent claims will need constant adjustment, not only to stay ahead of those who would commit fraud, but also to limit any negative impacts of the processes on providers and patients. To address these concerns, we propose an Advisory Board that consists of not only State Medicaid and Colorado Department of Law officials but also representatives from associations such as the following: Colorado Medical Association; Colorado Hospital Association; and Colorado Medical Directors' Association. a)We propose an actively maintained portal with links to all other relevant information produced by State and Federal entities. This one-stop-shop for all relevant information can be integrated with social media capabilities to encourage provider collaboration and the exchange of ideas and can be a venue to conduct e-learning programs. Beyond the portal, the above-mentioned provider associations will be instrumental in active outreach. Rather than reinvent the mechanisms to reach participating providers, the State can leverage these associations and their networks to improve the odds of reaching all participating providers. b) Northrop Grumman operates the Fetal Alcohol Spectrum Disorders (FASD) Center for Excellence (the Center), which was established in 2001 by the Center for Substance Abuse Prevention (CSAP), Substance Abuse and Mental Health Services Administration (SAMHSA), U.S. Department of Health and Human Services (HHS). The purpose of the contract is to address the spectrum of disorders caused by a woman's use of alcohol during pregnancy. Northrop provides training and technical assistance (TA) designed to manage and transfer knowledge in order to increase care capacity among individuals, programs, agencies, systems, and states.

Vendor #11: OPERA SOLUTIONS, LLC (JERSEY CITY, NJ)	**Criteria #7**: Opera's FWA Solution will leverage a Predictive Engine that is built around a patent pending claims outlier detection solution, which includes a set of machine learning and pattern recognition algorithms to automatically capture the complex relationship among diagnosis, procedures, and patient prfile in claims data. The outliers are then identified by examining their derivation from the norm. Once key innovation is that the toolset includes both supervices and unsupervised approaches, thereby making the solution more sensitive to FWA than the outlier detection approach relying solely on either a supervised (manual) or unsupervised (automatic) mode. Opera's approach has provided a unique combination of critical experience allowing us to develop a comprehensive and innovative program to proactively prevent, detect, and mitigate fraud, waste and abuse.	**Criteria #8**: a) Opera will work closely with Colorado providers during the implementation phase to understand the current process and to be able to incorporate well with their existing system. Opera solution believes in a 2 way approach that not anomaly provides capability to identify fraud and abuse but allow the end user to provide feedback that can be incorporate back into the system to improve the prediction capabilities. Our system will continuously work with providers to supply them with constant education to improve their systems and utilize industry best practices to minimize any waste occurring in the system. b) We focus our training on skill acquisition and enabbling end users to become self sufficient in the use of the predictive modeling solution application software. With our user-friend training materials, training aids, and job aids, the end-user reference and suport is ongoing.
Vendor #12: OPTUM GOVERNMENT SOLUTIONS (ERIE, CO)	**Criteria #7**: As a result of Optum's extensive experience blending pre-payment and post-payment fraud detection with provider and recipient screening, the Optum program integrity team has an unparalleled ability to use information from across detection, screening and review activities. a) Optum employs a successful, all-of-the-above pre-payment detection and review strategy that includes sophisticated predictive analytics, detection rules based on clinical logic and industry best practices and a provider flagging and alert system based on pre-payment and post-payment analytical and review results. Many of the claims Optum suspends for review are identified and stopped by automated processes running sophisticated predictive analytics and clinical rules. These analytics are designed to incorporate feedback from review efforts on a near real-time basis and the Optum analytics team has formal processes for monitoring and assessing the results of these analytics.	**Criteria #8**: a) Proactive provider and stakeholder outreach is essential to successful implementation of any fraud, waste, abuse or other program integrity undertaking. Without appropriate outreach and education, provider pushback and appeals will proliferate. More concerning is that providers may become disenfranchised from the Colorado Medicaid Program, impacting the Department's ability to provide services to the Medicaid population. Stakeholder outreach also mitigates the likelihood of misunderstanding the project and legislative backlash. It has been our experience that the vast majority of providers support properly designed and implemented fraud, waste and abuse programs. By working closely with the Colorado provider community and soliciting feedback and input from the members, Optum and the Department will make certain that the program operates successfully and as intended. b) The following is a listing of some sample documentation that we have used when working with provider associations and individual providers, and can be found in Appendix A. A partial listing of materials we have created in the past include: a PowerPoint presentation we presented to the Kentucky Hospital Association as its Medicaid Recovery Audit Contractor; a PowerPoint presentation that we developed for our outreach and education program for individual Kentucky hospital providers; an excerpt from a letter that was used to educate a provider that he was using the wrong modifiers for surgery claims when he was submitting claims to the Kentucky Medicaid program.

Vendor #13: **PALANTIR TECHNOLOGIES INC.** **(PALO ALTO, CA)**	**Criteria #7**:a) Palantir Gotham enables integration and analysis of historical claims data, medical records, suspect provider databases, high-risk identification lists, and direct recipient and provider interviews. Our reporting framework allows Department users to easily export their analysis into shareable formats, such as PDF, PowerPoint, or Excel. Once exported, these files can be sent to third parties like providers, giving them the opportunity to review and correct identified problems. Palantir Gotham can be configured to conduct such analysis pre- and post-payment according to the Department's needs. Please see RFI Responses 2 and 4 for for a full description of our fraud detection capabilities.	**Criteria #8**: An integral part of the Palantir methodology is partnership with our clients. We work closely with our clients to gain an in-depth understanding of their hardest problems. We then iterate with them to design workflows that build on our platform's existing capabilities and produce the most effective and efficient solution to meet their goals. Palantir engineers can also collaborate with Colorado providers to the extent it would serve the Department's mission and system design goals. We fully sustain software deployments with extensive training and technical support. We provide ongoing, one-on-one training for a wide range of skill levels. Our support team is available for on-demand troubleshooting of user, administrator, or system issues. As a product-oriented company, however, Palantir does not conduct education and outreach programs. We would be happy to partner with a company or organization that specializes in that area to achieve the Department's goals.
Vendor #14: SAS (CARY, NC)	**Criteria #7**: As a technology company, we do not provide direct fraud investigative services. In past implementations, our SAS Fraud Framework solution has regularly included the types of data sources that you list here in RFI Question 7, such as: Historical claims data; medical records; suspect provider databases; high-risk identification lists, as well as past fraud and overpayment outcomes. Education and low-level interventions are highly encouraged by SAS as well as supported directly through some of our implementations. Alert thresholds and routing rules have been utilized by some customers to automate generation of letters of inquiry or asking for specific action from a recipient or provider. Others have taken an approach that was not fully automated, but still pulled certain alerts aside for a phone call or letter that provides a quick and light-handed approach to improving education and ultimately, compliance.	**Criteria #8**: a-b) As a technology company, we have partnered with customers and third-party vendors to achieve a wide range of compliance solutions to prevent not only fraud, but abuse and error. However, we do not develop education and outreach programs in-house.

| Vendor #15: **TERADATA GOVERNMENT SOLUTIONS (ANNAPOLIS, MD)** | **Criteria #7**: The real-time engine applies the risk factors, scenarios and fraud models to both real-time transactions such as click streams, payment systems and teller transactions to identify and stop fraud in process. Additionally, real-time engine can be used in batch processing to identify related transactions that appear legitimate individually, but represent fraud in aggregate. When the fraud system identifies a possible fraudulent transaction the system generates an exception and delivers the exception to a fraud investigation group for disposition via a programmatic workflow. The analyst will use case management tools to collect the exception and exception data. (e.g. descriptive data regarding the suspected fraudulent transaction.) The analyst may also bring historical data into the case management system including prior exceptions for the same customer and the outcome, data for related parties, external data – public records, location data, bureau data and more. Ultimately the analyst will reach a decision regarding the suspected fraudulent transaction – Confirmed Fraud or False Positive. The suspected fraudulent transaction will advance in the workflow to the Business Intelligence and Knowledge Management phase. Besides the analytical assets at the Department and within Teradata's Advanced Analytics Center of Excellence, we identified two companies, Health Integrity and Cahaba Safeguard Administrators, which have subject matter expertise in the field of healthcare waste and auditing. Health Integrity, LLC, is ISO-certified and provides a range of healthcare-focused services, such as predictive modeling, data mining, data analytics, compliance auditing, reimbursement policy analysis, and fraud detection and investigation. Furthermore, Health Integrity is building a Fraud Prevention System at CMS that helps identify and stop payment on suspicious fee-for-service Medicare claims until they can be sufficiently validated. Cahaba Safeguard Administrators is a service company that uses analytics to enhance clinical reviews, audits, and investigations. | **Criteria #8**: Please refer to our answer for RFI Response 7. |

Vendor #16: **TRUVEN HEALTH ANALYTICS (BALTIMORE, MD)**	**Criteria #7**: Truven Health has successfully provided services to its clients that meet the full spectrum of its client's needs, from development of prepay edits, claims reviews for prior authorization, writing or interpreting policies that align with federal and state laws and regulations, enrollment and reenrollment activities, to postpay audits and investigations, recoveries and collections. We have many partners that we use for our solutions, including thousands of investigators that can be deployed to develop cases for law enforcement. Working with clients, we identify needs and make recommendations, and then deploy whatever resources are necessary to get the job done. a) Development of a prepay solution can be accomplished through a variety of approaches, including systemically and through selected claims review by Subject Matter Experts. Each approach requires a different track, however. Truven Health recommends all the approaches be developed in concert to minimize duplicative investment costs and maximize ROI. Truven Health would be happy to detail our solutions for Colorado and provide a comprehensive prepay solution.	**Criteria #8**: Truven Health believes strongly in bringing together subject matter experts who can address current issues in fraud, waste, and abuse, and who can speak to issues specific to our client's stakeholders. As such, we would work closely with Colorado staff to identify key stakeholders and hold conversations with these stakeholders, many of whom are likely providers, to identify their concerns and propose solutions to address those concerns. a and b) Truven Health believes that strong communication with providers is key to reduction of fraud, waste, and abuse. As such, we build secure access portals for providers to obtain information about their claims, to receive alerts about their practices and behaviors that may be problematic, and to obtain general information about federal and state changes that may affect them. Additionally, Truven Health utilizes mailings and regular publications to educate providers on program changes, as well as issues that impact their profession. We conduct outreach activities by holding seminars and training individually at their site, or collectively presenting to groups of providers in coordination with provider associations and organizations. We make sure providers have the tools at their fingertips, to access information and resources quickly and easily.
Vendor #17: **VERIZON BUSINESS NETWORK SERVICES, INC.**	**Criteria #7**: The Verizon Team's medical record auditors and data analysts have worked with Medicaid and Medicare program integrity efforts based both on retrospective historical data analysis (Audit MIC, state focused audits) and pre-payment reviews (Medicare CERT program, which helps establish national Medicare error rates. a) Pre-payment complex medical audits require no additional resources than those required for traditional post-payment audits – the procedure is identical. As noted above, the team has conducted these audits for the Medicare CERT program and has accomplished them within the time limits required by statute, regulation and program policy.	**Criteria #8**: a) The Verizon Team, via HCRS, has skilled and experienced trainers in every domain of health information management, including coding, documentation and medical record keeping. The team includes coding, documentation and medical record keeping. The team includes certified trainers for ICD-10-CM and PCS coding sets required for universal use effective October 1, 2014. b) For over a decade, HCRS conducted a comprehensive coding and documentation improvement program for Air Force hospitals across the country.

VENDOR NAME	Criteria #9: Provide an explanation of resources and capabilities needed by a Medicaid program (specify the number of full time employees) to investigate potential fraud and recover inappropriate payments. Specify resources first for pre-payment then for post-payment.	Criteria #10: Provide cost/price itemization that will allow HCPF the ability to understand the detailed costs of purchasing, implementing, operating, maintaining, and updating vendors' product.
Vendor #1: CERNER (KANSAS CITY, MISSOURI)	Criteria #9: Cerner did not address the capabilities or the number of full time employees needed by Medicaid. a, b and c) Please see response to RFI request #3.	Criteria #10: Cerner estimates that total cost will range from $7.75-$9 million annually. Work effort and services provided under that cost are as follows: System installation and implementation; receipt of data from state and uploading; normalization data; creation of specific predictive models for State's purposes; end-user interface; database creation/maintenance; remote hosting and end user support.
Vendor #2: DUN & BRADSTREET (SHORT HILLS, NJ	Criteria #9: Since D&B is primarily involved in the provision of data assets to help support State Program Integrity offices in the identification of Medicaid Fraud and not as much with the analytics / technology solution and implementation / integration services—especially related to complete outsourcing models—we do not have sufficient knowledge to provide guidance in this area. In addition, Program Integrity offices that we are and have been engaged with do not typically share resource commitments and the number of investigators they have supporting Program Integrity activities.	Criteria #10: D&B pricing for the above services is based on volume, frequency and data enrichment levels. This is an estimate based on an input of 9,000 organizational Provider records and a one-year data license with quarterly updates, D&B estimates an annual investment of $75,000. In addition, there would be approximately a $45,000 annual subscription fee to Data Integration Batch (DNBi) services. DNBi is D&B's secure, web-based, core access tool used to gain real-time insight to business information. The tool is user specific and protected with unique ID's and Passwords that are assigned by D&B or a Department Administrator. Without transaction volume or potential users an accurate estimated investment cannot be determined. However, the above-referenced $45,000 subscription price is based on similar D&B. Lastly, according to D&B's response, there may be another charge of $40,000 for Data Integration Batch Monitoring and DNBi alerts.

| Vendor #3: DETICA CORPORATION (BOSTON, MASSACHUSETTS) | **Criteria #9**: NetReveal brings together all relevant data needed to make rapid and accurate decisions into one place. This dramatically increases the Department's existing fraud investigators' efficiency without a need for more staff. During the design phase of implementations Detica works with clients to determine the optimal number of alerts that should be generated based on the size of the investigative team and the Department's priorities. Detica will configure the thresholds of fraud scenarios to conform to the Department's needs, as too many alerts would mean the majority would not be able to be worked before they timed out and were paid. Alternatively, too few alerts would cause investigators' time to be underutilized and a higher level of fraud to be tolerated to pass through the system. Department investigators will need a solid understanding of Medicaid claims processing and investigation as well as knowledge about providers, recipients, and regulations. a and b) As the NetReveal solution went live in Massachusetts in May, outcomes have begun to accrue, but unfortunately due to the sensitive nature of this information, Detica is unable to report the specifics in a public venue. c) NetReveal provides all the information investigators need to make rapid decisions in one place. HMRC's users commented that "you can see quickly what you need to get on with or put aside which is a massive help to our investigators." | **Criteria #10**: Due to the unique way in which we work with our customers, we are unable to provide specific pricing given the information contained within this RFI. Detica has a long history of highly successful and value-added implementations and we look forward to the opportunity to meet with the Colorado Department of Health Care Policy and Financing to efficiently scope and price a highly effective customized solution. |

| Vendor #4: DYNAMICS RESEARCH CORPORATION (ANDOVER, MASSACHUSETTS) | **Criteria #9**: a) Pre-Payment: EOHHS has hired a full-time staff of 5 pre-pay investigators with a supervisor, (Predictive Modeling Initiative or PMI Team) to design, learn and actively work with the NetReveal® tool suite that is currently in production. The current EOHHS PMI Team has a combined background in forensic accounting, post-payment review, bank accounting, and some amount of investigative processes. This staff was initially tasked with working with the DRC team to select the complete set and initial set of data sources, define the data mappings and initial scorecards to target recipient and provider abuse, learn the operation of the tool suite and monitor/adjudicate the alerts generated by the tool suite. Since this is an entirely new approach, with no internal state staff working as fraud investigators prior to the go-live, EOHHS is taking a conservative approach to implementation, with a 10-month stabilization/enhancement period and anticipates eventually doubling the size of the PMI team once the scorecards, data sources, processes and procedures are fully deployed over the next year. Post-Payment: The outsourced fraud investigation services does not currently utilize predictive analytics or modeling in their investigative services nor does the Attorney General's Office but that may be a future activity. b) Since EOHHS has only recently gone live, there are no outcomes to report at this time. c) Pre-Payment: The outsourced fraud investigation services does not provide pre-payment investigative services nor does the Attorney General's Office, at this time. Post-Payment: Prior to the implementation of the pre-payment model and in parallel with it, EOHHS has traditionally used the services of UMass Medical School's Center for Health Care Financing (Center) to analyze claims based on investigative experience, to identify and document potential waste, fraud and abuse. To support the investigative process, EOHHS has a set of Cognos cubes and data mining reports for post-payment review processing. Once documented, the information is turned over to the Attorney General's Office for investigation and recovery. No predictive modeling tools are currently used in this process and EOHHS is expecting that once the pre-pay modeling tool suite is tuned and the Predictive Modeling Initiative team is in full operations, the post pay arrangement may no longer be necessary or may evolve to a different focus. | **Criteria #10**: a) The predictive modeling and analytics tools and services provided to EOHHS included the following scope that was completed within a 12-month Base Year: — integrate with the existing Medicaid claims processing system; — integrate with third party data and data sources; —analyze claims using predictive modeling; — provide a score for each claim in real-time which will indicate the probability that the claim may be improper; — incorporate a user friendly workflow to allow analysts to review and investigate highly-scored claims; — capture claim disposition and; — provide management reporting capabilities. b) Although the official provider and recipient verification process is an MMIS function governed by the agency's eligibility determination practices and policies, the NetReveal® solution includes certain data verifications and associated alerts of the data includes conflicting information in this regard. This is a part of the standard NetReveal® data extract. No separate cost structure is associated with this function of the solution. c) NetReveal® uses an Oracle database that is created to hold and interactively update/link the 'ingested' data, scorecards and business rules and is maintained as part of the services. d) Pre-Payment: These services are currently provided by 5 state staff using our predictive analytics tool suite as implemented by the DRC team for pre-pay analytics. Documented cases of fraud and abuse are then turned over to the State Attorney General's Office for prosecution. The plan is to increase the staffing to 11 which will include a supervisor. However, DRC does recommend that a solution implementer component of fraud investigation services be part of the RFP. Since an entirely new business model is being implemented for which an organizational structure, internal skill sets and/or processes and procedures do not yet exist, having an experienced implementer provide this initial support, mentoring, consultation and knowledge transfer would be extremely useful for getting a new PMI team up and going during the first 6 months. Post-Payment: Traditional post-pay fraud investigation services are provided by the Center and documented cases of fraud and/or abuse are then turned over to the State Attorney General's Office for prosecution and recovery of funds. |

Vendor #5: EMDEON (LINCOLNSHIRE, IL)	**Criteria #9**: Project Manager (State Employee); Clinical Analyst (State Employee); Integration Engineer (State Employee); IS Staff (State Employee). Additionally, virtually all of the support and maintenance will be provided by Emdeon after implementation. We will need a technical contact from the Department if there is a connectivity issue or data-related issues once the interface goes live. This contact will only be needed, if a support issue develops. a) Team Emdeon suggests that high scoring claims should be reviewed and decisions made by experienced claim reviewers – typically certified coders, medical professionals, etc. who have an innate curiosity about aberrant claims, who are committed to the elimination of fraud, waste and abuse, and who have a good understanding of the payer's payment policies. b) Team Emdeon will perform initial verification of the data using ProviderPoint and will complement this validation with data driven analytics to score providers for aberrant patterns in their enrollment or billing data. During early stages of project definition a gap analysis shall be performed to determine gaps between Department requirements and the existing capabilities of the system as described herein. Emdeon shall provide documentation of this gap analysis and a project plan defining commercially reasonable steps to address these gaps. c) For over 20 years Emdeon's Special Investigation Unit (SIU) has been analyzing claims for potential fraud, waste, and abuse. This seasoned team includes clinicians, coders, investigators, law enforcement agents, etc. These individuals request and review medical records and investigate claims. Our analysis incorporates data mining and analytic techniques and includes both clinical and investigational review on all identified claims.	**Criteria #10**: Emdeon will provide detailed pricing requested during any future Request for Proposal. The pricing models would vary based on the services contracted by the State. Technology pricing is typically based on a volume-based license, with separate fees for implementation and any State-specific hardware requirements; this would include the creation and maintenance of any data bases and data source links. Fraud investigation services may be priced on a case or contingency basis, depending on the type and breadth of investigations performed for the State.

Vendor #6: GRANT THORNTON (ALEXANDRIA, VA)	**Criteria #9**: In order for successful implementation and ongoing success, we anticipate the following demands on Colorado Medicaid staff as a result of the scope of services: Access to investigative staff for solution optimization and training; Availability of working leads; assessment of analytic results relative to the existing base of Colorado Medicaid program knowledge; suggestions of lines of analytic inquiry that are recognized as having potential significant value; broker access to additional information that may be needed to validate results or define analytic targets. This could be additional sources of data within the State, or occasional outreach to the provider community for the testing of results; normal and expected project management activity, including participation in onsite meetings, conference calls, etc. by appropriate staff; additional program specific expertise. Based on this necessity, the following CO Medicaid resources should be provided as part of the assessment: Designated CO Medicaid project manager/point of contact to facilitate the transfer of data, project meetings, data link to CO Medicaid and all other project management needs; an Information Technology point of contact; access to claims data and a file transfer feed; a presentation or review package detailing CO Medicaid's historical fraud findings, a review of CO Medicaid's current solution; review of CO Medicaid's claim systems to facilitate the CO Medicaid-EIS interface. In order for successful implementation and ongoing success, Performant advises special attention to the following areas: Structured coordination of Performant and State activity, as related to the solution; access to State-owned processes, procedures, and related documentation; availability of timely, ongoing feedback from the State.	**Criteria #10**: Staff assigned to the project will depend on scope, workload and volume thresholds determined through the scope of work and contract discussions. The teams can range from 2 to 4 professionals supporting the program on a full time basis for a small program, and expand to 8 to 10 professionals for a larger program. Pricing is highly dependent on the size and scope of the engagement.

Vendor #7: HEALTH MANAGEMENT SYSTEMS (IRVING, TEXAS)	Criteria #9: Resources needed to conduct FWA reviews vary depending on the scope of the reviews. Using the numbers provided in the RFI, HMS resource requirements for implementation of the full FWA solution include the following: Managing the Outcomes for our Behavioral Analytics, including predictive modeling and analytics tools: One FTE is required, more FTEs can be employed if Colorado wants to be actively involved in FWA targeting; the number of Colorado resources that are needed for recipient verifications depends upon how IntegriMatch is implemented. Dependencies include the depth and breadth of required data matches; one FTE would be required to manage investigation services, if Colorado chooses to have HMS perform all investigative functions.	Criteria #10: HMS's cost structure and fees vary depending on the scope of services ultimately required based on the project's financial and program integrity goals. Based on Colorado's documented goals, an FWA project could be handled on a pre-payment or post-payment basis or a combination of both, and pricing would be adjusted accordingly. HMS has found that a Per Member per Month (PMPM) or fixed fee payment method is best employed for prospective analysis services since it promotes the application of all relevant compliance requirements regardless of financial impact. While HMS can provide both retrospective or prospective services, we recommend prospective services as it targets both low-dollar and high-dollar overpayments efficiently. SIU services are offered for an hourly fee, which ensures that any investigation identified and conducted is performed in an unbiased manner. Recipient verification fees are offered on a per case per year basis so that data matching and integrity checks can occur not just at application or redetermination points, but also periodically throughout the year. HMS would recommend allocating between $900,000 - $3 million annually for budget purposes based on the scope and services required of the final project, or $0.12 - $0.40 PMPM.
Vendor #8: LEXISNEXIS (DALLAS, TEXAS)	Criteria #9: a) The LexisNexis provider and recipient verification and screening solutions are highly configurable, and designed to provide flexibility in returning results based on the policy and available staffing of each customer. While the exact number of staff is dependent upon the programs' volume of claims, number of providers, number of beneficiaries, and the types of services covered, we can quickly demonstrate what the most cost effective number of staff should be in your office. b) We offer all of the functionality of a program integrity office and also offer extensive knowledge of the new requirements of the Affordable Care Act (ACA). This includes how to report recoveries, preventions, and how to account for the funds associated with the same. Our ability to help your state time recoveries and account for funds can make millions of dollars of difference in the general fund.	Criteria #10: LexisNexis Fraud, Waste and Abuse solutions are comprised of several pieces, for which we offer a mix of pricing options. Our goal is to keep the Department's costs as predictable and manageable over the life of the contract as is reasonable. Thus, several components may be structured on a fixed-price basis or may include variable charges for items such as percent of recoveries, or optional Performance-based incentive fees. As the Department continues to evaluate and refine the particular solutions and services that will meet your needs, we would like to further discuss ways that our solutions align with those business and budget needs.

Vendor #9: McKESSON CORPORATION (SAN FRANCISCO, CA)	**Criteria #9**: a) Implementation and support services would be performed by experienced McKesson employees. Further scoping would be required to establish what InvestiClaim offerings would be appropriate for the Department and number of full time employees need to support the solution. b and c) McKesson does not offer outcomes reported by data verification and screening technology solutions.	**Criteria #10**: a and b) No response was given. c) Our COTS product licenses are offered on a term license basis. Without a specific set of requirements, McKesson is unable to provide a cost estimate. Many factors contribute to the cost of the solution such as the breadth of functionality to be deployed, number of covered lives, whether the solution is internally or externally hosted, and the division of ongoing operational responsibilities. d) McKesson does not offer fraud investigation services. McKesson is offering a COTS FWA software solution to the Department. e) Implementation and support services would be performed by experienced McKesson employees. During the solution design process, we will evaluate the solution implementation requirements and at the conclusion, McKesson will be in a position to provide staffing specific to the Department. However, we recommend the involvement of the following Department staff both during and post implementation for both pre-payment and post-payment use (percentage of commitment varies depending on the project phase both pre and post implementation): Program manager; project manager; IT Lead; SME; data analyst; internal training lead.
Vendor #10: NORTHROP GRUMMAN (McLEAN, VA)	**Criteria #9**: a-c) Because all information provided under this RFI is subject to the Colorado Open Records Act, Northrop Grumman is not providing labor estimates as requested. As pricing related information is considered proprietary, its visibility to our competitors could compromise our competitive position on any follow-on bid.	**Criteria #10**: a-e) We have a comprehensive approach and tools to develop prices for systems and solutions responses. In addition, to develop a price, we use our relationships with an array of hardware and software vendors to assess the capabilities required and the Total Cost of Ownership (TCO) to the customer. We also use a significant quantity of data from prior programs to develop basis of estimates (BOEs) using techniques such as engineering estimates, historical data analysis, and similar analysis to accurately quantify labor estimates. We will apply these tools and techniques if given the opportunity to purse future solicitations.

| **Vendor #11: OPERA SOLUTIONS, LLC (JERSEY CITY, NJ)** | **Criteria #9**: The requirement of number of full time employees in fraud investigation unit will largely depend on several factors: Claims volume; score threshold; and analyst productivity and the requirement for closing a case. Vendor's response does not specifically address a-d of the RFI's request. Vendor's response does not specifically address a-d of the RFI's request. Vendor's response does not specifically address a-c of the RFI's request. | **Criteria #10**: Opera Solutions recommends a two phased approach that consists of a Diagnostic Phase and an Implementation Phase. The diagnostic Phase (Phase I) is typically completed in 8-12 weeks and consists of gathering info, and assessing the available date to confirm model development and deployment options. We prefer to price the Diagnostic Phase as a Time & Materials effort to cover our personnel and travel costs. A Planning number of $250-300K is typically the cost of such an engagement. The Implementation Phase (Phase 2) is typically completed in 6-12 months and consists of determining the model(s) to be build implementing the Vektor platform, developing the models using Opera Solutions algorithms and methodologies, and building case manager software. The overall cost for the Implementation Phase falls under the following headings: software license fees; customization and implementation fees; application hosting and related costs and expenses; business consultation services; fraud investigation services; and maintenance. |

| **Vendor #12: OPTUM GOVERNMENT SOLUTIONS (ERIE, CO)** | **Criteria #9**: Optum's predictive modeling and screening solutions are flexible and adaptable enough to accommodate a variety of staffing arrangements. The number of claims reviewed by State staff may differ greatly from one State to the next, depending on each State's approach to preventing improper payments. This is also true of the resources needed to review provider and recipient eligibility cases, though the degree of variation and overall staffing requirements will likely be lower for this solution. a) Some Medicaid states may wish to review all claims identified by the scoring engine as having a likelihood of improper payment (of any kind) above a certain level, e.g., 60%, in the expectation that providers will correct their billing and re-submit the claims. This approach can lead to significant pre-payment and post-payment savings; but may also require more full-time employees than a lower volume approach. b) Optum estimates that one full-time employee would be required for the Department's use of Optum's provider and recipient screening solution. This may be one dedicated staff member or two of them each performing different types of reviews with part of their time. These employees should have some fraud detection and/or auditing experience and have an in-depth knowledge of Department provider and recipient eligibility policy. Similarly to the predictive modeling solution, Optum can supply experienced fraud and eligibility reviewers to supplement Department staffing if needed. c) The Fraud investigation services described in Response 7 would complement and support the Department's review efforts. Optum believes that these services would improve the effectiveness of the Department efforts, increasing savings and reducing provider abrasion, without requiring any additional post-payment or pre-payment review employees. | **Criteria #10**: Given the general nature and purpose of the RFI to seek to determine to what extent products exist in the marketplace, lack of final Department decision making of the requirements that will ultimately be incorporated into the BIDM, uncertainty whether the optional prepayment and EVV solutions will ultimately be incorporated into the 2013 MMIS RFP award, and an inability for RFI respondents to mark sections as proprietary and confidential, Optum is unable to provide specific pricing detail for items a and e in RFI Response 10 at this time. However, we provide some pricing-related recommendations and observations for the Department to consider below. For the OPRS solution, Optum suggests a fixed fee contract; however, the Department could also consider a contract based on a per-claim or per-member-per-month basis. The primary factors influencing the cost of a system like OPRS are likely to be: Design, development, implementation; the number of recipients enrolled and the corresponding claims processed; whether OPRS would use a dedicated database or leverage data from another system; maintenance, modifications and updates; whether the Department seeks a hosted solution; training for end-users at startup and ongoing. |

Vendor #13: PALANTIR TECHNOLOGIES INC. (PALO ALTO, CA)	**Criteria #9**: a-c) As a scalable platform, Palantir Gotham is can be used by teams ranging from 20 to 2,000 members. Our platform produces cutting-edge fraud detection by combining human expertise with computing power and visualization capabilities. We can adapt Palantir Gotham to maximally achieve the Department's fraud detection goals with the resources available to it.	**Criteria #10**: a-e) Palantir Gotham is licensed based on the number of "server cores" required to run the platform. This places no hard limit on the number of users or the quantity of data. Instead, it accounts for both factors as increased user and data scale requires more processing power. The specific number of cores required for this deployment will depend on the scale of the project, including the types of data sources involved, the amount of data to be integrated, and the quantity of concurrent users that will access the platform. There is a non-linear relationship between data/user scale and number of server licenses needed. For example, if the number of Palantir users (or the amount of data) doubles, the organization will not need to license double the number of server cores.
Vendor #14: SAS (CARY, NC)	**Criteria #9:** a-b) The number and type of alerts generated will be based on Colorado's actual data and past cases utilized for predictive modeling, which is not currently available to SAS. Our solution is highly configurable to threshold-based alerts depending on risk score (likelihood of fraud, waste or abuse) as well as potential severity (dollars at risk). This last piece is critical, as we have implemented solutions in the past for customers that expected no increase in audit or investigative resources, and even some that faced further cuts. c) As a technology company, we do not provide direct fraud investigation services.	**Criteria #10**: A variety of factors determine cost, therefore, we welcome the opportunity to meet with the State to gain additional insight prior to providing a specific estimate. Colorado will need to make some specific decisions, as well as provide additional data points, including: Implementation for providers, claimants or both; only post-payment, or pre-payment as well; number and types of data sources to be integrated and modeled against; Number of providers and volume of billings; approximate total volume of data (in TB); number of expected users; hosted or non-hosted solution.
Vendor #15: TERADATA GOVERNMENT SOLUTIONS (ANNAPOLIS, MD)	**Criteria #9**: Please refer to our answer for RFI Response 7.	**Criteria #10**: Unfortunately, Teradata cannot provide level-of-effort or cost itemization without understanding more about the Department's current system hardware, analytical environments, and data requirements. However, we offer a low-cost Proof-of-Concept Workshop in which Teradata's industry-leading consultants spend a day at your worksite to better understand the Department's needs.

| **Vendor #16:** **TRUVEN HEALTH ANALYTICS (BALTIMORE, MD)** | **Criteria #9**: a) All of Truven Health prepay and postpay models output is geared to highlight those providers and recipients who present the highest risk and to maximize investigative ROI. As such, all the reports, graphs, maps, and other output of our analytic tools identify the worst offenders first, allowing clients to deploy their resources to address the most serious cases and recover the most overpayments. b) Truven Health's results and output provide risk scores on individuals and entities that compare targets against others to highlight the worst offenders. As such, clients can quickly and easily pursue recoveries, and have defensible criteria to support their actions. c) Truven Health provides services that run the entire gamut of possible services, including prepay and postpay analytics, audit and investigative services, development of unique solutions tailored to particular client needs, case management services, enrollment and reenrollment activities to meet ACA 6028 compliance requirements, and many other services. We utilize many sources of public data to build profiles of individuals and entities that are used in our link analysis tools; we even provide fingerprint-based FBI background screening. | **Criteria #10**: Truven Health is mindful of client budgets and resources, and as such, prices our solutions in a way that ensures all clients have a positive ROI in comparison to cost. Truven Health will price its recommended solutions for Colorado when submitting its proposal in response to your RFP. |
| **Vendor #17:** **VERIZON BUSINESS NETWORK SERVICES, INC.** | **Criteria #9**: The official current national error rate for Medicaid payments is 7.1%.1 Nobody really knows how much of that is fraud, but it is clear that Colorado's current fraud recovery rate of 0.1% can be significantly improved. Staffing the Fraud Control Unit will not be driven by the amount available for recovery – that will amount to hundreds of millions potentially – but by the practical realities of government staffing. a-c) This is still a relatively new science, but experience suggests that resources invested in investigating and bringing forward providers identified as aberrant at three standard deviations from the profile mean in a predictive modeling solution produce ROI in the range of $7 to $16 for every dollar invested. If the FWA solution is working correctly, the limitation is not the amount of money to be recovered but the practical reality of how many FTEs are available for deployment. | **Criteria #10**: Verizon's solution and supporting optional services deliver a rapid return on investment to customers through the identification of fraud, waste and abuse opportunities and optimization of operational activities to manage prevention. Verizon is able to offer the Department multiple options for the implementation of its solution and would work with the Department to provide the best value and approach based on the following services: Managed Service Model; Price by Component; Professional Services Hourly Rates; Custom based on individual customer requirements |

ATTACHMENT C
SUMMARY BY VENDOR

CERNER

EXPERIENCE: Cerner is the leading U.S. supplier of health care information technology solutions that optimize clinical and financial outcomes. Around the world, health organizations ranging from single-doctor practices to entire countries turn to Cerner for our powerful yet intuitive solutions. Cerner offers clients a dedicated focus on health care, an end-to-end solution and service portfolio, and proven market leadership.

Cerner Math's suite of fraud detection models utilizes works including Benford's Law. Benford's Law works because nature produces more small things than large things. Benford's Law predicts that amounts will start with the digit 1 more often than the digit 9, and it provides a mathematical formula describing the percentages. The digit 1 should show up about 30 percent of the time, while the digit 9 should occur less than 5 percent of the time. In medical claims, the distributions of digits deviate from Benford's Law due to payer constraints and charge master rates, but nonetheless the digit distributions can accurately detect outliers and fraudulent transactions, through the use of Kolmogorov-Smirnov and related tests. Cerner Math's Bendford-type models have previously been successfully applied to ambulatory physician-office and clinic claims (e.g., for CPT-4 codes 99201-99205, 99211-99215, 99241-99245). In the past, Cerner has performed such model-based tests nightly 'batches' of transactions.

In our project with State of Tennessee, a set of 574,940 claims yielded 58,113 instances of fraud or abuse, comprised of 52,032 cases of fraud by recipient consumers and 6,081 cases of fraud and abuse by providers/pharmacies. Flagged transactions were not paid, pending supervised human review. Therefore, Cerner Math and Tennessee implemented a proactive fraud abatement and automated pre-payment process to avoid costly 'pay and chase' models.

PROCESSESS: Cerner Math's fraud detection and fraud prediction and pre-payment prevention models run in a cloud-based computing environment. The data are extracted, translated, and loaded continuously into the cloud and thus do not require separate data-transport and duplication as occurs in other systems that utilize SAS or other traditional statistical packages. Cerner Math fraud detection and pre-payment fraud prediction methods use cutting-edge machine-learning algorithms such as Bayesian Networks, co-clustering, and Support Vector Machines. Cerner Math performs correlation checks to delete redundant features; and the discriminating power of each feature is tested and only those features with discriminating power above a certain threshold are retained in the predictive models. In our work to-date, the number of features selected for fraud detection ranges from 8 to approximately 50.

For the best results, payers like Colorado aim to deploy predictive analytics before payment, either prior to or during adjudication. Unlike rules-based systems, data-driven analytics detect data anomalies and trends and find not only aberrancy that exhibits previously-recognized features, but also identifies unknown and emerging schemes that rules-based analytics do not recognize. The Cerner Math models provide reasons and contextual information so investigators and analysts have actionable evidence upon which to make decisions.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Today, most competitors' pre-payment systems are rule-based and utilize clinical code screens and edits. These software solutions apply clinical code edits to incoming claims to determine if the claims comply with the payer's payment policy. Payers can use these solutions pre- or post-adjudication, but always before they pay a claim. Rule-based systems require continual manual updating to accommodate changes in policies and in medical practice. By contrast, Cerner Math's stream-based pre-payment co-clustering models and Bayesian networks do not entail labor-intensive human updating. Cerner Math's models produce scores that represent the probability that each claim is fraudulent. Your organization determines a threshold value where a claim, provider or beneficiary behavior causes a claim to go from a condition that is considered normal to a new and different condition, which is labeled as either potential fraud or abuse. The score is defined as the value that represents the probability that one or more of the claim, provider or beneficiary features, as measured on a scale of zero to one, is likely fraud or abuse. At a predetermined value on the scale between zero (0) and one (1), the likelihood of being an aberrant claim, patient or provider is so great that the observation is labeled as "likely fraud or abuse."

OUTREACH AND PROVIDER EDUCATION: Cerner is widely respected for our transparency and access to data. In the past, Cerner has developed user portals to gather information, written and published white papers on findings, and offers additional services for the Cerner solutions including training and educational resources. Cerner has created, for all our clients, a portal called uCern where clients can find additional information, resources and topics related to their solution set. Any client can gain access to the resources and customize the content to their specific area of interest.

REQUIREMENTS AND STAFFING: Colorado state data sources are all that are needed. A separate database will be required. This database will be built and maintained by Cerner. Depending on the State's preferred implementation Cerner may integrate into the MMIS in a variety of ways. Data feeds from the Cerner maintained database may be considered, or web services calls via APIs. Cerner may also deliver single-sign-on technology allowing the MMIS user to launch and use the Cerner application within their normal MMIS workflow, allowing for time savings and convenience.

COSTS: Cerner estimates that total cost will range from $7.75-$9 million annually. Work effort and services
provided under that cost are as follows: System installation and implementation, receipt and upload of data from the State, normalization of data, creation of specific predictive models, end-user interface, database creation and maintenance, remote hosting and end user support.

To realize the full value of a payment integrity solution, the state must have adequate processes and trained staff to manage the solution. Workflows and processes will likely be adjusted, but subsequent benefits are likely to be apparent to internal departments and divisions as they achieve more effective fraud and abuse prevention. Though payment integrity solutions should include the best and latest technology, the right blend of services and personnel is essential. In particular, when fraud is detected pre-payment, there is a need for discerning and experienced fraud investigators and analysts.

DUN & BRADSTREET

EXPERIENCE: For over 30 years Dun & Bradstreet (D&B) has supported and assisted Federal, State, and Local government departments and agencies in the mission critical areas of Data Management, Financial Oversight, Fraud Detection, Homeland Security, Acquisition Management, Law Enforcement/Intelligence and Regulatory Compliance. Based in Arlington, VA just outside of Washington, DC; D&B's Government Solutions division has over 60 government-dedicated team members, who are physically located in nine states to provide nationwide coverage. The Government Solutions division is supported by the technology and information powerhouse that is the D&B Corporation. D&B is the premier provider of commercial business intelligence and Customer Data Integration (CDI) solutions.

PROCESSES: Global Data Collection aggregates data from hundreds of sources to provide superior breadth and depth of business information. Sources of information that may be pertinent to the Department include coverage of all U.S. courthouses for suit, lien and judgment information as well as Excluded Parties List System (EPLS), a web-based system that identifies parties excluded from receiving Federal contracts and subcontracts, and Federal financial and non-financial assistance and benefits.

DUNSRight™ is D&B's proprietary process for collecting and enhancing data. The foundation of DUNSRight™ is Quality Assurance which includes over 2,000 separate automated and manual checks. DUNSRight ™ encompasses five quality drivers that work sequentially to aggregate, standardize and enrich information.

Entity Matching is D&B's process that allows for and corrects variations in spelling (e.g. IBM vs. International Business machines), formats trade names and addresses, and associates data from disparate sources (e.g. a state business license, a Federal 10k filing, and a Yellow Pages listing) with the appropriate D&B record.

The key to the DUNSRight™ process is the D-U-N-S® Number - D&B's unique, nine-digit, location specific identifier, which D&B assigns as a means of identifying and tracking companies globally throughout their lifecycle. Once assigned, a D-U-N-S® Number is neither reused nor assigned to another business. Used by the world's most influential standards-setting organizations, the D-U-N-S® Number is recognized, recommended and/or required by more than 50 global industry and trade associations.

Finally, our Predictive indicators use statistical analysis to rate a business' past performance and to indicate how likely the business is to perform that same way (failure, fraud or financial distress) in the future. Predictive indicators leverages the analytical capabilities of experienced PhD's to build the underlying predictive models, with unique D&B data capabilities.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: D&B believes that Department can increase awareness, minimize and control fraudulent activity (internal and external) and reduce improper payments prior to adjudication through implementation of D&B's proven identification and authentication process.

D&B's products and services related to third-party business and consumer data give the Department unparalleled Provider and Recipient insight, and custom predictive analytics to make the best use of the third party data and toolsets to identify the riskiest and most suspicious targets of Medicaid fraud.

OUTREACH AND PROVIDER EDUCATION: D&B takes training and customer service very seriously. Every member of D&B's team is trained and evaluated on customer satisfaction and we have a corporate goal of world class customer satisfaction scores. The State and Local Government team is dedicated to delivering value to our customers by ensuring that they are able to take full advantage of our services by providing training.

D&B training can be provided on-site, via a web-ex or conference call. The method of training delivery depends upon the client needs and the product in question. We have a dedicated number for our government clients to ensure that your specific needs are met timely and accurately.

REQUIREMENTS AND STAFFING: Mandatory data elements required from the Department are: Internal ID, Business Name, Address, City, State, Zip and Telephone. DNBi is a secure, web based tool that is user specific, and is protected with unique ID's and Passwords for each user that is assigned by D&B or a Department Administrator. All user(s) will need is a web browser to access the DNBi system. D&B solutions can be in the form of data assets delivered to the Department that would be consumed and integrated with the database / analytical tool of Department's choosing. The Department would be required to build custom fields or tables to store/embed D&B data elements including, at a minimum, the D&B D-U-N-S® Number. IT resources would also be required to integrate data back into operating systems.

COST: D&B estimates (based on approximately 9,000 Organizational Providers) that the integration of a complete set of business insight solutions profiled in our response would require an annual investment of approximately $100,000 at the low end and $300,000 at the high end.

DETICA SOLUTIONS

EXPERIENCE: Detica is the global leader in providing advanced fraud detection technology; combining the latest in big data analytics with link and social network visualization to identify wasteful and abusive claims, providers, and recipients in both real-time and post-pay settings. Over the course of the last decade, Detica's NetReveal business unit has become a world leader in developing and implementing fraud detection and data analytics solutions, with a focus on predictive analytics and social network analysis.

PROCESSES: NetReveal identifies fraud by harnessing its proven propriety technology to ingest data from multiple sources and uncover hidden networks and relationships, otherwise undetectable in the raw data. NetReveal automatically joins and risk scores data from a wide range of sources, including, but not limited to, claims, managed care encounter data, provider registrations (in-state and NPPES) and exclusion lists, such as the Office of the Inspector General's (OIG) List of Excluded Individuals/Entities and State Exclusion and Sanction lists. In a pre-payment setting, NetReveal then incorporates these social networks and historical behavior profiles into real time predictive models that identify and suspend the riskiest and highest value claims for further investigation. NetReveal conducts all of the normally manual investigation steps automatically.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: NetReveal is used in the Commonwealth of Massachusetts' Executive Office of Health and Human Services (MassHealth) as its primary solution to combat Medicaid fraud, waste, and abuse through real time detection of improper payments. The NetReveal solution uses a combination of predictive modeling techniques and social network analysis (SNA) to identify potentially abusive or fraudulent claims before a payment is made.

Through automated processing, NetReveal integrates disparate data sources into social networks and historical profiles that are then used to automatically identify potentially abusive claims during claim processing or in a post-pay setting. NetReveal then routes these alerts for investigation via an intuitive alert management tool. NetReveal uses a range of analytics on transactions, providers and recipients, and their social networks to maximize hit rates and only alert transactions worth investigating.

OUTREACH AND PROVIDER EDUCATION: Detica will also take advantage of Colorado providers' clinical and technical expertise to configure an implementation that will best suit the needs of the Department. We will work with healthcare professionals prior to the go live date to validate our models so that our team of analysts understand common provider filing mistakes and ensure these errors do not trigger unnecessary investigation.

In cases where it is necessary to provide outreach, Detica will work with the Department to develop an effective educational program. Detica worked Her Majesty's Revenue and Customs (HMRC), the UK tax agency to develop appropriate outreach strategies to inform their constituents how to comply with standards.

REQUIREMENTS AND STAFFING: NetReveal can integrate with MMIS in a variety of ways, and the best way to suit the Department's specific requirements and operational context would be agreed during the analysis and design phase between Detica, the Department, and the Department's MMIS vendor. Detica will rely on the state to help establish user groups, queues, roles and permissions, configurable reports and screens beyond what is offered in the base product to ensure that the solution meets Colorado's needs.

NetReveal brings together all relevant data needed to make rapid and accurate decisions into one place. This dramatically increases the Department's existing fraud investigators' efficiency without a need for more staff. Department investigators will need a solid understanding of Medicaid claims processing and investigation as well as knowledge about providers, recipients, and regulations.

COSTS: Detica is pleased to provide information to the Colorado Department of Health Care Policy and Financing about our industry leading predictive analytics and Social Network Analysis solution with advanced alert management functionality. Our solutions are customized to each of our client's unique needs and as such no two implementations are alike. Due to the unique way in which we work with our customers, we are unable to provide specific pricing given the information contained within this RFI.

DYNAMIC RESEARCH CORPORATION (DRC)

EXPERIENCE: The Company's New England roots run deep. Founded in 1955 as an off-shoot of the Massachusetts Institute of Technology's Instrumentation Lab, now called Charles Stark Draper Laboratory, our engineering consulting work soon led to a contract with the U.S. Navy's ballistic missile program in 1958. This began DRC's relationship with the Navy that continues 50 years later at Navy locations throughout the U.S., including the Portsmouth Naval Shipyard, in Kittery.

DRC serves Department of Defense, Federal Civilian Agencies and State & Local government. We provide solutions and professional services in 5 areas: Information Technology, Training and Performance Support, Business Transformation, Management Services and Engineering and Science.

DRC has been providing services to the State of Colorado since 1997, when we began a project to design, develop and implement Colorado Trails, the Child Welfare case management system which is still being used today. DRC operates the IT infrastructure used to deliver applications such as CBMS, CHATS and Trails to all 64 of Colorado's counties. Over our tenure in Colorado have provided services as a valued partner to several state agencies and the Governor's Office of Information Technology.

PROCESSES: In 2013, DRC implemented the Predictive Modeling Initiative for the Executive Office of Health and Human Services (EOHHS).The Predictive Modeling Initiative analyzes Medicaid claims to detect improper claims prior to payment. This is accomplished through a Network Analytic and Modeling tool that is integrated with EOHHS' MMIS.

The Network Analytic portion of the tool combines provider records, member records and data from a number of external sources (e.g. Social Security Death Master, State Exclusion Lists, National Fraud Investigation Database) to develop 'social networks'. Attributes of providers and members, such as addresses, phone numbers, and names are used to develop 'social networks' that represent groups of individuals with relationships.

As Medicaid claims are processed, the social network of the member(s) and provider(s) involved are appended to the claim to augment the amount of information available for predictive models. The enhanced claims are then passed through an analytical engine that applies fraud models to the enhanced claim, looking for common patterns that would indicate fraud, waste and abuse.

DRC presents the Detica NetReveal® suite of products for predictive analytics. NetReveal® is a suite of generic products which are configured to detect particular types of fraud within an industry such as the Healthcare. Our solution in Massachusetts integrates BAE Systems' Detica NetReveal® Healthcare solution with the Commonwealth's MMIS in real time. The solution is designed to either mark the claim for normal payment processing, deny the claim with appropriate reason attached to the claim, or suspend the payment and refer the claim (alerts) for further investigation.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Detica NetReveal Alert Manager™ is an application which allows you to view, track, and process alerts raised by NetReveal Scenario Manager™. In the healthcare domain the alerts may represent one or more of the following activity:

> A claim post payment which has indicators of fraud, waste or abuse;
> A claim pre-payment which has indicators of fraud, waste or abuse;
> A fraudulent recipient or provider

OUTREACH/PROVIDER EDUCATION: DRC's approach to system implementation of any type is to involve as many parties as possible, including service providers who typically do not use the system. Incorporating a wide range of viewpoints into the design, development, and implementation phases helps build a foundation of trust and confidence; it also ensures that the needs of the entire community are reflected in the final application.

Colorado could also create a web-based, provider-focused set of web pages that allows providers to identify and suggest solutions to systemic issues within the Medicaid program. It would be a way to leverage the knowledge and experiences of the medical community in order to improve Medicaid claim submissions and therefore reduce waste and abuse.

In our Ohio Statewide Automated Child Welfare Information System (SACWIS) project, DRC held Partnership Forums to solicit input from the 88 county child welfare agencies as to the design and construction of the new system. The partnership included key stakeholders supported by DRC personnel. The Partnership formed, built, and maintained a change management framework and sponsored/championed a change management process. Colorado could use the same concept for Medicaid providers and the Medicaid agency.

REQUIREMENTS/STAFFING: Since the solution is highly scalable, to provide the effort and cost to integrate MMIS with our solution would require joint design sessions and be part of the project to establish the predictive modeling solution for fraud, waste and abuse detection.

Since the tool suite implemented for EOHHS is highly scalable, the alert thresholds are tuned in accordance with the agency's "risk appetite", i.e. their bandwidth of being able to review and disposition individual alerts at any given time based on the size and experience of their internal (or external contracted) investigative team.

COST: Since we have only provided services for pre-pay predictive analytics, the responses that follow pertain only to pre-pay services as provided to EOHHS. Furthermore, due to the requirements of the Massachusetts Information Technology Services master agreements, products and services must be bid separately. The EOHHS Predictive Modeling Initiative procurement was solicited and bid in total under the ITS43 services master agreement but the software licenses (including Oracle and NetReveal®) were procured directly and separately with the third party tool vendors under the ITS42 and ITS19 master services agreements.

EMDEON

EXPERIENCE: Specific to Program Integrity, Emdeon has key competitive advantages including our mastery level, professionalism, advanced technological approach, proprietary processes under continuous refinement, genuine sensitivity to clients' requirements, established credibility across the provider community, and extensive experience over the last 20 years delivering these important services to both the public and private sectors.

Emdeon prides itself on recruiting, training and managing mastery level audit professionals with the necessary credentials to perform these complex services. We have implemented vigorous pre-employment testing and a heavy qualification process to ensure only the most qualified and experienced auditors are hired. As mastery level coding and RN audit resources are in high demand and short supply, less than half the certified coders we evaluate for employment become qualified candidates for open positions.

As an EDI solutions vendor for more than 1,200 payers across the country today, Emdeon is uniquely positioned with the depth and breadth of data needed to bring a predictive analytic solution to the market today. While pre-payment and multi-payer predictive analytics are relatively new to the market, the foundation components of the solution, including the FICO predictive analytics, are in use today at large public and private sector payers -- including one of the largest state Medicaid programs, as well as one of the nation's largest Blue Cross Blue Shield plans -- producing substantial cost avoidance savings.

FICO IFM is currently used by seven commercial health care payers, by two state Medicaid programs, and by one Medicare Administrative Contractor. Additionally, IFM has been used in the past by other commercial payers and state Medicaid programs.

PROCESSES: Emdeon has teamed with FICO, the predictive analytics organization which serves as the backbone of the credit card fraud detection industry, to develop and deploy a solution unparalleled in the health care industry. This powerful solution uses a combination of patented profiling technology, predictive models, statistical analysis and rules to achieve a level of detection accuracy that is unmatched. As stated previously, the analytics models are seeded with close to one billion claims from Emdeon, enhancing the power of the data to learn and detect aberrancy. By pairing FICO's analytics models with Emdeon's proprietary analytics and claims data and experience, the team has created an unparalleled predictive analytics engine that is able to dig deeper into the data to find more potential savings.

The predictive modeling and risk scoring process enables the Department to employ commercial industry best practices for predictive analytics by harnessing the greater power of a substantially broader data set than would be possible when looking at the Departments' claims in isolation. The data samples used in developing the Emdeon solution included broad samples of data from across the health care spectrum with a reasonable and significant geographical spread. The Department would be able to leverage the knowledge and power of the combined data as samples are updated on a frequent and regular basis to ensure that emerging trends are identified.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Emdeon's Fraud Investigative Services combine retrospective claims analysis and prospective fraud detection techniques. We review and analyze historical claims data, medical records, suspect provider databases and high-risk identification lists while also conducting patient and provider interviews. With our audit and recovery services, we also provide both desk and onsite audit capabilities.

Emdeon's solution for improvement of waste, fraud and abuse detection, prevention and recovery for the Department consists of provider and criteria flags, predictive analytics that are based upon a powerful Emdeon data asset, and FICO's IFM software solution. Emdeon's industry-leading data processing and data warehousing capabilities integrate a database of proven provider and criteria flags that are used to screen claims prospectively.

OUTREACH/PROVIDER EDUCATION: Involvement of Colorado providers in the technical design will be limited with any COTS offering, therefore. However, Emdeon will work with the Department to involve Colorado-based knowledge as appropriate. As the solution is neural, the data learns based upon the inputs – this means that the tools and technologies described will continue to evolve, learning and applying detections to behavior and billing patterns specific to Colorado Medicaid.

Emdeon offers remote WebEx and video training for all of our solutions to assist our customers with any post-implementation training that may be necessary. Training videos and FAQs are posted to ON24/7 and can be downloaded to the user's desktop for frame-by-frame guidance. Emdeon provides quick reference guides and comprehensive user manuals, which are updated periodically and may be downloaded from the Emdeon web portal at any time.

Emdeon holds introductory and annual intrastate outreach meetings with consumer advocacy groups that represent the constituents most impacted by Medicaid.

REQUIREMENTS/STAFFING: Emdeon's Program Integrity Suite of solutions can be customized to integrate into the Departments' current strategies and system requirements. As a flexible and modular suite of solutions, offered in a SaaS model, it is adaptable to changing environments, eliminating the potential for waste and disposal in the face of a future MMIS acquisition. This means there is little, if any, need for the investment in software, hardware, or ongoing system maintenance by the Department.
In order to implement a pre-payment, prospective program integrity suite of solutions, claims would have to be sent to Emdeon for review prior to disbursement of funds to the providers.

The Department Staff and Expertise Needed:

Project Manager
Clinical Analyst
Integration Engineer

Additionally, virtually all of the support and maintenance will be provided by Emdeon after implementation. We will need a technical contact from the Department if there is a connectivity issue or data-related issues once the interface goes live. This contact will only be needed, if a support issue develops.

COST: Emdeon will provide detailed pricing requested during any future Request for Proposal. The pricing models would vary based on the services contracted by the State. Technology pricing is typically based on a volume-based license, with separate fees for implementation and any State-specific hardware requirements; this would include the creation and maintenance of any data bases and data source links. Fraud investigation services may be priced on a case or contingency basis, depending on the type and breadth of investigations performed for the State.

GRANT THORNTON

EXPERIENCE: Founded in Chicago in 1924, Grant Thornton is one of the largest accounting and management consulting organizations in the world. Grant Thornton LLP has nationally recognized expertise and thought leadership in reducing improper payments related to fraud, waste and abuse in Federal Government benefit programs. We have best-in-class investigative and forensic review and assessment expertise in every major industry, including healthcare claims reviews. Among our subject matter experts is James Huse, a former Inspector General of the Social Security Administration and former CEO of a progressive Program Integrity company. He is recognized as a national authority on government FWA mitigation and on identity fraud crimes and prevention. Mr. Huse develops unique program integrity solutions for Federal agencies, state agencies, and private sector entities, administering program benefits in social insurance, including healthcare. Mr. Huse led IntegriGuard LLC, a Medicare program safeguard contractor, as its principal officer, with approximately 200 multidiscipline employees in multistate locations.

To most optimally support the DHCPF's need for advanced analytics focused on fraud prevention and detection, Grant Thornton can utilize our partnership with Performant Financial Corporation (Performant), a firm that has the depth of subject matter understanding, enabling technology platforms, and unique experience in the deployment of advanced analytic technologies to address program integrity issues at their core.

As the CMS Recovery Audit Contractor (RAC) for Region A, Performant identifies and documents claims that have been improperly paid, reports to CMS, creates provider outreach campaigns, and determines trends that may result in investigations for FWA. Performant's proprietary data analytic technology, Insight Data System™ (Insight™) is deployed for advanced, big data analytics and rapidly sorts through large quantities of data, runs statistical models, and optimizes recovery.

PROCESSES: The EIS solution involves a three-prong technological approach delivered through Insight™ that is designed to (1) leverage a zero-footprint, browser-based hosted system that offers rapid startup, minimal impact on existing systems and operations, and faster access to data, (2) provide advanced data processing technology and comprehensive analytic services to mitigate fraud and recover payments from liable parties, and (3) address the needs of Colorado Medicaid with a holistic and scalable fraud solution.

Performant's proprietary technology platform, Insight™, performs analyses of claim services related to counter fraud efforts, including the detection and verification of suspected FWA. Insight™ rapidly sorts through large quantities of data, runs statistical models and optimizes recovery opportunities.

Insight™ will use proactive methodologies to uncover both subtle and complex patterns in Colorado Medicaid's data. In doing so, it will serve three critical functions:

- Act as a business intelligence environment that delivers data exploration and drill-down capabilities to EIS data analysts in an easy-to-understand browser interface

- Employ a wide range of detection techniques that go beyond traditional transaction level edits. It finds deviations, morphing behaviors, global billing patterns, clustering, fuzzy logic and networks—all with a focus on entities
- Provide effective response times, even when working with hundreds of terabytes of data from multiple sources

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: The application of EIS to address client goals and the items requested in the RFI is summarized in the following: Prioritize the identified transactions for additional review and prevent payments from being made based upon the likelihood of potential waste, fraud, or abuse. Discovering recipient attributes that indicate improper eligibility. Undertake and automate such analysis before payment is made to minimize disruptions to operations. Discover recipient attributes that indicate improper eligibility.

OUTREACH/PROVIDER EDUCATION: Performant has conducted outreach on two successive CMS Recovery Audit contracts (MSP Demonstration and Region A). This was done when Recovery Auditors were still a new concept to most providers, so the outreach process had to be developed with the objectives: (1) simplifying the Recovery Audit experience, (2) informing the audience and (3) minimizing unnecessary client and provider burden. Consistency in communication with the provider community is demonstrated through continuous outreach, timely and provider-focused customer service, and productive working relationships—all of which will be utilized for Colorado Medicaid to minimize the burden on providers.

Grant Thornton LLP has successfully supported clients by incorporating change management both formally and informally into its projects. Our Grant Thornton teams work with clients to help them reach their goals, minimize their risks and increase the likelihood of success. As such, we know well that managing the people side of change is a critical success factor. In addition, we work with our clients in a train-the-trainer capacity or a facilitative capacity to share knowledge and empower individuals to own the change and the capacity to manage it. Grant Thornton makes it our corporate policy to invest substantial resources into thought leadership, focusing on methods such as surveys and special projects done in conjunction with professional associations.

REQUIREMENTS/STAFFING: The type and number of staff assigned to the project will depend on scope, workload and volume thresholds determined through the scope of work and contract discussions.

Performant has extensive experience interfacing with various systems resident in state and federal governments as the system of record. Using Insight, Performant has experience loading direct extracts from the Fiscal Intermediary Shared System (FISS), Multi-Carrier System (MCS), National Claims History (NCH) system, and most other claims processing systems used in Medicare, Medicaid, and commercial healthcare operations. Performant's IT environment is tailored to (1) flex and scale to the high demands of Colorado Medicaid's program, and (2) meet specific Colorado Medicaid requirements and broader agency goals. Performant has the data capacity necessary to meet and perform requirements stated in the RFI.

COST: Pricing is highly dependent on the size and scope of the engagement; however, we recommend that CO Department of Health Policy and Finance consider the following key drivers in evaluating costs:

- Pre-payment medical review (supplemental review of medical records in the pre-payment timeframe)

- Post-payment recovery (although an effective pre-payment solution will identify many instances of FWA, no solution will identify every claim. This leaves cases that will need to be addressed on a post-payment basis)

- Staffing model (type of Agency staff leveraged [e.g., investigators] and type of staff required by contractor)

- Compensation model (e.g., fixed-fee, contingency, hybrid)

LEXISNEXIS

EXPERIENCE: For over 40 years, LexisNexis has been a trusted source and leading provider of decision-making information that help Human Services Agencies such as the Department. LexisNexis is the premier provider of decision-making intelligence solutions to businesses and government. Through numerous successful implementations, LexisNexis has developed significant expertise in providing identity-driven fraud detection and recovery solutions to Social Services Agencies, with solutions deployed in New York, California, Massachusetts, Texas, Georgia, Florida and across the United States.

New York State Department of Health (State Medicaid Agency): LexisNexis have been providing advanced data analytics software tools to support the State of New York's effort to combat fraud, waste and abuse in the State's $45 billion Medicaid program. The LexisNexis solution started with the build and successful deployment of a cloud-based database that contained every New York State Medicaid claim (almost ten terabytes of data).

Florida Department of Children and Family Services (DCF): Complying with both State and Federal rules and regulations for security and privacy of information, LexisNexis implemented one of our pre-payment fraud prevention tools that performs patented algorithmic analysis of identity data at the front-end. These tools detect fraudulent, incorrect and/or incomplete identity information in real time during the application process, significantly reducing the cost of fraud, waste and abuse, and streamlining the process to provide benefits to deserving Floridians.

PROCESSES: LexisNexis Provider Management Solutions provide the Department confidence Providers participating in Medicaid are eligible to do so, and constantly monitors for, and alerts to, any changes in Provider status.

Similar to Provider Management, LexisNexis offers comprehensive Member Management solutions for enrolling and monitoring Members (recipients). By pinpointing high risk recipients for items such as deceased, incarcerated, state of residence, unusual asset ownership, and many others, LexisNexis is able to identify recipients at high risk for causing fraud, waste and abuse both prior to payment and after enrollment.

LexisNexis Identity Management solutions provide the Department with the ability to electronically verify the identity of a recipient or provider that is both accurate and owned by the claimant, prior to enrollment in a program.

LexisNexis' Intelligent Investigator is a product capable of analysis of massive volumes of claim data, and presents investigative staff with well documented, easy-to-understand analytics.

SourceHOV's FRAUDExchange is the complete Program Integrity solution for managing every case, finding, correspondence, and recovery. The solution offers key dashboards to various users including managers, investigators, recovery personnel, etc. It automates document creation, tracking of all correspondence and manages any and all digital files, evidence or findings.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: LexisNexis' PrePayment Manager is an advanced fraud prevention system that engages prior to the disbursement of funds. PrePayment Manager acts as management's command center for avoiding the payment of potentially fraudulent claims, with full flexibility in flagging and reviewing incoming claims, testing new rules and analytics before they impact the claims system, and simple integration with existing MMIS systems. In addition, PrePayment Manager integrates with Intelligent Investigator for a Pre-to-Post payment feedback loop, informing the analytics and maximizing efficiency in both systems.

This holistic approach starts with a provider and recipient assessment that when combined with the data analytics findings help identify and prioritize investigative matters. The process includes a comprehensive link-analysis of providers, recipients, and operational characteristics.

Using our proprietary linking technology we uniquely identify each individual, and complete an evaluation for potential indications that the individual (beneficiary) may not be representing legitimate, eligible enrollments in Colorado Medicaid.

OUTREACH/PROVIDER EDUCATION: We have numerous partners in the field of healthcare educational outreach programs that contribute to our library of learning. This library may be included with the solution or simply utilize the Reach-Out platform for addressing issues as they arise. The Reach-Out platform has been utilized for not only education, but also employee/customer retention, address updates, and other data verification requirements by entities both externally (with their customers) and internally.

REQUIREMENTS/STAFFING: The proposed hosted COTS/Software as a Service (SaaS) solution would utilize two databases. The Department would not be responsible for the setup or operation of either of these databases. The first would hold the claims data for analysis and long term tracking. The second would be utilized to track all cases generated as a result of the claims analysis process. The integrated case tracking solution would log a copy those claims identified via analytics for audit and evidence chain of custody.

While the exact number of staff is dependent upon the programs' volume of claims, number of providers, number of beneficiaries, and the types of services covered, we can quickly demonstrate what the most cost effective number of staff should be in your office.

COST: LexisNexis Fraud, Waste and Abuse solutions are comprised of several pieces, for which we offer a mix of pricing options. Our goal is to keep the Department's costs as predictable and manageable over the life of the contract as is reasonable. Thus, several components may be structured on a fixed-price basis or may include variable charges for items such as percent of recoveries, or optional Performance-based incentive fees. As the Department continues to evaluate and refine the particular solutions and services that will meet your needs, we would like to further discuss ways that our solutions align with those business and budget needs.

The key driver of the price is the total population of providers and/or recipients to be processed by the system, as each access of the LexisNexis data store incurs a cost. In addition, the type of information accessed is also an important element.

HEALTH MANAGEMENT SYSTEMS, INC. (HMS)

EXPERIENCE: With more than 20 years of experience in performing cost containment and program integrity projects for Colorado, HMS understands both the policy that informs the Colorado Medicaid program as well as the underlying realities that an FWA solution would be brought in to address. HMS staff, which includes a former HCPF employee as the local Program Director, maintain a deep understanding of Colorado data, coverage and billing requirements, and payment method in addition to well-established data exchange capabilities.

Through many years of experience, HMS has emerged as the industry thought leader, sharing our best practices and innovations with clients across the nation. The following depicts our history of innovation:

- ► Consultations with U.S. Congress on provisions regarding the maximization of recoveries included in the Deficit Reduction Act.
- ► Full Deployment of COG/Manager, a real-time pharmacy cost avoidance solution.
- ► Launch of Health Kids Express, a CHIP outreach assistance program.
- ► Provide pre-payment FWA services for State clients.

PROCESSES: While other solutions focus primarily on outlier/anomaly detection, we consider several areas to ensure that we can significantly impact FWA for our clients. The solution HMS describes in the following pages translates key focus areas to the concerns Colorado raises in its RFI as the solution HMS can tailor for effective and practical FWA analysis. Our solution offers several FWA recommendations for consideration to supplement existing efforts, such as:

Automated pre-payment analysis
  Actionable results for claims, members, and providers that clearly indicate known fraud and abuse and potential financial risk for investigation or audits.
  Seamless integration within the claims process
  Near real-time results; ensuring on-demand reports are available as soon as data loads.
  Automatic Colorado regulatory compliance verification and review through the application of regulatory logic.
  Application of analytics to capture Colorado-specific FWA schemes
  Documentation of Colorado Medicaid regulations made available to key staff and stakeholders
  Low level of false positives. Our appeal rate for FWA findings is less than .5%.

Advanced analysis
  Provider Screening. HMS verifies and validates provider information against industry recognized external sources for third party validation.
  Geo-Spatial Analysis. HMS's geo-spatial analysis maps provider and recipient activities and can be used to identify geographic inconsistencies and aberrations in billing/claims data.
  Provider Anomalies. Providers engaging in aberrant and outlier behavior are flagged automatically through HMS's anomaly routines.

Provider Scoring. Providers' risk scores are created based on claim history, behavior patterns, and billing and coding history.

Predictive Modeling. HMS's efforts reflect those of CMS's Expedited Advanced Planning Document (ADP) mandates to qualify for 90% match

Ongoing development and modification of analytical tools to meet Colorado specifications, as required.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: HMS can apply clinical and operational expertise to any area of claims, provider, or recipient review. HMS offers recipient verifications and has partnered with leading industry vendors to deliver provider validation and screening services. HMS's SIU uses a variety of analytical tools, behavioral analysis, data mining, reporting, and claim analysis to identify and target recipients and providers for potential investigation**.**

OUTREACH/PROVIDER EDUCATION: As a program integrity vendor, HMS has a wide breadth of experience in supporting provider outreach and education initiatives. These initiatives vary in depth and scope in accordance with the core project and client goals.

Previous outreach efforts have included the following:

Provider Portal. On the online Portal, providers can access information regarding their claim data, thus supporting regular claims adjudication (deny, adjust) claims, medical record review, and recovery projects.

Webinars/in-person seminars. HMS has conducted live education sessions to support specific project initiatives, including educating providers on:
Compliance requirements
Proper billing procedures
Common coding/billing errors
Common FWA schemes

Focused education seminars. HMS can review provider peer/segmented group data to identify high-risk issues and conduct focused education seminars tailored to their billing behavior.

Claim-based outreach. HMS can support our claim and transaction-based logic with an accurate and supportable audit trail that can also facilitate education efforts. This claim-based logic can be conveyed through a return file or on-demand reports.

HMS will gladly provide specific references during the RFP procurement process.

REQUIREMENTS/STAFFING: As a SaaS model, HMS's solution does not need to directly integrate with the MMIS but rather operates in parallel to provide an independent, objective analysis of FWA activity. We work with data extracts and submit our findings via return files for integration into the MMIS, Decision Support System, or other databases as requested by our client.

Our recommendations can be seamlessly integrated as part of Colorado's claims process and work in conjunction with Colorado's Medicaid Management Information System solution.

Managing the Outcomes for our Behavioral Analytics, including predictive modeling and analytics tools requires one FTE, more FTEs can be employed if Colorado wants to be actively involved in FWA targeting. The number of Colorado resources that are needed for recipient verifications depends upon how IntegriMatch is implemented.

COST: HMS's cost structure and fees vary depending on the scope of services ultimately required based on the project's financial and program integrity goals. Based on Colorado's documented goals, an FWA project could be handled on a pre-payment or post-payment basis or a combination of both, and pricing would be adjusted accordingly. HMS has found that a Per Member per Month (PMPM) or fixed fee payment method is best employed for prospective analysis services since it promotes the application of all relevant compliance requirements regardless of financial impact. While HMS can provide both retrospective or prospective services, we recommend prospective services as it targets both low-dollar and high-dollar overpayments efficiently. SIU services are offered for an hourly fee, which ensures that any investigation identified and conducted is performed in an unbiased manner. Recipient verification fees are offered on a per case per year basis so that data matching and integrity checks can occur not just at application or redetermination points, but also periodically throughout the year. HMS would recommend allocating between $900,000 - $3 million annually for budget purposes based on the scope and services required of the final project, or $0.12 - $0.40 PMPM.

McKESSON

EXPERIENCE: McKesson Corporation is the nation's oldest and largest healthcare company. McKesson has been in continuous operations for 180 years (since 1833) and is headquartered at One Post Street, San Francisco, CA. McKesson Corporation ranks 14th on the Fortune 500 list and is publicly traded on the New York Stock Exchange under the stock symbol MCK.

McKesson is organized into two divisions: McKesson Technology Solutions and McKesson Distribution Solutions. McKesson Health Solutions, which is responding to this RFI, is part of the McKesson Technology Solutions division.

McKesson Health Solutions (MHS) delivers industry-leading clinical evidence and expert technology to help payers and providers collaborate for better healthcare outcomes at lower costs. While individual solutions meet key needs in a time of rapid industry change, the breadth of our portfolio allows healthcare organizations to combine our solutions in innovative ways to turn challenge into opportunity.

PROCESSES: Our network management and financial management tools help payers optimize business performance to operationalize today's complex volume-based and value-based payment models. Our FWA solutions are delivered by this business unit.

Our decision management solutions — including InterQual — help connect payers and providers to align decision-making, improve outcomes and reduce unnecessary utilization.

Our RelayHealth financial solutions streamline and optimize billing communication between providers, patients and payers to help optimize the revenue cycle management process.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: To meet the Department's advanced predictive modeling and analytics needs, we are proposing our InvestiClaim predictive analytics solution. Our complete InvestiClaim solution combines predictive analytics with the intelligent, proprietary pre-pay clinical rules and a full-service consultative approach to help identify both suspected and unknown billing aberrancies. The partnership of predictive analytics and pre-pay clinical editing rules helps you to identify and avoid a higher volume of wasteful and abusive claims up front and makes fraud recovery efforts more efficient on the backend. Once patterns of abuse have been identified through the analytics, editing rules can be created and deployed through the rules engine to support those policies pre-payment. You will be able to use the prospective analysis aspect of InvestiClaim to deny claim lines that are identified as exhibiting aberrant patterns before payment goes out the door.

McKesson does not offer fraud investigation services. McKesson is offering a commercial off-the-shelf (COTS) FWA software solution to the Department. InvestiClaim can process and score hundreds of claims per second in either pre-payment or post-payment mode.

OUTREACH/PROVIDER EDUCATION: McKesson does not offer educational or outreach programs to providers on issues relating to coverage, coding, industry best practices and medical record keeping.

REQUIREMENTS/STAFFING: Implementation and support services would be performed by experienced McKesson employees. Further scoping would be required to establish what InvestiClaim offerings would be appropriate for the Department and number of full time employees need to support the solution.

COST: Our COTS product licenses are offered on a term license basis. Without a specific set of requirements, McKesson is unable to provide a cost estimate. Many factors contribute to the cost of the solution such as the breadth of functionality to be deployed, number of covered lives, whether the solution is internally or externally hosted, and the division of ongoing operational responsibilities.

NORTHROP GRUMANN

EXPERIENCE: Northrop Grumman Corporation is a leading global security company that provides innovative systems, products and solutions to government and commercial customers worldwide. We are a nationally recognized tier-one systems integrator with $34 billion in annual revenues and a workforce of 75,000 persons.

Our substantial and successful experience in state and federal health and human services is demonstrated by our Health Information Technology (HIT) business unit's annual revenues in excess of $450 million. Northrop Grumman's HIT practice, which is part of our Federal and Defense Technology Division (FDTD), is vertically integrated to capitalize on our benefits management, interoperability, and public health experience across our customer base and to leverage the entire corporation's cyber security and other capabilities. Our health and human services (HHS) footprint extends into 12 states – providing mission-critical systems design, development, implementation, and support services critical to Medicaid eligibility, Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), Child Care, Child Welfare, and Child Support programs.

PROCESSES: Northrops' predictive models are run in parallel to generate alerts that are correlated into cases. Thus, the same claim line can contribute to the generation of several alerts. For example, claim lines that generate an "excessive procedures alert" are correlated into a case on the provider who submitted the claim, a case on the beneficiary, as well as a case on the location where the procedure was performed. The system provides a multidimensional perspective that links provider, beneficiary, and location. Geo-mapping techniques, coupled with charting features, further reveal the suspect relationships. Our proven modeling approach will enable Colorado to reduce the financial exposure associated with the current "pay and chase" methods significantly.

While the fundamental system has been operational for years, our FPS Team augments the solution with new capabilities to enable a more rapid implementation of models. These new capabilities will be integrated as part of a fraud prevention eco-system. The eco-system will support near real-time analysis and historical analysis on a common data platform to exploit new and unknown fraud patterns.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Northrop Grumman uses a variety of predictive modeling techniques and analytical tools to detect fraud, waste, and abuse. Our FPS for CMS runs numerous rules-based, anomaly-based, predictive models, and social network models to perform both pre-payment and post-payment claim analysis.

We also use a variety of statistical methods and techniques (e.g., decision trees, Bayesian models, linear discriminants, genetic algorithms, neural networks, and network analysis) that are directed at provider and recipient fraud. We use these techniques to develop Univariate Outlier Models, Multivariate Outlier Model, Text Mining, Predictive Model, and Social Network Analysis or Link Analysis Models.

OUTREACH/PROVIDER EDUCATION: There are many information sources available to the provider community when it comes to learning about preventing fraud, waste, and abuse. Entities such as the Department of Justice, the Department of Health and Human Services, the Office of the Inspector General, and CMS provide guidance to providers. These sources provide information applicable to the entities that they interact with frequently, namely, payers, other providers and vendors. Furthermore, readily available information about applicable Federal and State laws, such as the False Claims Act, the Anti-Kickback Statute, the Physician Self-Referral Law and the Social Security Act, will go a long way in educating the Colorado provider communities.

We propose an actively maintained portal with links to all other relevant information produced by State and Federal entities. This one-stop-shop for all relevant information can be integrated with social media capabilities to encourage provider collaboration and the exchange of ideas and can be a venue to conduct e-learning programs. Beyond the portal, the above-mentioned provider associations will be instrumental in active outreach.

REQUIREMENTS/STAFFING: Because Northrop Grumman uses a modern, big data management platform, time and effort to integrate data from Colorado's MMIS is much less than with traditional database management tools. We can more easily consume data and ensure that data accuracy and reliability is not compromised during the analysis processes. In addition, we will establish processes to check that the agreed-upon transaction timeframes are being met and that reference data is complete and compliant to those timeframes.
Our solution has an existing data management capabilities based on an open source, big data management platform that Northrop Grumman uses in civil, intelligence, and defense sectors to protect our Nation from the threats. The data management platform runs on an array of low-cost commodity hardware that can either be hosted in Colorado data center, a Northrop Grumman data center, or a third party data center. The hardware can be sized based on the Department's requirements relative to the billions of transactions managed by system in full-scale production at CMS.
Northrop Grumman or State personnel can administer the data management platform and, based on our experience, the cost to maintain the platform is much lower than the cost of maintaining traditional relational database technologies, such as Oracle, DB2, and database appliances such as Teradata, Greenplum, or Netizza.

COST: Because all information provided under this RFI is subject to the Colorado Open Records Act, Northrop Grumman is not providing cost estimates as requested. As pricing information is considered proprietary, its visibility to our competitors could compromise our competitive position on any follow-on bid.

OPERA SOLUTIONS

EXPERIENCE: Opera Solutions was founded in 2004 with a notion that the world's flow of information, just then starting to intensify, was going to be the oil of the 21st century. Today, Big Data has exploded and Opera employs 660+ people, with offices in New York, Boston, San Diego, London, New Delhi, and Shanghai. We have amassed the largest community of scientists in the private sector and have been atop the leader board of the global Netflix Prize and the Heritage Health Prize both, which measured machine learning capabilities.

PROCESSES: Opera Solutions offers a leading medical fraud solution, which consists of three key components namely: fraud detection algorithms, case management software and the Vektor technology stack. The Opera Medical Fraud Solution uses highly advanced analytic techniques to maximize the accurate detection of high or fraudulent charges while minimizing false positives. Leveraging world-class expertise in machine learning and pattern recognition. Opera Solutions has developed an analytic solution that uses historical patient billing data to more effectively identify high or fraudulent charges.

For inpatients, Opera Solutions applies linear and non-linear Dimension Reduction Methods to characterize the distribution of billed amounts associated with each Diagnosis Related Group (DRG). Using advanced analytics, the models reconstruct the invoice and compare it to the actual bill to identify outlier behavior. For outpatients, the solution employs an Ensemble scoring methodology that combines multiple models. Each has a unique ability to address a particular aspect of the problem. This allows the solution to capture the complicated structure of procedure and diagnosis codes at the visit level and maximize performance in predicting outliers.

The algorithms include pattern detection, anomaly detection, supervised predictive modeling, and network analysis with interactive visualization. Instead of basic rule based approaches, our algorithm toolset is built around patent pending claims outlier detection solution, which includes a set of machine learning and pattern recognition algorithms to automatically capture the complex relationship among diagnosis, procedures, and patient profile in claims data.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: The current revenue integrity system is used both in pre-payment as well as post payment. The impact in pre-payment scenario is much higher as it allows end user to make changes not only on higher value charges but also for low value anomalies. Post payment scenario allows analysts to look back at historical claims and make changes to high value charges if they were not attended to in pre-payment scenario. This dual approach ensures that no anomalous claim slips through the system.

Opera FWA products provide a comprehensive and intensive FWA solution, targeting abnormal billing patterns across claims, recipients, and providers.

OUTREACH/PROVIDER EDUCATION: Opera will work closely with Colorado providers during the implementation phase to understand the current process and to be able to incorporate well with their existing system. Opera solution believes in a 2 way approach that not only provides capability to identify fraud and abuse but allow the end user to provide feedback that can be incorporated back into the system to improve the prediction capabilities. Our system will

continuously work with providers to supply them with constant education to improve their systems and utilize industry best practices to minimize any waste occurring in the system.

REQUIREMENTS/STAFFING: Leveraging our Vektor™ Platform, based on Open Standards (SOAP and REST Web services for SOA access and JDBC connectors for SQL databases), and designed to be able to plug in a variety of different database and middleware technologies, Opera, working with DHCPF team will be in a position to identify appropriate interfaces and integrate with the MMIS without any impacts to the existing processing times.

The requirement for the number of full time employees in fraud investigation unit will largely depend on several factors such as claims volume; score threshold; and analyst productivity.

COST: Opera Solutions recommends a two phased approach that consists of a Diagnostic Phase and an Implementation Phase.

The Diagnostic Phase is typically completed within 8-12 weeks and consists of gathering information and assessing the available data to confirm model development and deployment options. We prefer to price the Diagnostic Phase as a Time & Materials effort to cover our personnel &travel costs. A planning number of $300,000 is typically the cost of such an engagement.

The Implementation Phase is typically completed within 6-12 months and consists of determining the model(s) to be built, implementing the Vektor platform, developing the models using Opera Solutions algorithms and methodologies, and building case manager software. The overall cost is incurred under the following headings: Software license fee, customization and implementation fees, application hosting related costs and expenses, business consultation services, fraud investigation services, maintenance.

OPTUM

EXPERIENCE: Optum Government Solutions, Inc., and our affiliated Optum-branded companies, collectively referred to as Optum throughout our response, is a health services company dedicated to making the health system work better for everyone. With a combined Optum-wide workforce of more than 30,000 people, we deliver integrated, intelligent solutions that work to modernize the health system, improve overall population health and build and enable sustainable health care communities.

Optum serves the entire health ecosystem, including nearly 250,000 health professionals and physician practices; nearly 6,000 hospitals and facilities; more than 300 state and federal government agencies; 300 insurance companies and health plans. Optum has more than 20 years of experience with Medicaid, and our large national footprint in the market includes millions of Medicaid fee-for-service (FFS) and managed care lives.

For state Medicaid agencies, Optum provides cost containment solutions as a valued subcontractor to every major Medicaid Management Information System (MMIS) Fiscal Agent in the market today, including:
    Hewlett Packard Enterprise Services (HPES) and its former entity EDS
    CNSI
    Molina Medicaid Solutions
    Noridian Administrative Services
    Xerox (and its former entity ACS)

We are also the country's largest provider of cost containment solutions for the majority of lives covered by Managed Care Organizations (MCOs), representing almost 70 percent of the nation's Medicaid enrollees receiving benefits through MCOs. We work with the largest plans, including:
    Anthem/WellPoint
    Blue Cross/Blue Shield
    Gateway Health Plan
    Keystone Mercy Health Plan
    United Healthcare's Community & State Plans

PROCESSES: Fraud and Abuse Detection System (FADS) is a Medicaid Integrated Technical Architecture (MITA) aligned solution that features a suite of complementary tools designed to help identify and manage fraud and abuse investigations from detection through collection. FADS provides users the ability to research aberrant behaviors with a minimum of false positives. As a result, investigative staff can confidently pursue suspicious activity on the part of both providers and members without wasting time on non-productive investigations.

As one of a state's fraud detection tools, the Surveillance Utilization Research System (SURS) function should be one of the pivotal pieces of any Medicaid system because it supports the investigation of potential fraud, abuse, or misuse of the Medicaid program by providers or members. Unfortunately, SURS has typically been an underutilized tool by most states, due mostly to its complexity, extensive learning curve, long turnaround time for results, and difficulty of use (batch or batch-like mode which translate to infrequent runs).

The FADS' SURS component addresses this problem by providing investigative staff with an easy to use tool to analyze historical data and develop profiles of health care delivery and service utilization patterns. Optum's SURS enables users to build their own studies and queries without technical help, on-demand from their desktops, with results available online within hours. The FADS' SURS provides a full complement of reports that will be needed by investigators: ranking reports, provider and member profiles, frequency distributions, statistical summaries, and drill-down reports to supporting claims. Drill-down capability is embedded in these reports, allowing users to navigate from a summary total in a profile to the underlying claim detail with the simple click of a mouse. This powerful functionality speeds the analysis efforts and greatly increases the productivity of investigative staff.

To separate the true signals of improper billing from the other patterns inherent in Medicaid data, models need to be constructed around that data rather than designed for another industry (e.g., marketing or financial services) and moved into a health and human services setting. Thus the Optum Prepayment Review Solution (OPRS) makes extensive use of retrospective claims analysis to customize and train predictive models and analytics designed for Medicaid programs. This customization and training process can be part of or supported through a data warehouse such as the Department's proposed BIDM.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Optum has provided pre-payment analytics and review services for health care fraud and abuse, provider screening, and payment system vulnerability analysis for over a decade and for a variety of payers, including Medicaid managed care organizations, and commercial insurers. We have also provided post-payment recovery services to State Medicaid programs, Medicaid managed care organizations and commercial insurers for many years. Our experience with pre-payment predictive modeling is unsurpassed because of our work with over 65 commercial and Medicaid payers for whom we calculate numeric risk scores on over 1,000,000 claims daily on the likelihood of fraud, waste or abuse.

Our newest component of FADS is High Cost Members. The study can generate a list of those recipients who have high costs but no corresponding diagnoses in their past claims history (typically three years) that match any in the list as defined by the user. In other words, their claim history shows no serious illness or injury, yet their costs are high, thus indicative of high claim volume for smaller amounts or less serious diagnoses. Its purpose is to reveal to the user those members whose diagnoses do not seem to warrant the high costs paid for claims on their behalf. This could potentially indicate IDs that have been Stolen or sold by the member, friends, family, or others.

Optum has years of experience working with all of the major MMIS vendors (including Xerox, the Department's current MMIS vendor) in program integrity operations. This experience allowed Optum to design an interface that can be rapidly implemented to receive claims from an MMIS in near real time and return review recommendations and decisions to the MMIS for continued processing of claims. This interface rapidly returns an "allow", "pend", or "deny" recommendation to the MMIS based on analytical results for all scored pre-payment claims, along with analytics reason codes and other processing information as required by the Department.

OUTREACH/PROVIDER EDUCATION: It has been our experience that the vast majority of providers support properly designed and implemented fraud, waste and abuse programs. By working closely with the Colorado provider community and soliciting feedback and input from the members, Optum and the Department will make certain that the program operates successfully and as intended.

Optum will work collaboratively with the Department and Colorado providers to tailor an outreach and education program best designed to benefit affected stakeholders. Technology will allow us to reach out to the Colorado provider community in an efficient and effective manner to address the broad scope of policies and procedures.

REQUIREMENTS/STAFFING: OPRS can use a dedicated database or leverage data from the Department's proposed BIDM to support OPRS functions and to incorporate a variety of external datasets that will be used by predictive models and analytics to improve fraud and abuse detection. If a dedicated database is used, Optum would build and maintain this database.

OPRS will integrate seamlessly into the existing Medicaid MMIS claims processing system with minimal effort, time, and cost and with no disruption in the regulatory processing of claims. OPRS will interface with the MMIS through a series of data feeds. Data feeds that the Optum solution would require from the MMIS include: Paid Claims History, Newly Finalized Claims, Recipient Data, Provider Data, Reference Data, Post-Adjudicated, Pre-Paid Claims, Claims Outcome Information.

COST: Given the general nature and purpose of the RFI to seek to determine to what extent products exist in the marketplace, lack of final Department decision making of the requirements that will ultimately be incorporated into the BIDM, uncertainty whether the optional prepayment and EVV solutions will ultimately be incorporated into the 2013 MMIS RFP award, and an inability for RFI respondents to mark sections as proprietary and confidential, Optum is unable to provide specific pricing detail for items a and e in RFI Response 10 at this time.

PALANTIR

EXPERIENCE: Palantir Technologies was founded in 2004 by a handful of PayPal alumni and Stanford University computer scientists. Our headquarters are in downtown Palo Alto, California, with offices around the globe. Our company is dedicated to providing next-generation software in support of critical missions.

Palantir's software represents the intersection of data, technology, and human expertise. Our platform sits above traditional data systems, enabling people to ask the questions they need answered in a language they understand. Palantir is based on the simple idea that the human mind is the most effective tool to identify patterns in information, while computers are the most effective tool to manage enormous amounts of data. As a platform company, we ship open, extensible, scalable software platforms that can be deployed immediately against the entire class of problems facing an organization in any industry.

We designed Palantir from the ground up to enable real-time analysis and collaboration across teams and organizations while enforcing restrictions that protect privacy and civil liberties. Since its inception, Palantir has invested its intellectual and financial capital in engineering technology that can be used to solve the world's hardest problems while simultaneously protecting individual liberty. Robust privacy and civil liberties protections are essential to building public confidence in the management of data and are an essential part of any information system that uses Palantir software.

PROCESSES: Palantir has been successfully deployed against threats ranging from Medicaid fraud to contracting fraud to financial fraud. Based on these experiences, we have learned that algorithms alone do not provide the best means of detecting the patterns, trends, and anomalies that lie hidden in massive data sets. We have developed an approach to human-computer symbiosis that combines the computational power of machines with the best of human reasoning and creativity, enabling computer-assisted, human-driven analysis of data at massive scale. Palantir is designed to reduce the friction between our software and its users, optimizing the performance of both.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Palantir Gotham is a fully featured, highly configurable commercial-off-the-shelf (COTS) solution for Medicaid program integrity. Palantir's fraud detection approach starts by migrating all available data into a unified environment for search, discovery, and analysis. From this environment, users can access a private virtual sandbox where they can discover and explore connections between any person, provider, place, or event in their enterprise data stores. Whether that data is claims, claimant profiles, e-mails, or fraud hotline tips, Palantir reaches across all the data sources within an enterprise for any information that exists in an analyst's environment. With Palantir, the Department can implement a complete and extensible solution with predictable costs on a reliable, proven timeline.

OUTREACH/PROVIDER EDUCATION: We fully sustain software deployments with extensive training and technical support. We provide ongoing, one-on-one training for a wide range of skill levels. Our support team is available for on-demand troubleshooting of user, administrator, or system issues.

As a product-oriented company, however, Palantir does not conduct education and outreach programs. We would be happy to partner with a company or organization that specializes in that area to achieve the Department's goals.

REQUIREMENTS/STAFFING: Palantir Gotham fulfills the Department's needs for automated compatibility and integration with MMIS. Palantir can interoperate with the Department's third-party systems, applications, and data sources through Palantir's open APIs. This will allow the Department to leverage previous investments and continue to use systems with unique functionalities or capabilities that they do not wish to deprecate.

Integration with MMIS would be included in our total Fixed Firm Price. Since we do not charge for services, Palantir would undertake the integration work and ensure interoperability during installation. Once the deployment is stood up, this interoperability is automated, enabling a consistent, unified system. In addition, because Palantir Gotham is open and extensible, the Department does not risk being locked into a proprietary platform or losing access to any of its data. Palantir allows data owners to retain control over their data and creates analysis and reports in non-proprietary formats.

As a scalable platform, Palantir Gotham is can be used by teams ranging from 20 to 2,000 members. Our platform produces cutting-edge fraud detection by combining human expertise with computing power and visualization capabilities. We can adapt Palantir Gotham to maximally achieve the Department's fraud detection goals with the resources available to it.

COST: Palantir Gotham is licensed based on the number of "server cores" required to run the platform. This places no hard limit on the number of users or the quantity of data. Instead, it accounts for both factors as increased user and data scale requires more processing power. The specific number of cores required for this deployment will depend on the scale of the project, including the types of data sources involved, the amount of data to be integrated, and the quantity of concurrent users that will access the platform.

We offer two pricing options for Palantir Gotham: (1) monthly licensing per core for a Palantir Cloud, or (2) perpetual licensing per core. In addition to the perpetual core licenses, we charge 20% of the original core purchase price for Operations and Maintenance (O&M) each year after the initial year of procurement. The perpetual license model supports organizations with fixed requirements (e.g., situations where the user and data scales are known up front), while the monthly Cloud licensing model allows organizations to easily scale their Palantir deployments as their data and user needs fluctuate. Both pricing options are based on Palantir Gotham's standard MSRP pricing. Discounts are provided at scale.

Both pricing options include installation and data integration assistance, system configuration, and guidance in data modeling. We also provide training for analysts, administrators, and

developers as needed at no additional cost, including embedded support by cleared staff if necessary. Both options also include 24x7 access to our expert support team, the online support portal, and the online developer zone at no additional cost. Finally, both pricing options provide continuing support including deployment of patches and major product upgrades as they become available every few months.

SAS

EXPERIENCE: Headquartered in Cary, North Carolina, SAS is the largest privately held software company in the world with record 2012 revenue of $2.87 billion. We have been in the business for 37 years and our longevity is a testament to our superior software and customer service. Our mission is to deliver superior software and services that give people the power to make the right decisions.

SAS is an industry leader (recognized by industry analysts as a key market player) in the entire fraud prevention field, spending nearly three quarters of a billion dollars annually in research and development. The continued introduction of advanced analytical techniques, such as link analysis (also known as social network analysis), into the SAS Fraud Framework is further confirmation of SAS' commitment to leadership in the fraud space. Additionally, SAS has created a global Fraud and Financial Crimes Practice, with domain expertise specifically in health care fraud.

As the leader in business analytics, SAS helps organizations understand their business drivers and create answers to complex problems. SAS eliminates the complexity of sharing data and applications across the organization. SAS goes beyond other vendors' narrow definitions of business intelligence, offering business analytics—data management and predictive analytic capabilities that tell an organization not just where it has been, but where it should go next. SAS business analytics deliver the foresight and understanding that is required to meet and exceed goals. Predictive modeling and analytics are the backbone of SAS, going back to the first product released more than 3 decades ago. We hold more than 35% of the analytics marketplace, more than the next nine vendors combined, which held less than 24% of the market in 2011.

SAS serves more than 65,000 government, university, and business sites in 135 countries. SAS solutions are used extensively by all 50 state governments, all 15 federal departments and approximately eighty-five percent (85%) of federal sub-agencies and quasi-governmental affiliates.

PROCESSES: Because the solution helps to manage the entire fraud discovery and investigation workflow, pertinent information flows seamlessly throughout the process, and the outcome of each and every investigation is fed back into the detection engine to fine tune the analytics over time. The solution includes SAS Social Network Analysis to detect and visualize both top-down and bottom-up hidden and risky fraud rings and collusive networks to ensure they are visible to investigators.

With SAS, you can standardize, integrate and authenticate the data and consolidate program integrity activities. By harnessing your qualitative and quantitative data, you can better identify fraudulent activity and reduce improper payments going out the door by identifying risks within claimants and providers sooner.

The SAS Fraud Framework consists of a series of components that support the end-to-end detection and investigation process including: data Integration for creating a holistic view of entities; alert generation process for flagging suspect activities; alert management for

investigation/dispensation of alerts; case management (optional) for managing program integrity audits and investigations; learn and improve cycle for storing alert results as known outcomes.

The SAS Fraud Framework for Government can extract relevant data from different systems, external data sources, unstructured text and other disparate data sources, as well as import business rules for known fraud, waste and abuse schemes from existing rules engines.

Detection and alert generation components enable the systematic detection of suspicious activity using a fraud scoring engine that employs a combination of analytic techniques to determine the likelihood of the presence of fraudulent activity. The detection and alert components: score transactions in real time with an online scoring engine that lets you detect fraudulent activity using a combination of business rules, anomaly detection and advanced analytical techniques; calculate the propensity for fraud as billings are received and re-score transactions at each stage of the process as new data is captured.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Identifying potentially ineligible participants and taking action to remove them or prevent them from entering the State's program can avoid costs associated with both maintaining and providing services to ineligible recipients. SAS utilizes an analytically driven approach to risk score each enrollee as to the likelihood that they are actually ineligible. SAS solution automatically aggregate and profile data across multiple dimensions such as beneficiary, households, providers, provider networks, geographic areas, program service areas, etc., and utilize advanced link and social network analysis techniques to uncover potentially suspect relationships between and among participants to detect possible collusive networks and potential fraud rings, duplicate services or other suspicious associations.

OUTREACH/PROVIDER EDUCATION: As a technology company, we have partnered with customers and third-party vendors to achieve a wide range of compliance solutions to prevent not only fraud, but abuse and error. However, we do not develop education and outreach programs in-house.

REQUIREMENTS/STAFFING: Whether implemented on-site in Colorado, or through SAS hosting services, the SAS Fraud Framework does not require development of a new database. The solution leverages but does not provide proprietary databases. Based on past projects, we've seen that a solution can be very successful utilizing no more than the data that already exists within Colorado's Medicaid system on recipients, providers and billings.

The SAS Fraud Framework and its alert queue easily integrates with MMIS systems given our data integration/data quality capabilities. Our solution does not impact the performance of the MMIS. The effort, time and cost would be dependent on the level of integration. In addition, the data points discussed in RFI Response 10 would need to be addressed to provide more information on effort, time and cost.

By dialing in alerts to an amount that can be managed and ensuring that those with the worst severity are addressed first, great success can be achieved in program integrity by focusing on

areas with the highest ROI for each FTE. This applies whether our solution is only utilized in a post-payment implementation, or applied pre-payment as well.

COST: We welcome the opportunity to meet with the State to gain additional insight prior to providing a specific estimate. Colorado will need to make some specific decisions, as well as provide additional data points, including:

> ➢ Implementation for providers, claimants or both
> ➢ Only post-payment, or pre-payment as well
> ➢ Number and types of data sources to be integrated and modeled against
> ➢ Number of providers and volume of billings
> ➢ Approximate total volume of data (in TB)
> ➢ Number of expected users
> ➢ Hosted or non-hosted solution

As mentioned earlier in the RFI, we do not provide direct fraud investigation services, and additional resources from the Department are not necessarily required.

Despite all of these unknowns, an estimated cost range for our solution within Medicaid in Colorado is between $1.5 million and $5 million. The lower end of that cost range would represent only licensing and implementing modeling and scoring for either providers or recipients, and only post-payment. The higher end represents a full implementation for pre- and post-payment detection methods and streams for both recipients and providers.

TERADATA

EXPERIENCE: Teradata Corporation is the world's largest company focused on analytic data solutions through integrated data warehousing, big data analytics, and business applications. Teradata was founded in 1979 and is corporately headquartered in Dayton, Ohio, with additional major U.S. offices in Atlanta, Georgia; Rancho Bernardo (San Diego), California; Indianapolis, Indiana; and Raleigh, North Carolina. Teradata employs more than 10,250 professionals in almost 70 countries worldwide who are dedicated to analytical solutions.

Teradata has led the data warehousing market since its inception, with around 1,500 customers and more than 2,840 implementations, including:
- All of the top ten global telecommunications companies
- All of the top five global airlines
- Nine of the top ten global commercial and savings banks
- Eight of the top ten transportation and logistics companies
- Eight of the top ten global retailers

PROCESSES: Teradata® Database Software is regarded by customers and industry analysts as a superior choice for analyzing data and processing increasing volumes and complexity of queries without compromising performance. Teradata's processing architecture, combined with our database software provides the foundation for our unique ability to support and manage a wide range of data warehousing functions. These functions range from reports to ad-hoc queries to data mining and simultaneous data loading, all from a single data warehouse that integrates data from across the enterprise to drive business insight for the best decisions possible. Our Teradata Database software delivers real-time intelligence for our customers with capabilities such as support for mixed workloads, the ability to handle thousands of concurrent queries, robust and simplified system management, high system availability, event monitoring, and easy integration into the enterprise.

The Teradata Workload-Specific Platform Family offers our customers options that take full advantage of all the power of Teradata systems anywhere in the enterprise – as an active data warehouse, enterprise data warehouse, entry-level data warehouse appliance, special-purpose data mart or sandbox environment. Our platform family ranges from symmetrical multi-processing (SMP) to massively parallel processing (MPP), and is recognized for high performance, scalability, and easy supportability. Teradata platforms are known for the processing speed, the amount of data that can be queried and the number and complexity of queries that can be run. Teradata platforms are designed to protect our customers' technology investments, providing significant 'green' – environmentally friendly – advantages.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: For predictive analytics, the Teradata team will utilize the Teradata Health & Human Services LDM (H&HS-LDM) to jump-start the project. The H&HS-LDM extends the underlying tenants of the Medicaid IT Architecture and Teradata Healthcare Framework. It supports an unlimited number and depth of hierarchies and relationships to reflect a complete view of an individual with the programs, services, providers, claims, agreements, financials, clinical encounters, and contracts that support them.

The H&HS-LDM takes critical information, from every event and concept from account numbers and patient information to medical services and medical risk scores, and creates a common understanding of each claim. By mapping the Department's core requirements to its data, the H&HS-LDM delivers complete data visibility to identify risk drivers and ensure that vital information is used to preempt wasteful transactions.

OUTREACH/PROVIDER EDUCATION: Teradata partners with numerous software and solution providers to ensure our clients' needs are satisfied. These partnerships may take the form of in-house development efforts to enhance software capabilities, like those with SAS, Revolution Analytics, Fuzzy Logix, and Hortonworks. We also work with industry partners, like Thomson Healthcare, State Street, and Siemens, to develop readily transferrable solutions that satisfy recurring themes for industry players. Finally, we serve the public sector as both a prime and as a subcontractor on a variety of local, state, and federal contract vehicles.

Besides the analytical assets at the Department and within Teradata's Advanced Analytics Center of Excellence, we identified two companies, Health Integrity and Cahaba Safeguard Administrators, which have subject matter expertise in the field of healthcare waste and auditing. Health Integrity, LLC, is ISO-certified and provides a range of healthcare-focused services, such as predictive modeling, data mining, data analytics, compliance auditing, reimbursement policy analysis, and fraud detection and investigation. Furthermore, Health Integrity is building a Fraud Prevention System at CMS that helps identify and stop payment on suspicious fee-for-service Medicare claims until they can be sufficiently validated.

Cahaba Safeguard Administrators is a service company that uses analytics to enhance clinical reviews, audits, and investigations. Cahaba also works with CMS and is a Zone 3 Program Integrity Contractor for investigations, law enforcement referrals, data analytics, and medical review.

REQUIREMENTS/STAFFING: The H&HS-LDM is easily extendable by design, allowing you to add functionality without re-architecting. Nothing in this model is tied or linked to physical database design. It is purely a logical model and therefore requires physicalization. It is completely independent of database software and hardware.
When the fraud system identifies a possible fraudulent transaction the system generates an exception and delivers the exception to a fraud investigation group for disposition via a programmatic workflow.   The analyst will use case management tools to collect the exception and exception data. (e.g. descriptive data regarding the suspected fraudulent transaction.) The analyst may also bring historical data into the case management system including prior exceptions for the same customer and the outcome, data for related parties, external data – public records, location data, bureau data and more.

COST: Unfortunately, Teradata cannot provide level-of-effort or cost itemization without understanding more about the Department's current system hardware, analytical environments, and data requirements. However, we offer a low-cost Proof-of-Concept Workshop in which Teradata's industry-leading consultants spend a day at your worksite to better understand the Department's needs.

TRUVEN

EXPERIENCE: We have extensive domain knowledge of fraud, waste, abuse, and overpayment detection and investigation business processes. Throughout our history, we have had a special focus on program integrity and analytics that control healthcare fraud, waste, and abuse within state Medicaid systems, the federal government, and health plans.

Our products and services have assisted Medicaid agencies and the federal government in identifying tens of millions of dollars in healthcare fraud, waste, and abuse. Experiences in the government sector have provided us a robust framework that is used by commercial plans and managed care organizations to stop abusive billing practices.

We currently provide payment integrity support to 24 states directly and indirectly to 14 more states through our Federal-level contracts. Truven Health has been a leader in Medicaid program integrity analytics since the 1980s when we delivered our first Surveillance and Utilization Review (SUR) system. We have been a federal Medicaid Integrity Contractor (MIC) since the inception of the program in 2006 and a federal Medicare Zone Program Integrity sub-contractor for analytics since the program was authorized in 1996.

PROCESSESS: Due to the complexity of detecting and eliminating healthcare fraud, waste, abuse, and overpayment, a multi-faceted approach is required. This approach must combine multiple data systems, methodologies, areas of expertise, processes, education techniques, program design approaches, and policy improvements. In tune with these needs, Truven Health has developed a solution suite that incorporates the key components required to support a comprehensive fraud, waste, abuse, and overpayment prevention program. First, we work with you to review specific areas of focus and define a tailored payment integrity strategy that best addresses your organizations' individual needs. Then, we collaboratively identify the level of solutions and services needed to achieve your desired results. This may result in a comprehensive set of payment integrity tools and services, or it may consist of a targeted strategy to fill existing program gaps.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: Our solution addresses the following key areas: Prepay and Prevention, Provider Surveillance and Compliance, Advanced Predictive Models and Algorithms, Case Management, and Investigative Services.

Our deliverable can include a vulnerability assessment that is specific to your unique payment policies, to identify opportunities for savings in your existing systems. We can also work with you to review and make recommendations for payment policy clarifications and changes. In every single assessment we perform, we find significant opportunity for additional savings. The Truven Health algorithms and predictive models are not only comprehensive and current; they also have embedded clinical intelligence and flexibility for tailoring to specific plan characteristics. Each algorithm contains the rules, clinical constructs, and statistical processes required by topic.

All of Truven Health prepay and post-pay models output is geared to highlight those providers and recipients who present the highest risk and to maximize investigative ROI. As such, all the

reports, graphs, maps, and other output of our analytic tools identify the worst offenders first, allowing clients to deploy their resources to address the most serious cases and recover the most overpayments.

OUTREACH/PROVIDER EDUCATION: Truven Health believes strongly in bringing together subject matter experts who can address current issues in fraud, waste, and abuse, and who can speak to issues specific to our client's stakeholders. As such, we would work closely with Colorado staff to identify key stakeholders and hold conversations with these stakeholders, many of whom are likely providers, to identify their concerns and propose solutions to address those concerns.

Truven Health believes that strong communication with providers is key to reduction of fraud, waste, and abuse. As such, we build secure access portals for providers to obtain information about their claims, to receive alerts about their practices and behaviors that may be problematic, and to obtain general information about federal and state changes that may affect them. Additionally, Truven Health utilizes mailings and regular publications to educate providers on program changes, as well as issues that impact their profession. We conduct outreach activities by holding seminars and training individually at their site, or collectively presenting to groups of providers in coordination with provider associations and organizations.

REQUIREMENTS/STAFFING: The proposed solution in our RFI response is designed for flexibility of integration, which means it can be placed anywhere in the State's claims stream, and is not technically bound by existing workflow constraints. It is designed to easily scale in terms of processing volumes, addition of new agencies and claim types and identification of new fraud and abuse trends. Our recommended approach is so flexible, that should the State wish to, we can easily accommodate with our existing infrastructure any position.

COST: Truven Health is mindful of client budgets and resources, and as such, prices our solutions in a way that ensures all clients have a positive ROI in comparison to cost. Truven Health will price its recommended solutions for Colorado when submitting its proposal in response to your RFP.

VERIZON

EXPERIENCE: Our Team of Verizon, Verizon/Terremark and Healthcare Resolution Services, Inc. (HCRS) includes deep and broad expertise across the entire spectrum of Medicaid and Medicare regulatory and program integrity requirements, medical review, data mining, data management, and technology enablement.

Our Team provides a complete solution for comprehensive fraud detection, including near real-time data analysis, a repository for business intelligence and data mining, predictive modeling, risk scoring, case management and dashboards. These systems have been deployed and improved for more than 20 years and are used both internally and externally by our customers. They in fact are "Made in Colorado," with our engineering team based in Colorado Springs and our fraud operations center in Highlands Ranch.

PROCESSES: The solution is designed to provide high-volume predictive modeling capabilities in near real time to manage and prevent fraud and improper payments, integrate seamlessly with the Department's existing systems and deliver a full cross-program solution to monitor program performance and support policy initiatives. Our multi-layered solution can support both pre-payment and post-payment fraud detection capabilities.

Key strengths and features of the system include: High performance data reduction architecture with steps for data normalization; configurable predictive modeling tools that support linear pattern recognition and non-linear patterns; proven fraud model that are designed and tested to look for indicators such as high frequency utilization behaviors, geographic dispersion of participants and identification of aberrant practice patterns.

PREPAY/POSTPAY, PROVIDER/RECIPIENT INFO: The solution can process healthcare claims, provider and recipient transaction data in near real-time and applies domain-specific, predictive models, configurable edit rules, artificial intelligence algorithms and risk scores to identify inappropriate patterns and outliers.

OUTREACH/PROVIDER EDUCATION: Under the Department's guidance and leadership, the Verizon team will seek clinical and technical expertise from Colorado providers in the design and implementation of the tools and methodologies for fraud detection. In particular, HCRS has broad experience in working with providers during claims review audits while also providing research-driven advice aimed at prevention of incorrect payments based on the ongoing analysis of trends observed in the claims data.

REQUIREMENTS/STAFFING: Our solution can be seamlessly integrated with the Department's MMIS system and other systems with minimal impact to processing times. The time and effort required to integrate the Verizon solution depends on the complexity and number of interfaces required.   Pre-payment complex medical audits require no additional resources than those required for traditional post-payment audits – the procedure is identical. The team has conducted these audits for the Medicare CERT program and has accomplished them within the time limits required by statute, regulation and program policy.

COST: Verizon's solution and supporting optional services deliver a rapid return on investment to customers through the identification of fraud, waste and abuse opportunities and optimization of operational activities to manage prevention. Verizon is able to offer the Department multiple options for the implementation of its solution and would work with the Department to provide the best value and approach based on the following services:

Managed Service Model – costs are bundled together in a predictable monthly recurring fee Price by Component – provides transparency on cost details Professional Services Hourly Rates – customer determines need for services
Custom – based on individual customer requirements.