REDUCING FRAUD, WASTE, AND ABUSE IN GOVERNMENT

EMC delivers core technologies to address fraud, waste, and abuse
Fraud, waste, and abuse cost governments and taxpayers billions of dollars annually while eroding public trust. Fraudsters—individuals and organizations—falsify financial records and payroll information, file benefit claims under fictitious names, and misuse official positions for personal gain. A Gartner report on U.S. healthcare reform states that “of the more than $2 trillion spent annually in the U.S. on healthcare, the National Healthcare Anti-Fraud Association (NHCAA) estimates that about three percent, or $60 billion, is lost to fraud, thereby driving up the costs of healthcare, insurance premiums and taxes for all Americans.” The unemployment insurance and tax collection systems are also riddled with waste, fraudulent schemes, and abusive practices.

Systems that can prevent, identify, and curtail fraud, waste, and abuse are beginning to gain importance on the list of government spending priorities. For example in September 2011, the US Department of Labor awarded $191 million to 40 states, the District of Columbia, and Puerto Rico to modernize unemployment insurance systems. The funding is intended to "reduce UI improper payment rates; provide an opportunity for modernizing UI tax and benefits systems; and enable the design of technology-based tools to prevent, detect, and recover improper UI payments." Similarly, the U.S. Department of Health and Human Services 2012 budget includes a request of $581 million in discretionary funding to expand prevention focused, data-driven initiatives to improve Centers for Medicare and Medicaid program integrity. This request also supports the expansion of up to 20 Strike Force cities to target Medicare fraud in high-risk areas with the goal of cutting the Medicare fee-for-service (FFS) error rate in half by 2012.

There is no one solution that can always prevent or detect fraud, waste, and abuse. But EMC delivers core technologies that can play a major role in designing solutions to address these problems in three key areas: prevention (i), detection (ii), and governance, risk, and compliance (GRC) (iii).

PREVENTION

In 2010, the U.S. government recovered a record $4 billion from health care fraud cases. As impressive as that number is, what it doesn’t tell us is the cost of that recovery—in dollars, person-hours, and other resources. Though not as headline friendly, it’s much more efficient to prevent fraud than to “pay, chase, and recover.”

Among the many instances of fraud, waste, and abuse that plague government entities two stand out: tax evasion and improper payments. These examples are instructive because they point out vulnerabilities from the payment assessment and collection and payment issuing perspectives.
According to an IRS estimate the 2001 tax gap—the difference between taxes owed and taxes paid—amounted to $345 billion. A more recent study conducted in 2008 pegged the gap in the range of $450-$500 billion. At approximately $2 trillion, unreported income was 18-19 percent of total reportable income.

On the payments side, the unemployment insurance system has been hit hard by improper payments. Driven by a faltering economy, jobless claims have risen dramatically and with them overpayments. For the 12 months ending in June 2010, benefits overpayments accounted for more than 10 percent of jobless benefits—a record $16.5B of $156B in benefits. By March 2011, that rate had increased to 11.6 percent.

Unemployment insurance overpayments stem from a variety of causes. Some benefits recipients continue to receive payments after they’ve regained employment, others file fraudulent claims by misrepresenting their identities. Likewise, individuals should not receive unemployment benefits while receiving disability benefits.

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

It is now common for citizens to use online portals to apply for many types of social services benefits. Likewise, government agencies use the web to exchange sensitive information. The migration of services to the Internet increases efficiency and reduces costs, provides convenient self-service options for citizens, and helps agencies work more efficiently. Yet, this migration also makes the public sector vulnerable to cyber attacks of increasing sophistication.

RSA® Identity Verification is a strong authentication and fraud prevention service that validates 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. With industry-leading speed and accuracy, RSA Identity Verification conveniently confirms identities within seconds, without requiring an organization to have a prior relationship with the user. By using RSA Identity Verification, government agencies can reduce operational costs and fraud losses, increase efficiency and revenue, meet regulatory standards, and enhance the overall user experience.

ADAPTIVE AUTHENTICATION

RSA Adaptive Authentication is a multi-factor authentication and risk management platform that monitors and authenticates user activities based on risk level and organizational policy. Used by over 8,000 organizations and protecting over 250 million users, Adaptive Authentication is powered by risk-based authentication (RBA) technology that conducts a risk assessment of users behind the scenes. By weighing over one hundred risk indicators, Adaptive Authentication assigns a risk score to each activity, and users are only challenged when an activity is identified as suspicious or violates an organizational policy.

This transparent authentication enables organizations to increase security without compromising user convenience. When an activity is identified as high risk, the user is challenged with a secondary form of visible step-up authentication such as a challenge question, out-of-band phone call, or knowledge-based authentication question generated by the RSA 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.
INTEGRATED BENEFITS ELIGIBILITY MANAGEMENT

Today, government agencies that directly serve citizens operate in a harsh spotlight. Whatever the mission, they’re expected to perform it faster and better—regardless of budget constraints. This is especially true in social services. Over the past decade, demand on U.S. programs that provide food stamps, housing, jobs, and medical care has steadily increased. In 2008, for example, nearly 10 million people lived in subsidized housing, a jump of 13 percent from 2000.11 With passage of the Affordable Care Act, 20 to 30 million new applicants will be knocking on the doors of social services agencies by 2014.

As demand soars and resources to meet that demand recede, the potential for fraud, waste, and abuse across benefits programs has increased. Social services agencies are scrambling to make service delivery less prone to fraud while increasing efficiency and lowering costs. Yet these efforts are hindered in an IT environment of siloed information systems that impede data sharing and analytics as well as cross-program auditing.

Powered by the industry’s most comprehensive and configurable information infrastructure, EMC® solutions for integrated benefits eligibility management 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 agency staff 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.

Just such a system is being deployed by the Los Angeles County Department of Public Social Services (DPSS), which provides benefits and services to low-income county residents. The system, developed with Unisys, employs EMC Documentum® xCelerated Composition Platform (xCP) technology to manage eligibility determination across five programs:

• Temporary financial assistance and employment services
• Free and low-cost health care insurance
• Food benefits for families and individuals
• In-home services for elderly and disabled individuals
• Financial assistance and advocacy for federal disability benefits

Documentum xCP enables the capture, management, and archiving of critical information and processes. Using pre-built templates and components, Documentum xCP also provides a rich solutions infrastructure, optimized to deliver dynamic, case-based applications that can address the specific requirements of social service delivery—through configuration not customization.

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 the inefficiencies of 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, Documentum xCP also limits the exposure of personal and financial information, while controlling and tracking who has access to information.

DETECTION

As sited above, one of government’s biggest fraud challenges resides in healthcare. Medicare and Medicaid are rife with fraud from service providers and individual claimants. Conservative estimates place Medicare-Medicaid fraud at 6 to 10 percent of payments.12 In a state like Minnesota for example, which made $9 billion in Medicaid payments in 2010, that’s $900 million.13
As computer forensics and data mining specialist Eckhardt Kriel notes, “Fraud is based on deception—you are not supposed to find it. Deception is what distinguishes fraud from error.”"\textsuperscript{14} With fraud, plan A is prevention; but a strong plan B—detection—is clearly necessary.

As Kriel goes on to explain, when fraud occurs there is always evidence.\textsuperscript{15} The questions, of course, are where and how can it be found? These are the keys to fraud detection, in healthcare or any other government funded activity.

**RSA FRAUDACTION**

An outsourced, managed service, RSA FraudAction\textsuperscript{\textregistered} enables government organizations to quickly deploy a solution while minimizing resource investment. RSA FraudAction offers 24x7 monitoring and detection, realtime alerts and reporting, forensics and countermeasures, and site blocking and shutdown. In addition, FraudAction prevents phishing, pharming, and Trojan attacks that occur in the online channel. Today, more than 300 organizations have selected FraudAction to protect their customers against the latest online threats.

At the core of FraudAction is the RSA Anti-Fraud Command Center (AFCC). Its 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 AFCC has established direct communication with dozens of ISPs around the world and provides multilingual support in nearly 200 languages that enhance its ability to detect, block, and shut down sites anywhere in the world. To date, the Anti-Fraud 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 or public sector organizations, the evidence is in the data they produce and collect in various business processes. Through its Business Activity Monitor (BAM), the Documentum xCP 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 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 fraudsters. For more in depth analytics, BAM can also be integrated with business intelligence tools such as SAS, IBM Cognos, and SAP Business Objects.

**LEVERAGING BIG DATA TO BOOST DETECTION**

When data volumes reach “big data” proportions—data sets of 20 terabytes and above—parsing it for meaningful information requires very powerful data analytics. Yet traditional data warehousing and analytics are time consuming and expensive. In addition, they provide only a “rear view mirror.” To detect fraud quickly, organizations need realtime analysis of many data sources, structured and unstructured.

The EMC Greenplum\textsuperscript{\textregistered} Data Computing Appliance (DCA) 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.

At the heart of the Greenplum DCA is the EMC Greenplum Database\textsuperscript{\textregistered}, with a shared-nothing, massively parallel processing (MPP) architecture that has been designed for the business
intelligence (BI) and analytical processing that fraud detection requires. The Greenplum Database 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 Greenplum DCA 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

**MAXIMIZE GREENPLUM DCA BENEFITS WITH EMC GLOBAL SERVICES**

For the complex data analysis required to detect fraud, waste, and abuse, EMC Global Services provides a full range of planning, design, and implementation services for EMC Greenplum hardware and software. After implementation, EMC’s data migration services can safely migrate your critical data to your new system. EMC can also integrate the Greenplum DCA into existing infrastructure and analytics applications such as SAS, MicroStrategy, Business Objects, and Tableau. Our extensive data warehousing and BI deployment best practices accelerate business results without straining resources.

**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.16

As EMC Captiva® defines it, intelligent enterprise capture enables organizations to:

1. **Capture anything from anywhere**

EMC Captiva intelligent enterprise capture includes centralized mailroom operations, distributed capture that supports departments within large agencies as well networks of regional offices, ad hoc scanning from desktops regardless of location, and capture in the field using mobile devices.

2. **Connect document information to business systems**

Capturing anything from anywhere sets the stage for an agency to use its documents and its information more effectively to support all of its activities. Using a services-oriented architecture, Captiva intelligent enterprise capture can make data available to process monitoring tools as well as the massive data marts that serve large-scale data analytics applications.

3. **Leverage mission-critical scalability and availability**

Captiva intelligent enterprise capture 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 or 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 been practicing 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.

The vendor-neutral RSA Archer eGRC Platform serves as a point of consolidation for governance, risk, and compliance 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 into and out of the platform to support data analysis, process management, and reporting.

RSA Archer government solutions allow organizations to build an efficient, collaborative enterprise governance, risk, and compliance (eGRC) program across the IT, operations, legal, and finance domains. RSA Archer provides 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 can manage risks, demonstrate compliance, automate business processes, remediate issues, contextualize data, and deliver visibility into organizational risk and security controls. Because solutions are built on the RSA Archer eGRC Platform, individual agencies and organizations can easily tailor solutions and integrate them with multiple data sources through code-free configuration.

HOLISTIC MANAGEMENT
The RSA Archer eGRC Platform unifies policies and controls and the assessment of risks and deficiencies. The platform enables government agencies to:

- Demonstrate compliance with laws, regulations, and policies
- Ensure that multiple roles and business units use common processes and information
- 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

With RSA Archer, the enterprise can move toward a streamlined, coordinated, and consistent eGRC program that:

- Increases automation and efficiency and decreases reliance on cumbersome processes and inefficient spreadsheets
- Decreases the cost of preparing for and conducting regulatory audits
- Accelerates compliance with new regulations
- Focuses attention on high-priority risks and addresses them quickly
- Reduces operational costs through the consolidation of processes, information, and systems
- Increases awareness of policies, objectives, and responsibilities among staff and third parties

THE IMPACT OF FRAUD, WASTE, AND ABUSE—OPPORTUNITIES LOST
Because government agencies at all levels provide so many services to citizens, aggregate so much potentially valuable information, and constantly interact with each other and various private sector organizations, the potential for fraud, waste, and abuse in government is enormous. The dollars at stake—dollars that could be put to productive use—are staggering.

In the process of describing technologies that can prevent or detect fraudulent activity and manage its risk, this EMC Perspective has offered some high profile examples of fraud and abuse in the areas of healthcare, unemployment insurance, and taxation. However, these examples barely hint at the scope of the problem. Government procurement, especially in the military, international money laundering, and counter terrorism initiatives present ample opportunities for fraud—and this by no means completes the list.
Money lost to fraud, waste, and abuse represent opportunities unrealized—programs unfunded, jobs not created, and people denied much needed services. EMC would like to help.

ABOUT EMC
EMC Corporation is a global leader in enabling government agencies to transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, delivered in partnership with leading Government Contractors and System Integrators, EMC accelerates the journey to cloud computing, helping government IT departments to store, manage, protect, and analyze their most valuable asset—information—in a more agile, trusted, and cost-efficient way.

7. Ibid.
8. Ibid.
10. Ibid.
15. Ibid, p.3.

EMC, Captiva, Documentum, Greenplum, Greenplum Database, RSA, FraudAction, the EMC logo, and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. © Copyright 2011 EMC Corporation. All rights reserved. Published in the USA. 11/11 EMC Perspective H8984

CONTACT US
To learn more about EMC solutions, visit us at www.emc.com/publicsector, or call 1-800.607.9546 (Outside the U.S.: +1.925.600.5802).