Introduction

Fraud, waste, and abuse cost government agencies and taxpayers staggering amounts of money each year. All agencies remain susceptible to people who routinely falsify financial records and payroll information, file benefit claims for money they are not eligible to receive, or engage in other scams.

Healthcare is a prime target due in large part to the fact that every business day, Medicare processes about 4.5 million claims from 1.5 million providers.\(^1\)

In fiscal year 2013 alone, the Medicaid program covered about 71.7 million individuals at a cost of $431.1 billion. Disturbingly, the Centers for Medicare and Medicaid (CMS) estimated that $14.4 billion (5.8 percent) were improper payments.\(^2\)

Feds are trying hard to plug the numerous holes in the healthcare dam. The Obama administration announced on June 25, 2014 that a new anti-fraud program in Medicare doubled the amount of improper payments it identified or prevented this year.\(^3\) The Fraud Prevention System at CMS recovered or prevented more than $210 million of improper payments in its second year, the agency told Congress in a report.\(^4\) The program, which uses predictive analytics to study billing patterns, also prompted CMS to take action against 938 providers and Medicare suppliers.\(^5\) The administration said its efforts have led to a record $19.2 billion in fraud recoveries over five years.\(^6\)

Undoubtedly, fraud, waste, and abuse are widespread, but not all agencies are equipped with the technology to root out these pervasive problems.

The old guard of companies relies on static solutions and remains unable to make changes in real time to analytics software, or help agencies sift through multiple sets of structured and unstructured data to search for anomalies.

Agencies on the cutting edge of prevention and detection are taking advantage of technology that provides deep analytics to sift through terabytes of data hundreds of times faster than they used to, and with greater accuracy than ever before. That technology is being developed by companies that are armed with teams of data scientists.

The landscape changes constantly, so agencies must do all they can to stay ahead of fraud.

PREVENTION

Agencies must focus on prevention if they hope to curb fraud, waste, and abuse. Once the bad guys walk away with money they aren’t supposed to receive, it is incredibly hard – and expensive – to reclaim the funds.

Identity verification and authentication are cornerstone technologies for preventing fraud in any scenario where a government agency pays a monetary benefit to citizens or tries to collect money owed.
IDENTITY VERIFICATION

The migration of services to the Internet reduces costs, provides convenient self-service options for citizens, and helps agencies work more efficiently. Unfortunately, it also makes the public sector vulnerable to cyber attacks of increasing sophistication.

EMC identity verification provides strong authentication and fraud prevention services that validate user identities in real time, reducing the risk associated with identity impersonation. Utilizing knowledge-based authentication (KBA), identity verification challenges users with a series of top-of-mind questions generated from information within databases that contain billions of public and commercially available records. EMC's solution confirms identities within seconds without requiring an organization to have a prior relationship with the user. Identity verification allows government agencies to reduce operational costs and fraud losses, increase efficiency and revenue, meet regulatory standards, and enhance the overall user experience.

ADAPTIVE AUTHENTICATION

Adaptive authentication is a multi-factor authentication and risk management platform that monitors and authenticates user activities based on risk level and organizational policy. EMC's solution is powered by risk-based authentication (RBA) technology that conducts a risk assessment of users behind the scenes. By weighing more than 100 risk indicators, EMC's adaptive authentication technology assigns a risk score to each activity, and users are challenged when an activity is identified as suspicious or violates an organizational policy.

Transparent authentication enables organizations to increase security without compromising user convenience. When an activity is identified as high risk, the user must respond to a secondary form of visible step-up authentication such as a challenge question, out-of-band phone call, or KBA question generated by the identity verification service. Adaptive authentication also enables site-to-user authentication, which assures users that they are transacting with a legitimate website by displaying a personal security image and caption that has been preselected by a user at login.

ENTERPRISE CONTENT MANAGEMENT

EMC's enterprise content management solutions for integrated benefits eligibility help agencies transform a maze of service-specific paper forms, office visits, and interviews with a single, integrated, Web-based "front door" that enables citizens to apply for multiple services at once. Such an approach also provides agencies with a unified electronic view of each client – detailing their needs and situation across program boundaries. This enables agency staff to ensure that applicants receive all the benefits for which they are eligible, while typical abuse scenarios – such as multiple claims from one address – are automatically flagged for investigation. Agencies must have the ability to know immediately whether an individual's claim for benefits is valid.

These applications allow agencies to apply elements of a financial services "straight-through processing" model to case work in programs such as Medicaid, Temporary Assistance for Needy Families (TANF), the Statewide Automated Child Welfare Information System (SACWIS), and the Supplemental Nutritional Assistance Program (SNAP). An electronic case file manages all case-related information, such as identity verification, proof-of-income, and expense documents, which validates a recipient's eligibility for programs. Electronic case files eliminate paper and aggregate any type of content relevant to a case – not just documents, but audio and video files, images, and discussion threads. To minimize identity theft, EMC technology limits the exposure of personal and financial information, while controlling and tracking who has access to information.
DETECTION

One of the most critical lines of defense in curtailing fraud, waste, and abuse is detection. It is vital that agencies use all available data and technologies to identify fraud when it occurs. With fraud, plan A is prevention; but agencies must have a strong plan B – detection.

DATA ANALYTICS

When data volumes reach “Big Data” proportions, parsing it for meaningful information requires very powerful data analytics. Traditional data warehousing and analytics are time consuming and expensive. In addition, they provide only a “rear view mirror.” Detecting fraud quickly requires real-time analysis of many structured and unstructured data sources.

The EMC solution is a purpose-built, open systems data appliance that architecturally integrates database, server, and storage into a single, easy-to-implement system that is deployable and expandable in days – not weeks or months. The appliance integration and pre-tuning ensures predictable performance, while dramatically simplifying the data warehouse and analytics infrastructure, resulting in reduced administration overhead.

The solution has a massively parallel processing (MPP) architecture, designed for the business intelligence (BI) and analytical processing that fraud detection requires. The EMC solution moves data processing dramatically closer to the data and its users. Computational resources process every query in a fully parallel manner, use all storage connections simultaneously, and flow data efficiently between resources as the query plan dictates. This allows a wide variety of complex processing to be pushed down in close proximity to the data for maximum processing efficiency and incredible expressiveness. The solution delivers:

- Fast query execution, unmatched data loading, and linear scalability
- A single platform for data warehousing, data marts, text mining, and statistical computing
- Greater insight and value from data with advanced analytics and unified data access

FRAUD DETECTION

EMC’s fraud detection solutions provide 24/7 monitoring and detection, real-time alerts and reporting, forensics and countermeasures, and site blocking and shutdown. They also prevent phishing, pharming, and Trojan attacks that occur in the online channel. Hundreds of organizations use EMC fraud solutions to protect their customers against the latest online threats.

EMC’s Anti-Fraud Command Center (AFCC) is central to these efforts. An experienced team of fraud analysts deploy countermeasures, conduct extensive forensic work to stop online criminals and prevent future attacks, and work to shut down fraudulent sites. The Command Center has established direct communication with dozens of Internet Service Providers (ISPs) globally and provides multilingual support in nearly 200 languages that improve the ability to detect, block, and shut down sites anywhere in the world. To date, the Command Center has shut down more than 500,000 cyber attacks in 185 countries and has worked with more than 13,000 hosting entities.

BUSINESS ACTIVITY MONITORING

For most private and public sector organizations, the evidence is in the data they produce and collect in various business processes. The EMC platform delivers real-time visibility into agency business processes. It enables organizations to actively track key performance indicators and automatically generate alerts and actions for conditions that fall outside established limits.

Through dynamic, intuitive, and configurable Web 2.0 dashboards, the platform’s reporting capabilities supply critical insight into performance issues such as service level agreement enforcement, resource utilization, and cycle time. They can also alert agency officials to other out-of-pattern activity. For example, in a benefits claim environment, process activity monitoring could flag the number of reopened or continued claims from

EMC® AT WORK

The Fraud and Compliance Group within the Washington State Department of Labor and Industries needed to analyze multiple data sets as it worked to improve the detection of fraud in its workers’ compensation program.

Fraud investigators built a centralized data mart that collected data from multiple departments and databases. To analyze these large data sets in new ways, the group deployed fraud analysis software that:

- Identified unusual claims activity
- Screened for known and unknown patterns
- Detected fraud via predictive models and associative link patterns

Prior to system deployment, investigators uncovered true fraud in only 50 percent of their investigations. Centralizing data resources pushed that figure from 50 percent to 60 percent, with a recovery average of $8,000 per audit. Detection rose to 73 percent with the deployment of fraud detection software and fraud audits now recover more than $10,000 per investigation.

With just under $5 million invested so far, the organization expects to identify more than $8.3 million more in premium audits each year. This centralized fraud detection system is projected to achieve a positive Return on Investment (ROI) in less than two years.
the same telephone number or address when they rise above a certain threshold. This, in turn, can initiate a case to investigate and pursue potential fraud. For more in-depth analytics, agencies can integrate EMC’s solution with business intelligence tools such as SAS, IBM Cognos, and SAP Business Objects.

**INTELLIGENT ENTERPRISE CAPTURE**

No matter how sophisticated an agency’s data analytics capability, it’s of no use with information trapped in paper. Converting paper documents to a digital format (digitizing) is the essential first step that enables agencies to cope with large volumes of paper while improving every subsequent step in the fraud detection processes that includes formerly paper-based information.

EMC’s solution enables agencies to capture anything from anywhere. Intelligent enterprise capture gives agencies the ability to centralize mailroom operations, while distributed capture supports departments within large agencies as well as networks of regional offices. The solution also allows ad hoc scanning from desktops, regardless of location, and the use of mobile devices to capture data while in the field. Additionally, the technology gives agencies the ability to connect document information to business systems. Capturing anything from anywhere sets the stage for an agency to use its documents and information more effectively to support all activities. Using a services-oriented architecture, EMC’s solution can make data available to process monitoring tools as well as the massive data marts that serve large-scale data analytics applications.

Agencies have the ability to leverage mission-critical scalability and availability. EMC’s solution scales to meet high-volume operations that need to process millions of pages per day and provide on-demand availability. The same level of performance also applies to data extraction. The faster data can be extracted, the faster it can be accessed by the systems and applications that need it.

**GOVERNANCE, RISK, AND COMPLIANCE**

Governance, risk, and compliance (GRC) refers to an organization’s approach to managing these three areas. It describes how agencies can:

- Define appropriate objectives, policies, and procedures
- Pursue opportunities while avoiding or managing negative events
- Demonstrate adherence to laws, regulations, policies, contractual obligations, and industry standards

Organizations have practiced GRC in a piecemeal fashion for decades. But in a global environment of economic stress, heightened regulation, and increasingly complex risks, a GRC strategy must be holistically applied to manage risk and compliance across lines of business and agency functions.

A vendor-neutral GRC solution serves as a point of consolidation for GRC information of any type. The platform allows seamless integration of data systems without the need for additional software. It can automate the movement of data in and out of the platform to support data analysis, process management, and reporting.

The right solutions allow agencies to build an efficient, collaborative enterprise GRC (eGRC) program across the IT, operations, legal, and finance domains. It should provide several key government solutions – compliance, remediation, continuous monitoring, and continuity of operations (COOP) – as well as several out-of-the-box solutions that deploy quickly. These solutions manage risks, demonstrate compliance, automate business processes, remediate issues, contextualize data, and deliver visibility into organizational risk and security controls. Agencies must be able to easily tailor solutions and integrate them with multiple data sources through code-free configuration.
HOLISTIC MANAGEMENT
EMC solutions unify policies and controls as well as the assessment of risks and deficiencies. They enable government agencies to demonstrate compliance with laws, regulations, and policies, while ensuring that multiple roles and business units use common processes and information. Agencies have the ability to:

- Achieve business continuity
- Track and automate remediation through plans of action and milestones (POA&M)
- Support continuous monitoring with automated data collection, risk scoring, and advanced presentation and communication dashboards
- See the status of exceptions and issues and hold the appropriate personnel accountable for fixing them

STREAMLINED PROCESSES
With EMC eGRC solutions, agencies can move toward a streamlined, coordinated, and consistent program that increases automation and efficiency – while decreasing reliance on cumbersome processes and inefficient spreadsheets. This enables agencies to:

- Decrease the cost of preparing for and conducting regulatory audits
- Accelerate compliance with new regulations
- Focus attention on high-priority risks and addresses them quickly
- Reduce operational costs through the consolidation of processes, information, and systems
- Increase awareness of policies, objectives, and responsibilities among staff and third parties

REDEFINE POSSIBILITIES: THE IMPACT OF FRAUD, WASTE, AND ABUSE
Because government agencies at all levels provide so many services to citizens and aggregate so much information, the potential for fraud, waste, and abuse in government remains enormous.

Money lost to fraud, waste, and abuse represents opportunities unrealized, programs unfunded, jobs not created, and people denied much-needed services.

In an era of tight budgets, agencies do not have the resources to invest in personnel to detect and prevent fraudulent activity. But agencies are not powerless. Technology solutions are available to quickly and efficiently provide thorough analysis of records, claims, tax returns, and other documents in real-time to detect illegal activity and spot trends that may signal fraud.

Analytics give agencies the ability to sift through terabytes of data faster than ever, not just to detect and prevent fraud, waste, and abuse, but also to improve customer service and strengthen transparency and compliance efforts. Investing in these solutions provides a substantial ROI, while tackling one of the most prevalent problems plaguing agencies and taxpayers nationwide.

ABOUT EMC
EMC is a global leader in enabling government agencies to redefine their operations and deliver IT-as-a-Service. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect, and analyze their most valuable asset – information – in a more agile, trusted, and cost-efficient way.

CONTACT US
866.438.3622 (Press 1 for Sales) Or 508.346.8510 (Direct to sales)
www.emc.com

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark or trademark of VMware, Inc., in the United States and other jurisdictions. © Copyright 2013 EMC Corporation. All rights reserved. Published in the USA. 11/14. Solution Overview  H13614

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.