



**North Carolina's Enterprise
Fraud, Waste and Improper Payment
Detection Program**

January 2012

**North Carolina
Office of the State Controller**

David McCoy, State Controller

Table of Contents

I. Executive Summary	2
II. Background	3
III. Program Requirements	3
IV. Program Approach	5
V. Challenges	12
VI. Budget	14
VII. Next steps	16
Appendix.....	17
Appendix A: Session Law 2011, HB 200-145	17

I. Executive Summary

Measuring fraud, waste and abuse is a difficult task, and there is no single national agency that collects and reports comprehensive fraud statistics. In discussions with various organizations and professionals, as well as a review of the literature including topical industry white papers, it is reported that fraud, waste and improper payments are estimated to be approximately 12% of all government spending. Fraud, waste and abuse occurs across all government lines of business from health and human services, tax revenue collection and disbursement, unemployment insurance, workers' compensation, retirement benefits, insurance fraud and much more.

Since 2008, the Office of the State Controller has managed North Carolina's Statewide Data Integration Program. Data integration provides the ability to merge and reconcile varied and disparate data into common, consistent formats, for analytical and reporting purposes. Standardized data, as well as common tools and technology, support quick, agile, fact-based decision making to support the State's critical business functions.

The first enterprise data integration initiative, the Criminal Justice Law Enforcement Automated Data Services (CJLEADS) program, integrated statewide offender information into a single, secure, web-based application to support criminal justice professionals and to improve the safety of North Carolina's citizens. The successful design, development, implementation and deployment of the CJLEADS program demonstrated the value of a data integration initiative.

North Carolina State government's role is to serve the public and manage taxpayer dollars with integrity, financial responsibility and transparency. The ability to identify, resolve and prevent incidents of fraud, waste and improper payments is critical to the State's fiscal management of public funds. Session Law 2011, HB 200-145, directed OSC to develop an enterprise process to detect fraud, waste, and improper payments across State agencies. The OSC has contracted with SAS to design, develop and host the North Carolina Financial Accountability and Compliance Technology System (NC FACTS) leveraging the SAS Fraud Framework technology. The NC FACTS program will evolve under the guidance of the legislatively created Data Integration Steering Committee and will seek collaboration and partnership with state agencies having an interest in leveraging integrated data to detect incidents of fraudulent, wasteful or erroneous overpayments in their business areas.

In the last quarter, the OSC has met with a number of North Carolina State government agencies to discuss the NCFACS program and to understand the agencies' current fraud detection programs. OSC outlined the program approach and identified potential areas of pilot development while documenting agency concerns about participation in the NC FACTS program and the challenges associated with sharing data critical to fraud analysis and detection.

This report highlights the activities of the program since the October 1, 2011 report.

II. Background

Business data is a valuable resource for organizations in government and the private sector. Data enables organizations to analyze historical behavior, predict future trends and make decisions based on business facts rather than intuition and supposition. Over the years, however, data has been gathered and stored in siloed systems that were built to meet the business needs of individual organizations. When data is stored in varying formats and technical platforms, the process of gathering information from different lines of business can be time consuming and difficult.

In Session Law 2007-323, HB 1473, the North Carolina General Assembly recognized this challenge and directed the Office of the State Controller (OSC) to develop a strategic plan for the integration of databases and sharing of information among State agencies and programs. Since 2008, OSC has managed the Statewide Data Integration Program, including the design, development and statewide implementation of Criminal Justice Law Enforcement Automated Data Services (CJLEADS) criminal justice data integration program.

Session Law 2011, HB 200-145, directed OSC to expand the data integration program by developing an enterprise process to detect fraud, waste, and improper payments across State agencies. This effort will work under the guidance of the Data Integration Steering Committee and will seek collaboration and partnership with State agencies having an interest in leveraging integrated data to detect incidents of fraudulent, wasteful or erroneous overpayments in their business areas. The Data Integration Steering Committee is chaired by the State Controller and is comprised of:

1. One member with an information technology background appointed by the Governor.
2. One member with a background in law enforcement appointed by the Governor.
3. One member with a background in government accounting appointed by the President Pro Tempore of the Senate.
4. One member with government operations experience appointed by the President Pro Tempore of the Senate.
5. One member with a background in information technology appointed by the Speaker of the House of Representatives.
6. One member with a background in business management appointed by the Speaker of the House of Representatives.

III. Program Requirements

The ability to identify, resolve and prevent incidents of fraud, waste and improper payments is imperative to the State's fiscal management of public funds. Studies have found that individuals willing to commit fraud or abuse in one business area will often times be involved or associated with improper activity in another business area. The management of potential areas of abuse requires access to enterprise data, the ability to evaluate and analyze that data using filters, predictive models, and statistics that provides improved fraud

detection, accurate information for investigation and recovery, and the prevention of future improper payments.

To develop an enterprise program that will detect fraud, waste, and improper payments across state government, OSC will work with state programs and agencies to identify the data and business rules necessary to support related analytics and reporting. Data collected and stored to support one agency's business needs will likely also support other agencies' data information needs as they relate to this enterprise activity. Data governance addressing security protocols, role-based security access and memorandums of understanding and agreement will be critical to sharing North Carolina's information at the enterprise level.

Session Law 2011, HB 200-145 also directs State agencies to fully support and participate in the development of an automated fraud detection system by providing data and business rules to analyze data, develop models which determine data patterns, and identify anomalies which may indicate unusual and perhaps fraudulent behavior.

In developing the program, OSC shall:

- Develop a long-range plan to implement an automated fraud detection system;
- Determine costs, including vendor costs, for five years beginning July 1, 2011;
- Coordinate with State agencies to determine interest in participating in the project and identify potential applications that can be included in an initial request for proposal;
- Establish priorities for developing and implementing potential applications
- Evaluate savings from each effort;
- Coordinate efforts with the State's data integration vendor to begin the implementation process;
- Establish a pilot to begin the implementation process and identify and resolve issues associated with expansion of the initiative;
- Coordinate with participating agencies to ensure that each has the resources and processes necessary to follow up on incidents of fraud identified by the vendor; and
- Provide recommendations to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee for Information Technology, and the Fiscal Research Division of the General Assembly on potential future initiatives and the cost and savings of each.

The legislation also requires quarterly reports to the chairs of the Appropriations Committee, the Joint Legislative Oversight Committee for Information Technology and the Fiscal Research Division of the General Assembly. The quarterly reports are to focus on:

- Incidents, types and amounts of fraud identified by agency;
- Amount actually recovered as a result of fraud detection by agency;
- Agency procedural changes resulting from fraud identification and the timeline for implementing each;
- State costs for fraud detection for the previous quarter;
- Payments to vendor for the previous quarter; and
- Anticipated costs and vendor payments for the previous quarter for each of the next two years from the date of the report.

To manage the program, OSC was directed to enter into a two-year enterprise automated fraud detection contract at a maximum cost of \$8 million for a two-year contract period with the State's data integration vendor. The contract must be based on a public-private Partnership with the State's data integration vendor contributing resources in the amount of \$5 million in each of the two contract years (FY11-12 and FY12-13). This partnership -- with the active participation and commitment of executive management from the State and the data integration vendor ensuring that North Carolina's tax-paying citizens are the direct beneficiaries of the contract -- will concentrate efforts on activities that provide the best return for the State's investment. Both parties will coordinate efforts to report benefits realized for each area of fraud, waste or improper payment analysis.

While the program will expend considerable effort on data collection and integration--along with consequential data analytics and reports to identify fraud, waste, and improper payments--providing support to business programs responsible for analyzing and investigating the identified fraud incidents is critical. This effort, in collaboration with the business area, will identify the business processes and resources required to recover fraudulent or improper payments, to prevent future incidents of fraud, waste and improper payments, and to ensure that the analytics used to identify these incidents are continually being improved and refined to more accurately evaluate risk and fraud patterns.

IV. Program Approach

- **Project Management**

Manage Phased Design, Development and Deployment Activities

Traditional enterprise IT initiatives include a broad scope of work effort that addresses all business requirements and strives to complete all areas of data and business functionality in a single implementation. This "Big Bang" approach results in complex design and development activities that are at risk of delays, scope change and cost overruns.

NC FACTS' project approach, like the CJLEADS data integration initiative, will follow a unique iterative design methodology to quickly achieve success and to maintain momentum with phased development, implementation and deployment. OSC will identify one or more pilot areas of manageable scope that will allow the project to achieve success and report benefits realized. Using the pilot to build knowledge of the SAS fraud framework and prove the viability of fraud detection applications, OSC will be able to develop critical experience which can be leveraged to support additional business areas.

Establish Hosted Technical Environment

The State data integration vendor, in a public-private partnership with the State, will contribute resources valued at \$5 million to the project in each of the next two fiscal years. A portion of these resources will provide the implementation, hosting and management of a robust technical infrastructure to support the NC FACTS application(s). The vendor-hosted approach enables the technical environment to be established and ready for development in an expedited timeframe.

In accordance with the Strategic Plan for Data Integration, common technical platforms, toolsets and database technology will enhance the ability to share and utilize data across the enterprise for multiple business needs. Shared infrastructure and technology may also allow the State to achieve economies of scale and efficiencies, reducing the cost across all data integration initiatives.

Establish Data Governance

The ability to effectively identify enterprise fraud, waste and improper payments requires access to a wide variety of data sources. Vital records, for example, help identify when benefits are erroneously paid out to deceased recipients. Access to offender information that indicates a service provider has a history of fraudulent behavior may improve the ability to accurately predict risk when reviewing provider credentials and claims. Tax information may assist in determining accuracy of dependent eligibility for government services. The information needed to support enterprise fraud detection will include highly sensitive and protected information. The NC FACTS program must understand the legal, statutory, and regulatory requirements associated with sharing, storing and analyzing various sources of data. Data governance includes the data sharing agreements, security policy and procedures, application requirements, such as business rules, role-based security and auditing capabilities, necessary to maintain the appropriate control and integrity of the data.

Determine Benefits Realized

The key to demonstrating the success of an automated fraud detection system is the ability to report on benefits realized from the implementation of the program. The State of North Carolina has a number of fraud detection initiatives operating throughout its agencies and organizations. Benefits from an automated enterprise approach to fraud detection may include: enhancing or supplementing existing fraud detection activities to more accurately identify cases representing higher risk or higher priority for recovery; expanding data available to assist in the analysis of fraud and improper payments; refining assessments of risk to optimize investigation, recovery, and prosecution efforts; developing new fraud detection capabilities; and improving business processes to prevent future incidents of fraud and waste.

OSC will work closely with partner agencies to accurately identify and report new and incremental benefits associated with the implementation of the automated, enterprise fraud detection program.

Support Enterprise-wide Business Programs to Improve Government Operations

While data integration and business analytic tools may be able to improve the ability to identify, investigate, and recover fraudulent or improper payments, business programs focused on preventing fraud are essential to reducing waste in state government. Programs including ethics training and program integrity controls will help educate employees on ways to identify, document and report suspect behavior in their business areas. The State must consider ways to motivate employees to report suspect behavior and ensure that there is protection for the employee reporting improper activity. OSC will investigate programs in other states and the federal government to understand effective options for North Carolina.

- **Analysis**

Fraud, waste and improper payment detection is a challenging endeavor. The ways in which individuals and businesses engage in fraudulent activity is varied and continuously changing. Activity that may not raise a flag in one area of the State's business may be highly suspect when linked to the same individual's activity in another area of the State's business. While not all improper payment activity results from criminal intent, the analytics used to detect suspect activity can also help identify areas where controls are needed to prevent wasteful or improper payments as well.

In order to achieve enterprise level fraud, waste and improper payment detection, the ability to integrate, store, mine, and analyze broad centralized data is vital. NC FACTS' multi-dimensional approach will analyze data to detect patterns, anomalies, and linkages within business silos as well as across agencies boundaries to identify questionable or suspect activity. This analysis will include:

Identification

The NC FACTS system will strive to systematically verify that the individual or business entity is who they say they are. For example:

- Is the SSN or tax payer id provided by the entity a valid federal number? Is the number associated with a deceased individual?
- Is the business registered with the Secretary of State's office?
- Are phone numbers and addresses valid?
- Does the entity demonstrate the same attributes across all State areas of business, (i.e. do the entity's employment records match vendor information, revenue data or perhaps licensing board information)
- Has the entity's history or pattern of behavior changed abnormally over-time indicating possible suspect activity

Validation

The NC FACTS system will strive to validate if the individual or business entity is following the rules. For example:

- Is the individual or business listed on any of the “do not do business with” or “dis-barred” lists available at the state or federal level?
- Does the individual or business owner have previous criminal behavior that might indicate risk for a particular service or business area?

Association

The NC FACTS systems will strive to identify linkages between entities within a state program area or across program areas. For example:

- Is the owner(s) of this business associated with other businesses?
- Do business entities share addresses, P.O. boxes, phone or fax numbers?
- Do multiple businesses list the same employees?
- Are there other connections that may indicate collusion or fraud rings?

Identification, validation and association processes will require access to historical, detail-level data to enable detailed data mining and analytics.

● **Research**

OSC has conducted initial meetings with a variety of State agencies and organizations to introduce the program and to determine the level of interest in participating with OSC in developing analytical tools to support their service area. In each meeting, OSC learned about the agencies’ current efforts in identifying, recovering and preventing fraud, waste and improper payments. The following meetings have been conducted since the October 1, 2011 report:

The Department of Health and Human Services

The Department of Health and Human Services (DHHS) manages a wide range of services which support the health, safety and well-being of all North Carolinians. With a budget of \$14 billion comprised of federal and state funds to support Medicaid, mental health and disabilities as well as social services, the potential for fraudulent, erroneous and wasteful payments is high. Recognizing the potential for fraudulent activity, DHHS has instituted many initiatives, programs and sections to support investigations.

OSC met with the Secretary and executive management team of DHHS in September, 2011 and held a follow up meeting with DHHS in November, 2011. DHHS provided information on their current programs and efforts that are focused on identifying, investigating and recouping fraud and overpayments. The DHHS has a number of on-going fraud analysis and detection initiatives and within the Division of Medical Assistance (DMA) they have a Program Integrity section devoted to the analysis and collection of Medicaid overpayments. DHHS expressed concern that the NC FACTS

program activities may duplicate these on-going efforts and would place undue burden on the limited DHHS resources.

While the intent of NC FACTS is not to duplicate existing efforts, the program recognizes that many of the current DHHS efforts evaluate data only within the DHHS silo and are focused on identification of fraud that has already occurred. The investigation and recovery related to these incidents can be time consuming and complex. While NC FACTS will also analyze historical data, the objective is to use more comprehensive enterprise data to conduct analysis, leverage predictive models to identify suspect behavior patterns, and provide scoring and relationships to help investigators target their efforts on those individuals and entities who display the greatest risk. The application will also strive to identify methods for preventing future incidents of similar suspect behavior.

In addition, the DHHS data as well as their on-going fraud analytics results will be critical to examining fraud across the enterprise. Combined knowledge about businesses, and individuals will help to validate the information to other agencies across the enterprise.

OSC will continue to work with DHHS to establish a work group to understand how NC FACTS can use DHHS data in enterprise fraud detection and will identify areas of focus within DHHS that are not being addressed by current fraud efforts.

The State Health Plan of North Carolina

The State Health Plan of North Carolina (SHPNC) provides health care coverage for teachers, state employees, retirees, current and former lawmakers, state university and community college staff personnel, state hospital staff, and their dependents. In managing the health care products and services for more than 663,000 people, there is potential for fraud and overpayment.

The Interim Deputy Executive Administrator and executive management team of the State Health Plan provided information about their current efforts and challenges in identifying fraud and overpayments. The SHPNC works to identify fraud in areas such as provider billing for improper or unnecessary procedures, falsifying diagnoses, and billing for services not performed. Consumer fraud may include filing claims for services or medications not received or falsely claiming dependent eligibility. Better access to information and tools may aid in identifying these types of improper payments. The SHP expressed interest in participating in the NC FACTS pilot initiative and subsequent meetings have been held to identify data content, determine areas of analytic focus and to outline an approach for a State Health Plan pilot. The NC FACTS project team is currently drafting the pilot approach document for review by the SHPNC.

The Department of Justice – Medicaid Fraud Control Unit

The Department of Justice (DOJ) Medicaid Fraud Control Unit (MFCU) is a federally funded organization focused on the investigation and prosecution of Medicaid fraud incidents. Currently, the MFCU conducts most of its investigations as a result of case referrals from DHHS, tips from hotlines, or incidents that result from other criminal investigations. A part of these criminal investigations, sworn law enforcement officers, investigators, and attorneys, gather information from a variety of data sources to develop complete case information. This task can be time consuming, involves logging onto multiple systems and issuing individual requests for data, requires manual collection and evaluation of data.

The DOJ MCFU indicated that electronic access to data, access to additional sources of data, and the ability to combine and analyze information through automated tools would facilitate their investigative efforts.

The Department of Insurance

The Department of Insurance (DOI) provides oversight and regulation of the insurance industry, insurance agents, and claims adjusters in North Carolina, along with various other programs. DOI fraud investigators examine potential incidents of fraud reported by insurance companies, agents, and customer as well as tips from hotlines and website reports.

DOI investigators use a variety of data sources to identify patterns and indications of suspect behaviors. Some data is accessed through online systems while other data must be requested for each incident. DOI indicated that electronic access to more information as well as the ability to combine, analyze, and rank information through automated tools would facilitate their investigative efforts.

NC FACTS will evaluate the ability to use DOI information in the enterprise fraud detection application including DOI's State-Based System which tracks information about suspect cases.

The Department of Secretary of State

The Department of Secretary of State (DSOS) is responsible for the oversight and stewardship of information on business entities operating in the State of North Carolina. DSOS manages corporate registration with the State, Uniform Commercial Code, Charitable Solicitation licensing, and Notary Public commissions.

The DSOS investigates potential fraudulent incorporation or reincorporation incidents as reported to the department. Information such as addresses, phone numbers, office locations and business owner information may provide keys to identifying suspect information with DSOS. Access to this public information will also be valuable to validate information from other State business areas. The DSOS has offered to share its

public information with the NC FACTS application, and the technical team is working to establish the technical process to integrate the data.

The Office of the State Controller

The Office of the State Controller manages the North Carolina Accounting System (NCAS) and the BEACON HR/Payroll System. Both systems contain valuable information for the NC FACTS project.

NCAS manages a statewide vendor list which identifies the vendors that can be paid from the accounting system. This vendor file is currently used to perform debt set-off with the Department of Revenue and will be a valuable data source for NC FACTS to assist in linking vendors throughout state business areas.

The BEACON HR/Payroll system has employee payroll and time information. As NC FACTS works with the State Health Plan on member eligibility, this data will be valuable in confirming member eligibility and status.

NC FACTS is working with NCAS and BEACON to identify data to be integrated into the NC FACTS program.

Division of Employment Security

The NC FACTS team held a preliminary meeting with the Employment Security Commission (ESC) in September 2011. ESC has transitioned to the Division of Employment Security (DES) in the Department of Commerce. Following the initial meeting, information about security protocols and program objectives were provided to the DES and a more in-depth meeting was requested.

On December 2, 2011, the State Controller received a letter from Assistant Secretary Lynn Holmes indicating that DES has well established practices and systems in place for the detection, prevention, and recovery of improper payments as well as fraud detection efforts. As a result of these on-going efforts and with concerns that NC FACTS would over-burden existing resources, DES indicated that it is unable to participate in the enterprise fraud initiative at this time.

Other agency meetings reported in the October 1, 2011 report include:

- North Carolina Office of the State Auditor
- Office of State Budget and Management – Office of Internal Audit
- Department of Health and Human Services
- Department of Revenue

- **Pilot Program**

Following initial meetings with agencies, the State Health Plan has been identified as a likely candidate for a pilot NC FACTS area of focus. OSC is working closely with SHPNC to develop a pilot project proposal, identify specific data sources, address governance issues associated with data sharing, and establish a project timeline.

In addition to addressing State Health Plan fraud detection in the areas of member eligibility and claims analysis, the initial pilot will begin to build enterprise functionality that will be used for future business areas as they are added into the enterprise program.

Examples of these enterprise functions might include:

- Validating businesses with Secretary of State’s incorporation databases
- Verifying providers, recipients, members against Social Security Death Index
- Validation of payments against NCAS vendor files
- Development of a “do not do business” or “bad actors” file.

The enterprise functions will begin to build the linkages and interconnectivities that will support enterprise level analysis and reporting. As other critical data sources are added, the enterprise functions will be expanded.

V. Challenges

Data Sharing

The data needed for effective enterprise analysis will include highly sensitive and secured information. The ability to protect Personal Identifying Information (PII), adhere to security and compliance requirements for the Health Information Portability and Accountability Act (HIPAA), and meet the constraints associated with other state and federal regulations associated with tax information and employment data, will be critical to sharing information across the enterprise. NC FACTS will work with agencies to develop the required policies, procedures, contractual agreements, and memorandums of understanding or agreement necessary to define the parameters associated with data sharing of this key information within the State’s fraud initiative.

Stringent application security, including physical security, user authentication, role-based security, data encryption, and more will be key components in the implementation of an enterprise fraud detection system. The success of this initiative will be dependent on partner agencies who strive to find and implement appropriate policies and controls to enable data sharing.

In discussions with some of the agencies that are data stewards of key data sources, we have been informed that statutory or regulatory challenges prevent the ability to share critical data with this statewide initiative.

Department of Revenue (DOR) houses key information about business and individual income, revenue, sales and tax information. This information is critical to analyzing a

variety of areas including validating business and individual identities, reviewing provider claims and payments, analyzing recipient eligibility, and recognizing inconsistency in operations across the State's business areas. DOR data is critical to the enterprise effort, regardless of the participation of DOR in the new automated fraud initiative. DOR has indicated that federal and state statutes and regulations as well as the challenge of co-mingled federal and state data will prohibit the ability to share information with the NC FACTS initiative.

Division of Employment Security (DES) houses critical employer/employee filing information including employment tax data and unemployment claims data. Similar to revenue data, DES contains critical information to allow for validation of consistent business information as well as to provide key linkages across State agencies. While DES has indicated an inability to participate in the enterprise fraud initiative, the DES data remains a critical piece of the data puzzle for enterprise level analysis. DES has indicated that there are statutory and regulatory prohibitions to sharing key employment information.

Department of Health and Human Services (DHHS) houses key information about medical service providers, recipients, and claims, as well as other social services information. DHHS has also expressed concern about placing additional burden on their current fraud detection program resources with the NC FACTS effort. While NC FACTS may not engage in detailed fraud analysis within Medicaid, the data and results from current Medicaid efforts will again be vital to enabling linkages and an enterprise view of businesses and individuals. There will be regulatory requirements related to HIPPA protected information that must be addressed.

The NC FACTS program will need the support of these critical agencies and the General Assembly to address the statutory and regulatory inhibitors to data sharing. OSC has and will continue to request that each agency cite the specific statutory and regulatory prohibitions to sharing data as well as their recommendations for addressing each issue to ensure that data can be shared with this mandated state program. The OSC will provide regular updates to leadership on the need for legislative action to enable data sharing in support of the NC FACTS program.

Program Resources for Investigation and Recovery Efforts

As the automated fraud detection system is implemented and expanded throughout State business units, OSC anticipates an increase in the number of incidents and types of fraud identified. Identifying fraud is only one step in the process of improving government operations. The ability to investigate and recover funds that were improperly expended -- and more importantly the ability to prevent future incidents of fraud -- is critical to achieving measureable success in improving government operations.

Agencies and organizations must have the resources necessary, whether on staff or through contractual services, to analyze, investigate, and recover improperly expended funds. Programs must also have the resources necessary to adapt business policy and

procedures, and improve information technology systems to identify and prevent improper payments rather than trying to recover funds improperly expended.

Measurement of Benefits Realized

As previously mentioned, there are a number of on-going fraud detection initiatives throughout state government. The challenge will be the ability to clearly identify benefits associated with the implementation of the enterprise fraud detection initiative. To accurately measure and report on benefits realized, OSC will work closely with partner agencies and organizations to identify how enterprise data access supplements existing detection efforts and how new tools and capabilities enable additional fraud detection activities.

As the fraud detection improves the ability of state agencies to enact processes and controls to prevent fraud, quantitative reporting of prevention efforts may be challenging. Estimated benefits will consider historical fraud statistics as well as measured payments that were flagged and stopped prior to payment.

Maintenance of Analytical Models

Enterprise data and robust analytical tools will identify data patterns and anomalies in order to detect fraudulent and improper payments. With advanced analytics, it is likely that the number of identified data anomalies will increase significantly. Because State agencies and organizations have limited resources to review, investigate and recover improper payments, it is critical that the automated fraud detection system provide a feedback mechanism to refine the analytic models. As investigators determine which cases represent actual fraud versus cases that represent erroneous payments, the models can be adjusted to better identify high risk cases. Feedback will also allow the models to be refined so that suspect criteria are more specific and can reduce the number of “false positive” cases. The feedback can also provide information to stop suspect payments for a review process prior to expending funds.

As the State improves its ability to detect and prevent fraud, individuals who commit fraud will find alternative methods of gaining improper access to payments and services. All analytic models must be flexible and easy to modify to ensure the State’s fraud detection ability maintains pace with the creativity of those trying to defraud the state.

VI. Budget

Session Law 2011, HB 200-145, authorized funding of \$4.5 million in each year of the biennium budget for the development of an automated fraud, waste and improper payment data integration program. These funds will support OSC state project team staffing and expenses (\$500,000) as well as contractual services for the design, development and implementation of data integration and business analytic models for fraud detection (\$4 million). To ensure the public-private partnership of this initiative, the State’s data

integration vendor will contribute resources in the amount of \$5 million in each of the next two years. The vendor contribution will provide hosting hardware and technical environment infrastructure, software, support and services for design, development and implementation of data integration and business analytic model development.

Projected Budget

As of July 1, 2011	FY 2012	FY 2013
Fraud Detection Funding		
State Funding	\$4,500,000	\$4,500,000
Vendor Financial Contribution	5,000,000	\$5,000,000
Carryover from Prior Year		\$3,000,000
	<u>\$9,500,000</u>	<u>\$12,500,000</u>
Fraud Detection Expenditures		
State Project Team Expenditures	\$500,000	\$500,000
Vendor Contracted Services Payment - December, 2011	1,000,000	
Vendor Contracted Services Payment - July, 2012		3,000,000
Vendor Contracted Services Payment - December, 2012		3,000,000
Vendor Contracted Services Payment - June, 2013		1,000,000
Vendor Hosting, Software and Contracted Services Contribution	5,000,000	5,000,000
	<u>\$ 6,500,000</u>	<u>\$ 12,500,000</u>
NC FACTS Total	\$ 6,500,000	\$ 12,500,000
Budget Funds Remaining	<u><u>\$ 3,000,000</u></u>	

Actual Expenditures/Vendor Contributions

As of November 30, 2011	FY 2012 Actual	FY 2013
Fraud Detection Funding		
State Funding	\$4,500,000	\$4,500,000
Vendor Financial Contribution	5,000,000	\$5,000,000
Carryover from Prior Year		\$3,000,000
	<u>\$9,500,000</u>	<u>\$12,500,000</u>
Fraud Detection Expenditures		
State Expenditures		
State Project Team Expenditures	\$0	
Vendor Payments		
Vendor Contribution		
Vendor Hosting, Software and Contracted Services Contribution	320,010	
	<u>320,010</u>	
NC FACTS Total	\$ 320,010	\$ -
Budget Funds Remaining	<u><u>\$ 9,179,990</u></u>	<u><u>\$ 12,500,000</u></u>

VII. Next steps

- Establish a technical environment to support data integration, data storage and data analytic capabilities.
- Initiate pilot program
 - Complete the pilot proposal document
 - Identify data and business requirements
 - Establish data sharing agreements
 - Begin development activities for data integration and business rules
 - Develop analytic models and reports
 - Test and refine application
 - Establish business operations including user administration, training, and customer support
 - Train and support business users
 - Identify incidents of fraud, waste, improper payments
 - Provide program recommendations for recovery and prevention of identified incidents
 - Report benefits realized.
- Identify data sharing statutory and regulatory challenges and recommendations for addressing these challenges.
- Identify additional business areas of interest and plan for program expansion.

Appendix

Appendix A: Session Law 2011, HB 200-145

SECTION 6A.20.(c) As part of the State's continuing effort to develop a comprehensive enterprise-level data integration capability, the Office of the State Controller shall develop an enterprise process to detect fraud, waste, and improper payments across State agencies. State agencies shall fully support and participate in OSC's efforts to develop an automated fraud detection system

In support of the automated fraud detection effort, the OSC shall:

- (1) Develop a detailed long-range plan to implement an automated fraud detection system within State agencies.
- (2) Determine costs, to include vendor costs, for the effort for five years, beginning July 1, 2011.
- (3) Coordinate with State agencies to determine interest in participating in the project and to identify potential applications that can be included in an initial request for proposal.
- (4) Establish priorities for developing and implementing potential applications.
- (5) Evaluate savings resulting from each effort.
- (6) Coordinate efforts with the State's data integration vendor to begin the implementation process.
- (7) Establish a pilot to begin the implementation process and to identify and resolve issues associated with expansion of the initiative.
- (8) Coordinate with participating agencies to ensure that each has the resources and processes necessary to follow up on incidents of fraud identified by the vendor.
- (9) Provide recommendations to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly on potential future initiatives and the cost and savings associated with each.

SECTION 6A.20.(d) Beginning October 1, 2011, the OSC shall provide quarterly reports to the chairs of the Appropriations Committee of the House of Representatives and the Appropriations/Base Budget Committee of the Senate, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly. These reports shall include the following:

- (1) Incidents, types, and amounts of fraud identified, by agency.
- (2) The amount actually recovered as a result of fraud identification, by agency.
- (3) Agency procedural changes resulting from fraud identification and the time line for implementing each.
- (4) State costs for fraud detection for the previous quarter.
- (5) Payments to the vendor for the previous quarter.
- (6) Anticipated costs and vendor payments for each of the next two years from the date of the report.

SECTION 6A.20.(e) The Office of the State Controller is authorized to enter into an enterprise automated fraud detection contract for eight million dollars (\$8,000,000) for a two-year contract period. Under the terms of the contract, payments are limited to the following payment schedule:

- (1) December 2011—\$1,000,000.

- (2) July 2012—\$3,000,000.
- (3) December 2012—\$3,000,000.
- (4) June 2013—\$1,000,000.

Further, payments shall be contingent upon achieving the anticipated schedule of benefits realization.

To maximize cost reductions and savings, the Office of the State Controller shall enter into the agreement no later than September 1, 2011. To ensure this is a Public-Private Partnership, the Office of the State Controller shall ensure that the chosen vendor shall contribute resources valued at least five million dollars (\$5,000,000) during each of fiscal year 2011-2012 and fiscal year 2012-2013 for the project's success.

SECTION 6A.20(f) The Office of State Controller shall ensure that the State receives an appropriate share of intellectual property ownership or residuals, or both, accruing as a result of subsequent contracts between the vendor and third parties that utilize the innovations developed as a result of this contract.

SECTION 6A.20(g) Of the funds appropriated from the General Fund to the Office of the State Controller, the sum of one million five hundred thousand dollars (\$1,500,000) for the 2011-2012 fiscal year and the sum of seven million five hundred thousand dollars (\$7,500,000) for the 2012-2013 fiscal year shall be used to support the enterprise process to detect fraud, waste, and improper payments across State agencies in each year of the biennium. Of these funds, five hundred thousand dollars (\$500,000) each year shall be used by the Office of the State Controller to support the initiative. The remainder may be used to fund payments to the vendor.

Session Law 2011-391, HB 22. (Technical Corrections Bill)

SECTION 12.(c) Section 6A.20(c) of Session Law 2011-145 reads as rewritten:

"SECTION 6A.20.(c) As part of the State's continuing effort to develop a comprehensive enterprise-level data integration capability, the Office of the State Controller shall develop an enterprise process to detect fraud, waste, and improper payments across State agencies. State agencies shall fully support and participate in OSC's efforts to develop an automated fraud detection system and shall upon request provide in a timely and responsive manner accurate, complete, and timely data, business rules and policies, and support for project requirements. The agency head shall verify, in writing, the accuracy, completeness, and timeliness of the data. If any support or data is not provided as needed for the automated fraud detection effort, the OSC shall report that failure to the General Assembly for further review and action.

In support of the automated fraud detection effort, the OSC shall:

- (1) Develop a detailed long-range plan to implement an automated fraud detection system within State agencies.
- (2) Determine costs, to include vendor costs, for the effort for five years, beginning July 1, 2011.
- (3) Coordinate with State agencies to determine interest in participating in the project and to identify potential applications that can be included in an initial request for proposal.
- (4) Establish priorities for developing and implementing potential applications.
- (5) Evaluate savings resulting from each effort.

- (6) Coordinate efforts with the State's data integration vendor to begin the implementation process.
- (7) Establish a pilot to begin the implementation process and to identify and resolve issues associated with expansion of the initiative.
- (8) Coordinate with participating agencies to ensure that each has the resources and processes necessary to follow up on incidents of fraud identified by the vendor.
- (9) Provide recommendations to the Joint Legislative Commission on Governmental Operations, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division of the General Assembly on potential future initiatives and the cost and savings associated with each."