STATE OF ARKANSAS
Department of Finance and Administration

OFFICE OF THE DIRECTOR
1509 West Seventh Street, Suite 401
Post Office Box 3278
Little Rock, Arkansas 72203-3278
Phone: (501) 682-2242
Fax: (501) 682-1029
www.dfa.arkansas.gov

October 23, 2014

Senator Bill Sample, Co-Chair
Representative John Charles Edwards, Co-Chair
Arkansas Legislative Council
315 State Capitol Building
Little Rock, AR 72201

Re: Enterprise Fraud Pilot Project Study

Dear Senator Sample and Representative Edwards:

Pursuant to Section 20 of Act 275 of 2014, the Department of Finance and Administration was required to conduct an Enterprise Fraud Pilot Project Study and submit the report to the Arkansas Legislative Council. The report is attached.

If you have any questions, please contact Paul Louthian, Administrator, Office of Accounting at 501-682-1515.

Sincerely,

Richard A. Weiss
Director

cc: Paul Louthian, Administrator
Office of Accounting

DFA State of Arkansas
Department of Finance and Administration

Arkansas Department of Finance and Administration

Enterprise Fraud Pilot Project Study

Date: October 24th 2014

CONTENTS

I. Background

According to special language included in the Arkansas Department of Finance and Administration (DFA) 2014 Appropriation Bill, DFA was required to conduct an interagency study to determine the most economical and efficient means of implementing an enterprise fraud pilot program.

The study was to focus on an enterprise fraud pilot program that included the following scope.

1. Detects and prevents fraud, waste, abuse, improper payments, and employer noncompliance within the following three (3) programs.
   - The Unemployment Insurance (UI) program of the Department of Workforce Services
   - The Temporary Assistance for Needy Families (TANF) program
   - The Supplemental Nutritional Assistance Program (SNAP) of the Department of Human Services
2. Utilizes state-of-the-art enterprise fraud detection technology that further supports detection and prevention across State Agencies, programs, and functions.

The study was required to compare and contrast both Agency hosted (State licensed) and vendor hosted solution options. The content of the study includes without limitation funding requirements and substantive law changes necessary to implement Agency hosted and vendor hosted solutions.

The purpose of this document is to communicate the findings from the case study research and investigation that has been performed. The Executive Summary in Section II provides an overview of the case study results. Section III of the case study contains the detailed results that were compiled.

II. Executive Summary

Summary Recommendation

The research conducted by the Department of Finance and Administration (DFA) pursuant to Section 20 of Act 275 of 2014 was to provide the most economical and efficient means of implementing an enterprise fraud pilot programs:

- Department of Workforce Services (DWS) - Unemployment Insurance (UI)
- Department of Human Services (DHS) - Supplemental Nutrition Assistance Program (SNAP)
- Department of Human Service (DHS) – Temporary Assistance to Needy Families (TANF)

The State of Arkansas already has numerous fraud prevention and detection processes in place that meet the Federal Recovery, Audit, and Collection (RAC) requirements which are producing leads for agency investigators to pursue. DHS is currently in the procurement and implementation phases of two solutions that will replace current systems. Both of these solutions have fraud prevention and detection components. It is our recommendation to not make any changes until the full benefits of these new systems are realized.

Our research indicated that the addition of an identity authentication and verification solution similar to that which the State of Florida has implemented could provide additional benefits to the plans outlined above. It is estimated that it will cost between 4.5 and 5.8 million dollars ($4,457,750 - $5,792,250) to implement this solution and yearly system maintenance costs of 1.5 million dollars ($1,561,000).

We believe that an act of fraud will most likely involve multiple programs. Therefore, efficiencies and economies of scale would be better achieved if all fraud prevention and detection programs were placed under a single entity. With the recent establishment of the Office of Medicaid Inspector General for the State of Arkansas, it is further recommended that the fraud programs all be placed under their control.

Summary Research and Conclusion

DFA first developed our definition of the term "enterprise fraud program" to mean:

The use of technology software to identify and communicate patterns in data that are inconsistent with pre-defined analytic scenarios. The resulting output or fraud alerts are ranked, prioritized, and presented to investigators for research to determine if fraudulent activity is being attempted or if it has already occurred. If applicable, overpayment is calculated and attempts for collection are initiated as well as when necessary legal prosecution is sought.

The sources of information used for the research of this study were from two main categories: 1) State of Arkansas employees to assess the current efforts to prevent and detect fraud within the State of Arkansas related to the programs specified; and, 2) other states' related program personnel that have implemented enterprise fraud programs with similar requirements (Michigan, Kentucky, North Carolina, and Florida). The research compiled and the conclusions drawn were based solely upon information obtained from the sources mentioned above. Vendors of the competing product solutions were not contacted during this study.

The State of Arkansas programs included in this study (UI, SNAP and TANF) currently utilize enterprise fraud programs. The fraud program for UI (within DWS) varies from that of SNAP and TANF (within DHS) due to differences in IT systems, software, and program eligibility requirements. Both DWS and DHS have contracts with vendors to implement or have recently implemented new aspects to the technology used in these fraud programs. The current technology used is to assist in the detection of fraud that occurs after payment of

benefits. We did not research upgrades and enhancements that might be made to these systems in this process. Furthermore, it was found that while enterprise fraud technology was used, the majority of the investigations for SNAP and TANF occurred from face-to-face interactions of DHS county office workers.

Of the other States' that have implemented enterprise fraud programs with similar requirements, three (3) – Michigan, Kentucky, and North Carolina – have added to their existing fraud prevention program with new technology. The new technology was to assist in detection of fraud after payment of benefits. The vendor that all three (3) used was SAS. At the time of this study, impact or return on investment was too early to determine for each; however, it was stated that the new system for each had increased the number of investigations to the workload (an investigation does not necessarily indicate fraud) which turned out to be either an additional burden in personnel costs (9 FTEs in one instance) or inefficiencies in processing fraud investigations due to not having the personnel to work the cases. Michigan had an agency hosted version of the product which they applied to UI, SNAP, and Medicaid programs for an approximate initial cost of over 10.8 million dollars ($10,884,769) and approximate yearly maintenance cost of over a million dollars ($1,093,890 to $1,306,160). Kentucky and North Carolina choose a vendor hosted solution. Kentucky applied this solution to SNAP, TANF, and Medicaid for an approximate initial cost over 4.8 million dollars ($4,800,000) and approximate yearly maintenance cost of around four hundred thousand dollars ($400,000); whereas, North Carolina for programs not specified paid an initial cost of around 8 million dollars ($8,000,000) with an approximate yearly maintenance cost of around 1 million dollars ($1,000,000).

Florida opted to implement identity authentication and verification technology in addition to the already existing fraud program technology for the SNAP, TANF, Medicaid and other programs such as WIC and adoption assistance. This technology was to assist in prevention of payment to fraudulent applicants. In short, the basic notion is that an individual must verify their identity before having access to apply for assistance. Thus, those that are applying fraudulently are not paid, which in turn eases the burden of investigating and collecting. The vendor that was used was LexisNexis. According to Florida officials, the return on investment for the time period of March of 2013 to November of 2013 was approximately 12 million dollars ($12,152,956) in regards to identifying fraudulent applicants before payment. The approximate initial cost was 3 million ($3,000,000) with an approximate yearly service cost of 1 million ($1,000,000).

The cost figures outlined above represent the Vendor costs associated with software, implementation, and ongoing support. They do not include the State related costs associated with the implementation.

In conclusion, based on the research compiled, adding identity authentication and verification technology in addition to the current fraud programs already in place where attempted fraud is detected before payment would be the most economical and efficient in that the cost of fraud would decrease by non-payment of assistance to those attempting to defraud the system and it would lessen the burden of increasing cases for investigation and collection. An identity authentication and verification product, which is a type of fraud detection technology, could further support fraud detection and prevention across State Agencies, programs, and functions where identity verification of applicants is imperative.

III. Detailed Project Study

A. Case Study Overview

In order to support the objectives of the case study, the DFA assembled an investigation team. The team's research included existing fraud prevention and detection programs within the State of Arkansas and other States having recent and relevant experience with the implementation of enterprise fraud prevention and detection technology.

Enterprise fraud technology software is used to identify and communicate patterns in data that are inconsistent with pre-defined analytic scenarios. The resulting output or fraud alerts are ranked, prioritized, and presented to investigators for research to determine if fraudulent activity is being attempted or if it has already occurred. The source data used in the analytic scenarios originates in source system applications that are used to support daily business processes within the State.

The first key component of the case study included existing State of Arkansas research. The case study investigation included employees from the State of Arkansas who are actively engaged with the UI, SNAP, and TANIF fraud prevention and detection programs that are currently being supported within the State. Their expertise provided valuable insight into Arkansas's current collection of fraud programs, the people who support it, the types of fraud being investigated, and the data required for the analysis.

The second key component of the case study included research with other States. Employees from the States of Michigan, Kentucky, North Carolina, and Florida participated in the Study. Each of these States has had recent and relevant experience with the implementation of Fraud programs offered by third party software vendors. Their participation was valuable to the study and provided supporting details on actual implementation timelines, costs, and lessons learned.

In total, 24 of people participated in the case study.

Participants		
Case Study Investigation Team	**State of Arkansas Participants**	**External State Participants**
Stan King – Chief Information Officer, DFA	Tim Lampe, Asst Director for Quality Assurance, DHS	Jim Hogan, State of Michigan
Paul Louthian – Administrator, OA	Patrick Hallum, Program Manager, DHS	Dave Russell, State of Michigan
Ken Williams – Administrator, OIS	Jimmy Fields, Division Chief Financial Officer, DHS	Rodney Murphy, State of Kentucky
Ricky Quattlebaum – Administrator, Internal Audit	Drenda Harkins, ADD – Medical Services, DHS	Cher Randall, State of Kentucky
Maggie Garrett – Audit Manager, DFA	Ron Calkins, Asst Director for Unemployment Insurance, DWS	Jennifer Hart, State of Kentucky
Robin Morrissey – Administrator, DFA	Phillip Harris, Asst Director for TANF, DWS	David McMahan, State of Kentucky
Susan Smith – ERP System Manager, DFA	Don Denton, Program Administrator, DWS	Kay Meyer, State of North Carolina
Mark Rago – PMO Consultant, DFA		Carol Burroughs, State of North Carolina
Karl Foss – PMO Consultant, DFA		

B. State of Arkansas Research

The State of Arkansas owns software capable of detecting and preventing fraud in the SNAP, TANF and UI programs. None of this software is used on an enterprise-wide basis. Additionally, there are other techniques that are in place, such as activities to confirm identification, research services and to block IP addresses. Use of these techniques or software may be further shared, or expanded. There are some near-term plans to expand current activities.

Numerous computer systems are used to produce data related to the SNAP, TANF and UI programs. DHS administers the SNAP program, but they manage the software used for SNAP and TANF eligibility and fraud detection. All responsibility for TANF software will shift to DWS by 12/31/2014. DWS is solely responsible for UI.

1. DHS

Overview of Existing DHS Programs and Solutions

DHS uses the Arkansas Networked System for Welfare, Eligibility & Reporting (ANSWER) software as the system of record for SNAP and TANF eligibility. By 12/2014, DHS will phase out use of ANSWER and will transfer all support for the TANF program to DWS. ANSWER will be replaced by CURAM.

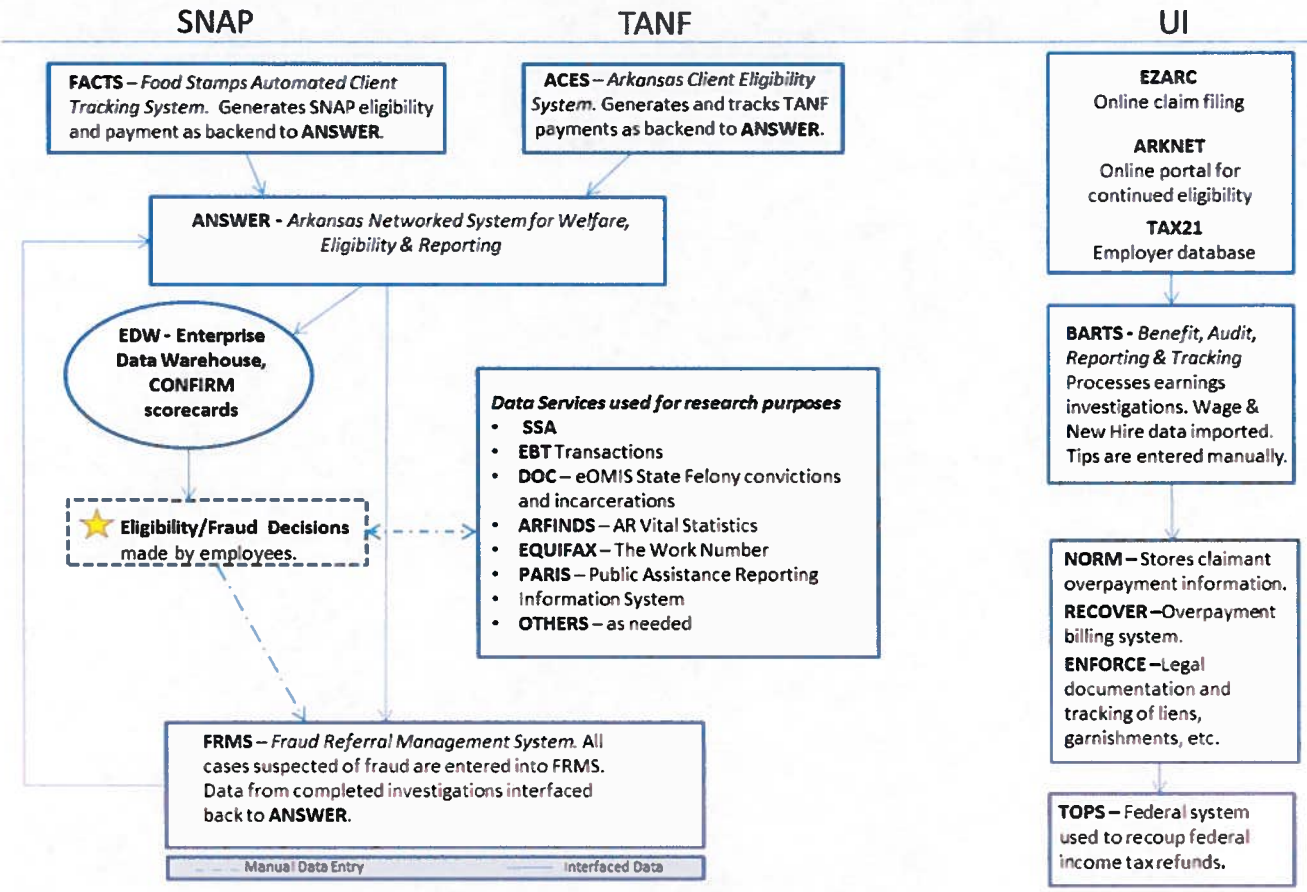
Eligibility data is cross-matched with other state, federal and private data using the Enterprise Data Warehouse (EDW). EDW produces reports and scorecards for investigators use. If fraud is suspected, data is input into the Fraud Referral Management System (FRMS), where the results are transferred back to ANSWER.

DHS has two units that investigate client fraud and DHS staff fraud. The State is not responsible for investigating or prosecuting retailer fraud. Approximately 97% of DHS fraud cases are related to SNAP.

The two investigative units are:

1. Division of County Operations (DCO) Special Investigations Unit (SIU)
    - Front-end investigations: includes interviews with neighbors, relatives, and friends of client. This unit investigates DHS employee fraud. If fraud is suspected after initial investigation, cases are referred to OQA. Of the 3,065 total initiated investigations worked from October to December 2013, 241 were referred to OQA. The yearly target rate for the number of referrals to OQA is 11-12%.
2. Office of Quality Assurance (OQA) Fraud Unit
    - Follow-up investigations: makes final determination if fraud has occurred and refers for prosecution (County Prosecutor's Office) and collection. Collections are handled by a different DHS office. Approximately 60-75% of the referrals from the SIU result in overpayment and/or fraud.

Overview of Existing Functionality:



Systems Currently Implemented

Name of System	Purpose of System	Agency Responsible	Person Responsible
Arkansas Networked System for Welfare, Eligibility and Reporting (ANSWER)	ANSWER is the eligibility database created by DHS. ANSWER is the system of record for DHS and DWS.	DHS until 12/14. DWS after 12/14	Northrop Grumman
Food Stamps Automated Client Tracking System	FACTS accepts data from ANSWER to generate and track SNAP eligibility and payments.	DHS	Northrop Grumman
Arkansas Client Eligibility System (ACES)	ACES generates and tracks TANF payments and participation.	DHS until 12/14. DWS after 12/14	Northrop Grumman
Enterprise Data Warehouse (EDW)	EDW can be used for a wide variety of data reporting needs. Data is imported from 7 data sources to produce CONFIRM scorecard forwarded to DHS and DWS investigators.	DHS	Tim Lampe

Name of System	Purpose of System	Agency Responsible	Person Responsible
Fraud Referral Management System	FRMS is used by all DHS investigators and county staff to record data about suspected fraudulent activity. Data is fed back to ANSWER when investigations are complete.	DHS	Patrick Hallum

DHS SNAP Results Produced

3,065 cases were reviewed for fraudulent activity from October 1, 2013 through December 31, 2013.

County Office caseworkers verify applicant information while application is processed. If fraud is suspected, the caseworker contacts the SIU unit. Caseworkers initiated 1,213 investigations between October 2013 and December, 2013.

County staff review client records or request an investigation for specific circumstances that may indicate fraudulent activity. For instance, a client has claimed no income or resources for several consecutive months (56 cases out of 3,065 from October to December 2013).

The SIU operates a fraud hotline. Between October and December 2013, the hotline tips generated 201 investigations. The hotline tips usually result in about an 18% yield of overpayments or fraud.

The SIU utilizes an Enterprise Data Warehouse (EDW) to assist in identifying suspected fraud. Reports and Scorecards known as CONFIRM are produced by this system. They are further analyzed by staff, who determines whether an investigation should be opened. Cases are delegated to investigators.

DHS Investigation, Oct – Dec 2013						Investigations driven from other data sources that may also be included in EDW:		
Cased Investigated by SIU	Cases Referred to OQA	Cases Initiated by Caseworkers	Cases Initiated by County Mgmt. Staff	Fraud Hotline	Investigation Directly Related to EDW Scorecard	Multiple Cards Replaced	Currently Incarcerated	Felony Drug Convictions
3065	241	1213	56	201	22	906	733	52

Current State Staffing Requirements

Description	Agency	# FTEs
Director of Fraud Investigation (Pam Greer)	DHS	1
OQA Investigators	DHS	17
SIU Investigators	DHS	19
Program Manager (Patrick Hallum)	DHS	1
Business Analyst	DHS	4
Project Manager	DHS	2

Description	Agency	# FTEs
Database Administrator	DHS	4
Data Architect	DHS	7
Software Engineer	DHS	1
TOTAL FTEs		56

2. DWS

Overview of Existing DWS Programs and Solutions

DWS Results for Unemployment Insurance (UI) and Temporary Assistance for Needy Families (TANF)

DWS supports several systems to assist with UI eligibility and to monitor ongoing claims. Those systems are described below. TANF eligibility data is managed in the ANSWER system that is currently maintained by DHS. This maintenance will shift to DWS by 12/2014. EDW CONFIRM Scorecards that identify potential TANF fraud are forwarded to DWS investigators for follow-up. ANSWER and EDW staffing and maintenance are discussed with DHS systems.

UI eligibility is managed with the Easy Arkansas Claims (EZARC) web-based system. Ongoing claims are supported in the ARKNET system for claimants and the TAX21 system for employers. 98% of all UI claims are entered by claimants into the EZARC system.

Fraud detection and prevention measures for DWS systems include:

- Creation of secure accounts
- Auto verification of SSN to name, gender, DOB
- Manual review of identification such as Driver's License
- Blocking all international IP addresses are blocked
- Blocking fraudulent United States IP addresses provided by the Dept. of Labor.

The Benefit, Audit, Reporting and Tracking System (BARTS) compares earnings with quarterly wage data, new hire data and tip information that is entered manually in order to determine fraudulent activity. If fraudulent activity is identified, data is submitted to the New Overpayment Recovery Module (NORM) for tracking. The RECOVER module is the billing system for overpayments, while ENFORCE generates legal paperwork such as liens, writs of garnishment, etc.

DWS does not import any external data into their systems for the purpose of detecting or preventing fraudulent activity.

There were 14,723 fraud cases identified in fiscal year 2014.

3. Future State Plans

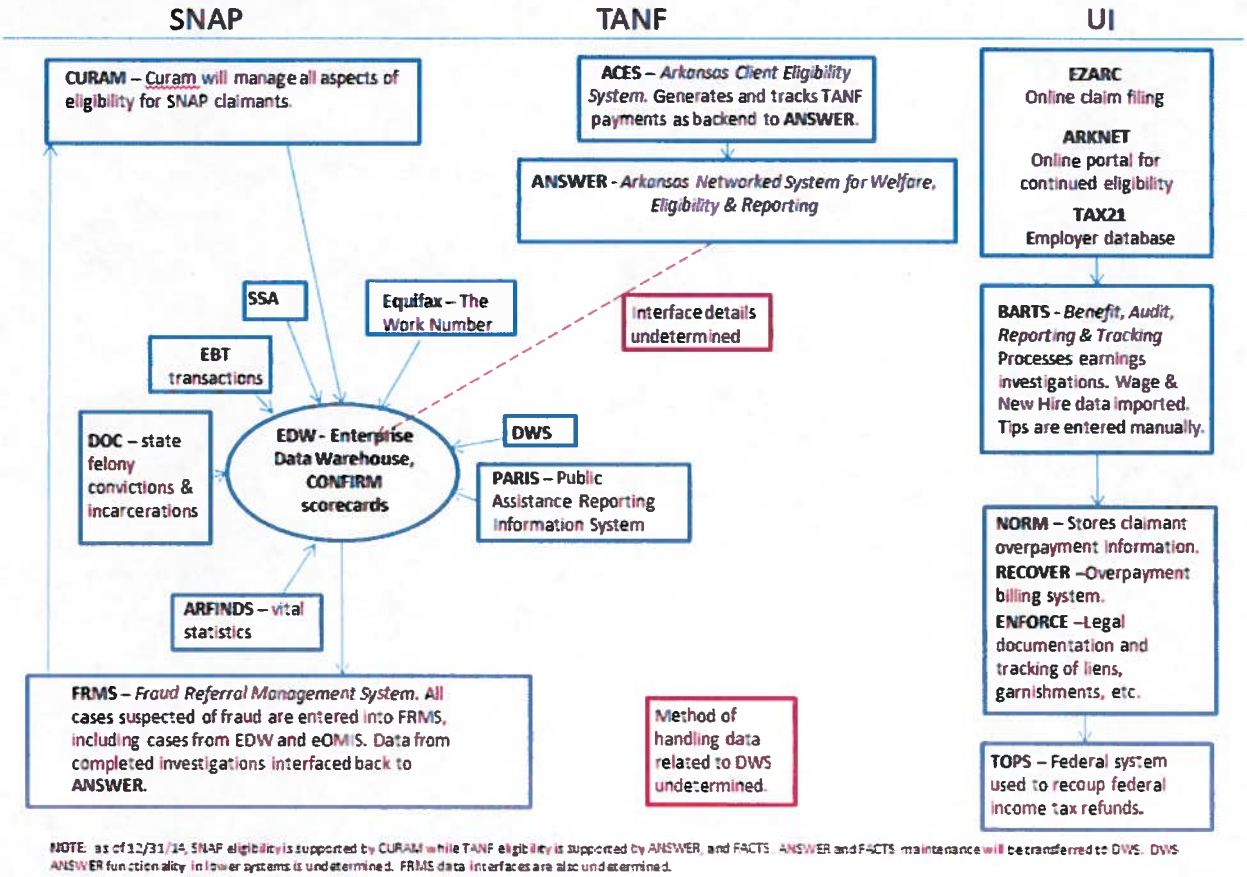
ANSWER will no longer be used or supported by DHS after 12/31/2014. Maintenance and support of ANSWER will shift to DWS for the TANF program. IBM's CURAM software is being implemented at DHS.

Known Future Systems

Name of System	Purpose of System	Agency Responsible	Person Responsible

Name of System	Purpose of System	Agency Responsible	Person Responsible
Electronic Benefits Transfer System	Target implementation scheduled for 11/2014. This system will produce additional scorecards for DHS investigators.	DHS	
Medicaid (EMFAD)	EMFAD is in very early stages at this time. A contract is expect to be awarded in FY2015. This should provide analytics using a wide variety of state data to determine Medicaid fraud. EMFAD is expected to be a vendor hosted (software as a service) solution.	OMIG	RFPs issued mid-2014
CURAM	Curam is a Commercial-off-the-shelf (COTS) solution intended to assist with determination of client eligibility as well as to track long-term client participation. DHS will maintain a Curam instance and DWS will maintain a separate Curam instance. Curam will replace ANSWER at DHS.	DHS and DWS	Richard Wyatt, DHS
OPTUM	Optum Decision Support System (V 1.0 for Arkansas)	DHS	Drenda Harkins

Known Future Functionality:



NOTE: as of 12/31/14, SNAP eligibility is supported by CURAM while TANF eligibility is supported by ANSWER, and FACTS. ANSWER and FACTS maintenance will be transferred to DWS. DWS ANSWER functionality in lower systems is undetermined. FRMS data interfaces are also undetermined.

4. Relevant Legislation and Law

DHS has data sharing agreements for each of the data sources used in the EDW system. There are no known statewide data sharing agreements. Discussions were held with state staff regarding HIPAA, FOIA and FERPA. Since all data is owned by the State of Arkansas, there is no known legal barrier from these 3 laws. Legal changes that could be beneficial are:

The expansion of the role of the Office of Medicaid Inspector General (OMIG) to encompass fraud detection and prevention through statutory authority for programs at DHS and DWS should include the authority to work with all data necessary to accomplish the mission.

Federal mandates do not allow state investigative staff to pursue retail fraud. State staff feels that local offices may be better staffed to manage these investigations.

Both DWS and DHS staff stated that federal income tax return data could be beneficial to their investigations.

While state incarceration data is available, city and county incarceration data is not. Better data sharing with local officials would yield a higher level of fraud data.

5. OMIG Medicaid Implementation

The Office of Medicaid Inspector General is required to establish a program known as the "Enterprise Medicaid Fraud and Abuse Detection" (EMFAD) program focused on fraud, waste, abuse, and improper payments within the Arkansas Medicaid Program by June 30, 2015. A Request for Information (RFI) was issued by the Office of

State Procurement (OSP). Twenty-one vendors responded to this RFI. EMFAD is expected to be a vendor hosted (software as a service) solution.

6. Medicaid Decision Support

DHS is implementing a new decision support system using IBM's OPTUM solution. OPTUM is a hosted solution that has fraud prevention and detection capabilities that could be useful in an enterprise solution.

C. External State Research

A core component of the Case Study are the findings from the research and investigation with other State Government entities who have recently implemented an enterprise fraud program using a 3rd party vendor software solution.

The DFA performed several interviews with targeted employees from four (4) States having direct involvement in the deployment of their fraud prevention and detection programs. Actual results were captured including implementation timelines and cost impacts. Lessons learned from their implementations were also shared and discussed.

State of Michigan – Implemented the SAS Analytics software for Food Assistance Program (FAP) initially in 10/2013 with the final FAP deployment targeted for 09/2014. Implementations for UI and Medicaid are in progress. Michigan elected to license the software directly through SAS rather than contract for a hosted solution with SAS. The driving force behind this decision was data ownership and data security concerns. Cost was not a contributing factor in the decision making process.

State of Kentucky – Implemented the SAS Analytics software for Medicaid in 02/2014. Implementations for SNAP and TANF are in progress. Kentucky elected to host the software with SAS rather than license the software directly. This decision was primarily a result of restricted State employee bandwidth and bench strength to support the implementing the solution in-house

State of North Carolina – Implemented the SAS Analytics software for Unemployment Insurance (Employer) in 12/2013 and Unemployment Insurance (Claimant) in 02/2014. Implementations for State Employee Health Benefits and Workers Compensation are in progress. North Carolina elected to host the solution with SAS to mitigate risks associated with employee turnover and loss of skills and knowledge to opportunities in the private sector marketplace.

State of Florida – Implemented the LexisNexis identity authentication and verification technology in addition to the already existing fraud program technology for the SNAP, TANF, and Medicaid programs in September of 2013. This technology was to assist in prevention of payment to fraudulent applicants. In short, the basic notion is that an individual must verify their identity before having access to apply for assistance. Thus, those that are applying fraudulently are not paid, which in turn eases the burden of investigating and collecting.

A common questionnaire was used to guide the research discussion with each State. Follow-on sessions were conducted as well, including a review of the case study content to confirm the accuracy of documented findings. Outlined below are the common themes discovered during the external State research.

- Each State has existing systems and processes in place for fraud prevention and detection. There are currently no plans to retire these systems. The new fraud implementation has augmented the existing business process procedures and provided additional analytic scenarios for investigators to pursue.
- The implementation of each program will require full time support from the State to prepare and verify data used by the analytic software. Staffing impacts must be analyzed closely.
- Data related issues were the primary challenge for each State during the implementation. Data sharing agreements memorandums of understanding were instrumental in removing barriers and garnishing cooperation amongst the Agencies for the project.
- Post go-live operations have been overwhelming at times for the users. The new system produces thousands of potential fraud leads, some of which may duplicate what is currently being produced through existing operations. Management and prioritization of the leads through all fraud system programs will be required in order to be effective. The system will need to be continually enhanced and tuned to reduce the volume of the non-actionable false positives leads produced.

- Each implementation is ongoing and will continue to be enhanced as fraud technology evolves.
- Each State indicated that it was too early in the implementation to calculate return on investment figures.

Outlined below are the detailed findings and results from the external State research that was performed.

1. State of Michigan

OVERVIEW

Since 2001 prior to the implementation of the new software solution, the State of Michigan has supported fraud prevention and detection through homegrown legacy data warehouse solutions and business processes.

The Michigan fraud initiative was launched, not through State Legislation, but rather through an Executive Management directive. The strategic goal was to coordinate a statewide data analytic solution to prevent and avoid the costly deployment of multiple fraud solutions throughout the State Agencies. It was determined that a common statewide solution for fraud prevention and detection would be more cost effective and produce better results than separate Agency solutions with silos of unintegrated data.

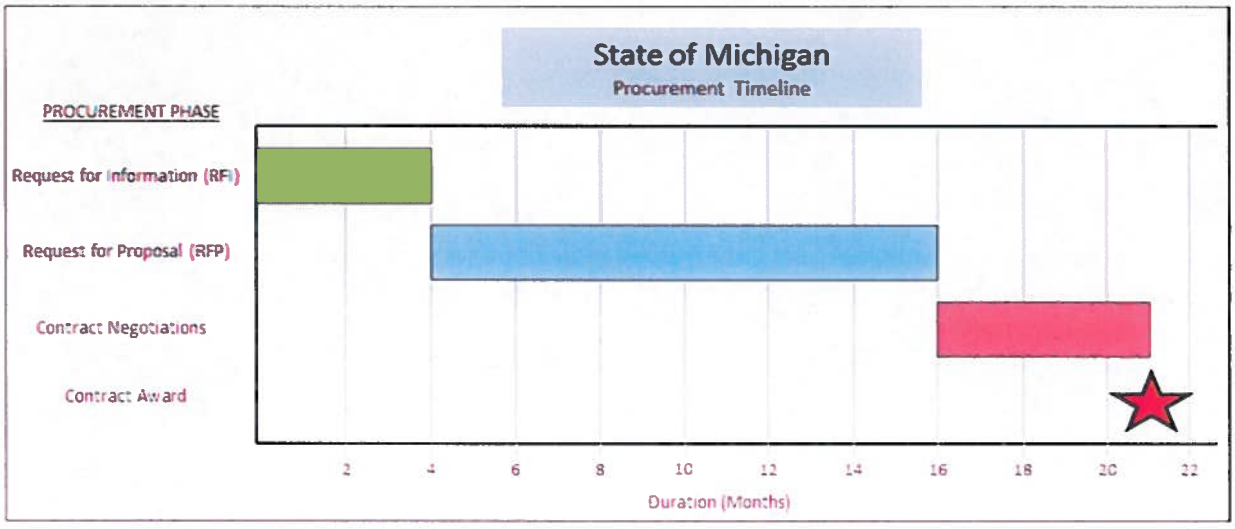
PARTICIPANTS

Outlined below are the people who participated in the Michigan case study interviews.

- Jim Hogan, Information Officer
- Dave Russell, State Administrative Manager

SOFTWARE SELECTION AND CONTRACT PROCUREMENT

The State of Michigan initiated their pursuit for the implementation of a fraud prevention and detection solution in April of 2011. The overall procurement process lasted approximately 21 months in duration leading to contract award in December of 2012.



The State of Michigan selected SAS and their analytic software as their vendor to support fraud prevention and detection. The State elected to license the software directly through SAS rather than contract for a hosted solution approach with SAS. The driving force behind this decision was data ownership and data security concerns. Cost was not a contributing factor in the decision making process.

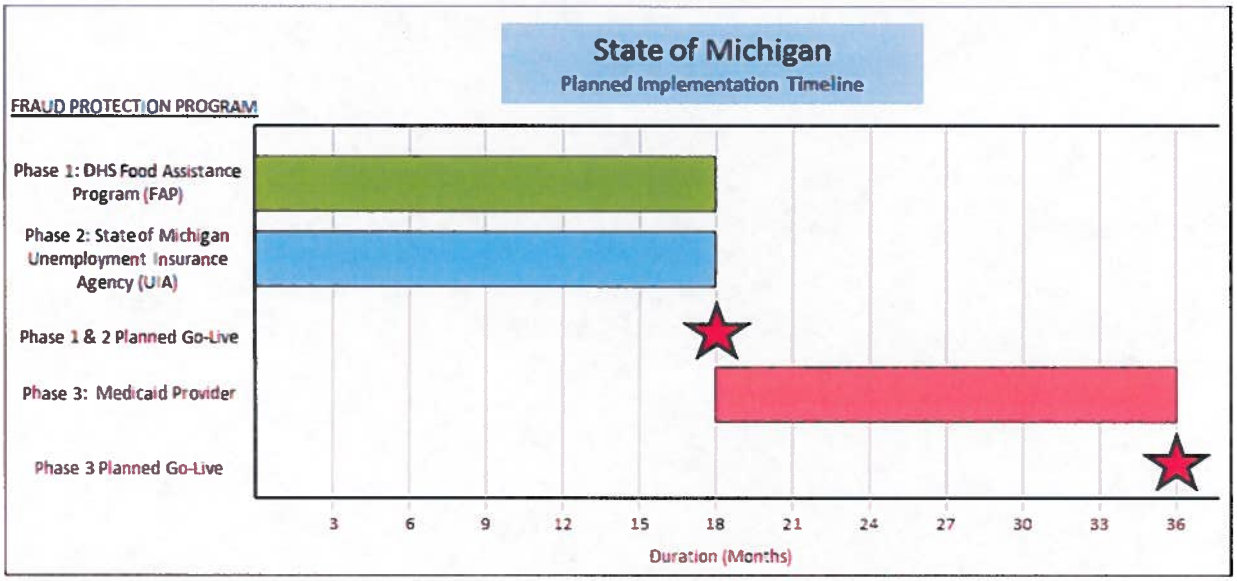
The original contract scope of work supports the implementation of the SAS analytic software for fraud prevention and detection in two phases.

- Phase 1: DHS Food Assistance Program (FAP)
- Phase 2: State of Michigan Unemployment Insurance Agency (UIA)

In September of 2013 the original contract scope was enhance through a change order to include an additional phase of implementation.

- Phase 3: Medicaid Provider

The planned project duration for phases 1 and 2 was eighteen (18) months in duration. Phase 3 was also planned for eighteen (18) months in duration and will follow the completion of phases 1 and 2.



Michigan signed a fixed price contract where SAS is compensated according to a defined deliverable payment schedule. The total cost for the implementation of all three phases of work is $10,884,769. The detailed breakdown of vendor costs is outlined in the table below.

SAS Implementation Costs			
Cost Component	**FAP and UIA**	**Medicaid**	**TOTAL**
Consulting Services	$1,150,798	$1,110,650	$2,261,448
* Software Licensing (Year 1 Only)	$3,059,860	$1,912,365	$4,972,225
Warranty, Maintenance, and Support (Year 1 Only)	$1,366,533	$854,063	$2,220,596
Contingency Funds	$430,500	$1,000,000	$1,430,500
TOTAL	**$6,007,691**	**$4,877,078**	**$10,884,769**

NOTE: annual software licensing fees (beyond year 1) are based on the number of physical or virtual process cores. Specific figures on these fees were not made available by the State of Michigan.

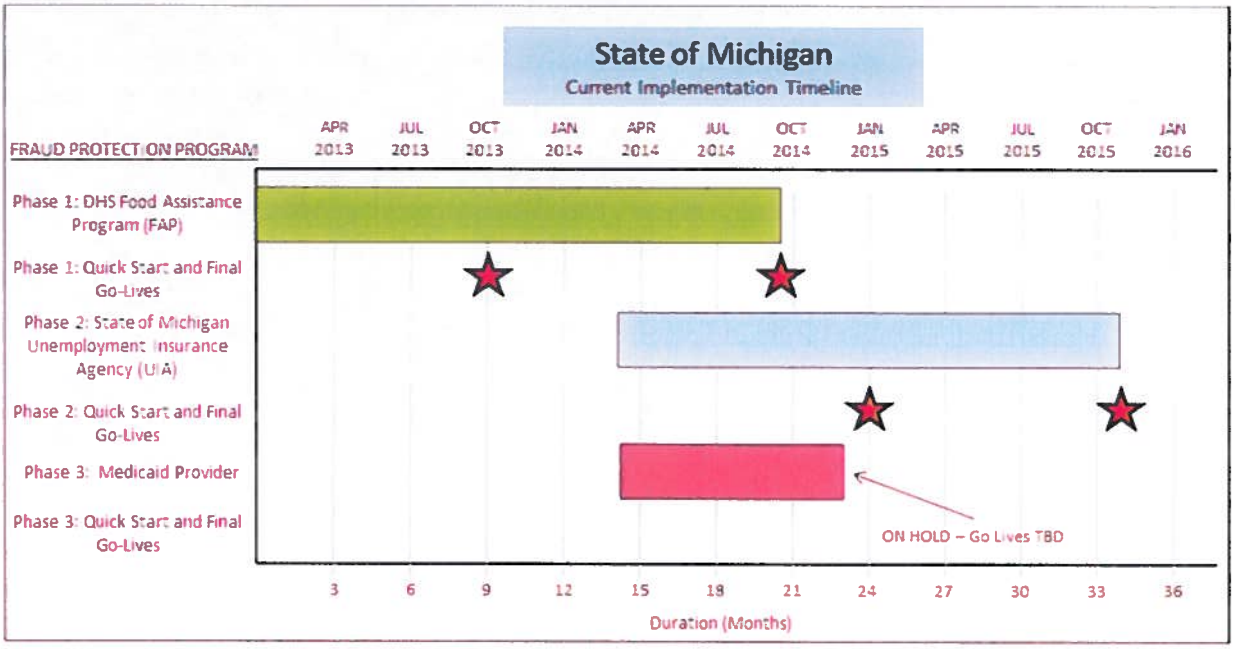
The vendor contract also includes optional annual Maintenance and Support fees (beyond year 1) to support the implementation of service packs, upgrades, and repairs for code defects. The detailed breakdown of the vendor costs for these services are outlined in the table below.

SAS Long-Term Maintenance and Support Costs			
Cost Component	**FAP and UIA**	**Medicaid**	**TOTAL**
Maintenance and Support (Year 2)	$673,169	$420,721	$1,093,890
Maintenance and Support (Year 3)	$693,364	$433,342	$1,126,706
Maintenance and Support (Year 4)	$714,164	$446,342	$1,160,506
Maintenance and Support (Year 5)	$735,589	$459,732	$1,195,321
Maintenance and Support (Year 6)	$757,657	$473,524	$1,231,181
Maintenance and Support (Year 7)	$780,387	$487,730	$1,268,117
Maintenance and Support (Year 8)	$803,798	$502,362	$1,306,160
TOTAL	**$5,158,128**	**$3,223,753**	**$8,381,881**

IMPLEMENTATION STATUS

When compared to the original plans, the implementation has proven to be more difficult and complex. Data sharing was a significant issue for the implementation. An Executive Directive on sharing data was issued to resolve this issue. The Directive was instrumental in gaining Agency support, cooperation, and participation on the project.

Due to other competing initiatives within the State, the actual implementation plans were revised from the original plans. The Phase 1 FAP was started in January of 2013. A "quick start" version of the FAP was implemented in October of 2013. The final version of FAP is targeted for release in September of 2014. Phase 2 UIA and Phase 3 Medicaid are in progress with data readiness and requirements gathering tasks. UIA is currently targeted for final version production release in November of 2015. Medicaid will be placed on hold after data readiness and requirements gathering tasks are completed. The final version production release is not known. The diagram below illustrates the current deployment timelines for the FAP, UIA, and Medicaid implementations.



The implementation team consisted of State employees and vendor consultants. The State of Michigan was required to provide the necessary staff and expertise to assist with business process questions, application development, data modeling, and data base administration. Functional experts were also required to validate the functionality, usability, and the accuracy of test results. Data source experts were required to provide data dictionary descriptions for each data source including data field name, description, type, and length. The State team members were primarily responsible for ensuring the source data was accurate and verifiable.

The project team consisted of approximately seven (7) full-time equivalents (FTEs) to support the computing infrastructure setup and data readiness. Subject matter experts (SMEs) from the supporting agencies were engaged as required for data readiness activities and tasks.

POST GO-LIVE OPERATIONS

Overall, the implementation of the new fraud analytics software has not had a measurable impact on operations and organizationally business processes remain relatively the same. The State continues to operate, support, and use their existing legacy fraud programs in parallel with the new fraud software solution. There are more automated tools and additional reporting available with the new software. Users of the business analytic data now have more information and potential leads to review and investigate. They are managing through the increased work load by focusing on the high ranking leads that have a high probability of fraud. More employee positions have been requested. From a fraud system support perspective, a portion of the original implementation team remains intact for on-going maintenance and support. A full-time project manager and several part-time system and data analysts are currently providing post go-live system support.

Although it is far too early in the overall implementation to determine what improvements and benefits will be gained, one visible improvement item that has been identified early has been the reduction in duplicate leads across the silos of data that exist.

RETURN ON INVESTMENT

Although the new Fraud Prevention System has been live since October of 2013, actual figures associated with return on investment have not been developed. The State has not had the opportunity to review actual results and determine the impacts and benefits realized from the implementation of the new fraud software solution. Based on their early experiences, Michigan considers cost recovery very difficult and that cost avoidance is a more effective goal to achieve.

KEY HIGHLIGHTS AND LESSONS LEARNED

Summarized below are the key highlights from the State of Michigan research.

- The fraud initiative was launched by the State to coordinate a statewide data analytic solution to prevent and avoid the costly deployment of multiple fraud solutions throughout the State Agencies.
- Consulting support was engaged for the development of solution requirements and RFP.
- The State has licensed the software from SAS. Data security and ownership were the key factors supporting the decision to license the software rather than have SAS host the solution.
- The scope of work include three programs (FAP, UIA, and Medicaid) and a vendor contract price of $10,884,769
- The initial timeline to implement FAP and UIA was 18 months. This timeline was not achieved as planned. FAP is live in production with "quick start" spreadsheet views of the information produced by the fraud software. The full solution for FAP is targeted for go-live in September of 2014. The UIA and Medicaid implementations are currently in progress.
- It is too early to determine the impacts and return on investment benefits of the new fraud solution.

- Organizationally, business processes remain relatively the same. More automated queries and additional reporting are now available to the State. The increased work load is being managed by prioritizing the fraud leads that are produced. New employee positions have been requested by the State.
- The Executive Directive on data sharing was the key element on gaining unwavering participation and collaboration on the project.
- Enabling a Governance Structure and enforcing Project Management disciplines were important for the project.

2. State of Kentucky

OVERVIEW

The State of Kentucky has a current program and solution for fraud prevention named Recovery, Audit, and Collections (RAC). The RAC program is required by Federal Law and therefore SAS will not be replacing it.

Approximately three (3) years ago Kentucky's Budget Director and the Governor's Chief of Staff attended a presentation by SAS on their fraud prevention software solution. Kentucky's fraud prevention initiative was further explored by Governor's Chief of Staff and eventually launched.

PARTICIPANTS

Outlined below are the people who participated in the Kentucky case study interviews.

- Rodney Murphy, Chief Information Officer
- Shari Randall, Division Director
- Jennifer Harp, Medicaid
- David McMahan, Fraud Project Manager

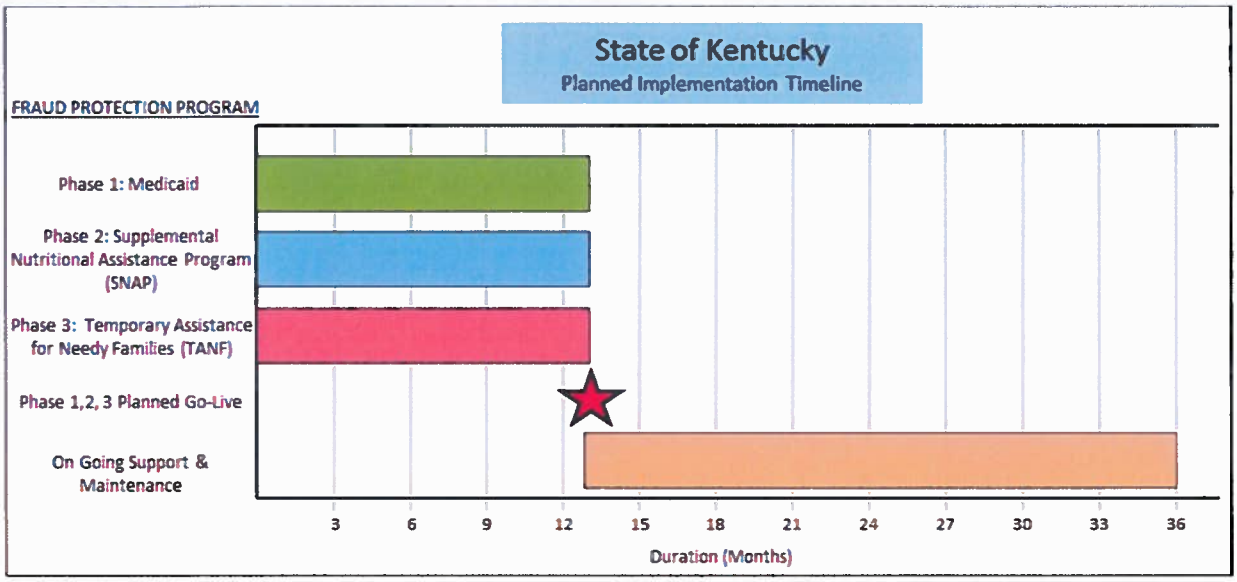
SOFTWARE SELECTION AND CONTRACT PROCUREMENT

Kentucky selected SAS and their analytic software as their software as their vendor to support fraud prevention and detection. A formal RFP process was avoided by expanding existing technology contracts with Deloitte to include the fraud prevention project. The State elected to host the software with SAS rather than license the software directly through SAS. The decision to host the solution was primarily based on the fact that they had restricted bandwidth and bench strength to support the implementing the solution in-house. Bandwidth and bench strength were a larger concern then data ownership and security. Regarding cost, Kentucky believed that costs were relatively the same when comparing hosted and licensed solution options.

The contract scope of work supports the implementation of the SAS analytic software for fraud prevention for the following programs.

- Phase 1: Medicaid
- Phase 2: Supplemental Nutrition Assistance Program (SNAP)
- Phase 3: Temporary Assistance for Needy Families (TANF)

The implementation timelines included thirteen (13) calendar months for each program. The implementations were originally planned to be performed in parallel.

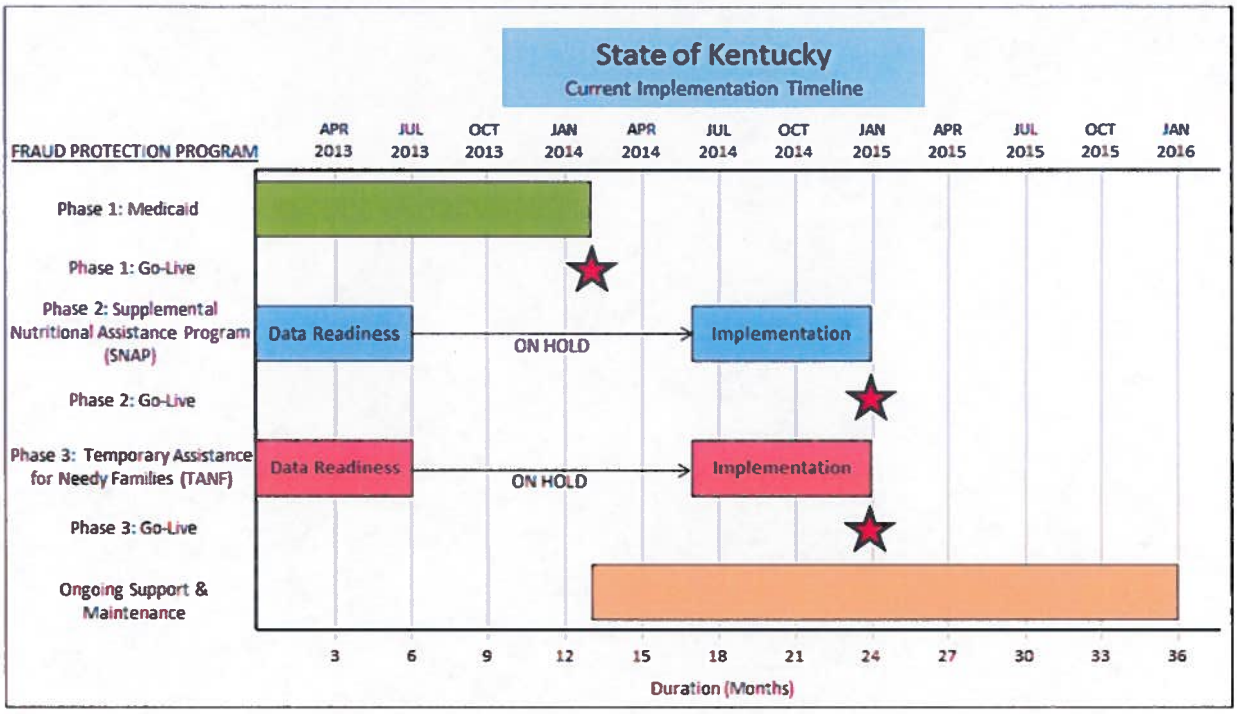


The contract cost for the implementation of the 3 programs included a one-time fee of $4,800,000, plus an additional yearly fee of $864,000 for licensing. Additional fraud programs available with the SAS fraud software solution could be added to the licensing contract for $300,000 each. The current contract will expire in 3 years at which time Kentucky will evaluate whether to continue forward with a contract extension for a hosted solution or explore the benefits and impacts of an in-house licensed solution.

IMPLEMENTATION STATUS

When compared to the original plans, the implementation has proven to be more difficult and complex. Data sharing was a complex issue for the implementation. Memorandums of Understanding (MOU) were issued to gain agreement on the exchange and sharing of confidential data. The MOUs were effective in gaining Agency support, cooperation, and participation on the project.

In order to mitigate State staffing bandwidth risks associated with parallel implementations, the actual implementation plans were revised from the original plans. The Phase 1 Medicaid was started in January of 2013 and full implemented in February of 2014. The data readiness tasks for Phase 2 SNAP and Phase 3 TANF have been completed and the implementation of the fraud analytics will begin in June of 2014 with a targeted implementation date of December 2014.



The project team consisted of State employees and Vendor consultants. With a hosted solution Kentucky has no involvement in the development of the SAS analytical tools. SAS was responsible for developing the software solution. Kentucky was responsible for ensuring that the source data was accurate and verifiable. They worked closely with the vendor team members on data definition and business process use. The State team consisted of twelve (12) full-time equivalents (FTEs) to support the overall implementation. Subject matter experts (SMEs) from the supporting agencies were engaged as required for data readiness activities and tasks.

POST GO-LIVE OPERATIONS

The State of Kentucky continues to operate, support, and use their existing RAC fraud programs in parallel with the new fraud software solution. Thousands of fraud alerts are currently being produced by the new software. Early on, many of these leads are considered false positives and not actionable. The system will require ongoing enhancements and tuning to reduce false positives and develop priority rankings schemes. Kentucky spent dedicated efforts to enable a processes and procedures to prevent duplication and multiple organizations from working on the same cases. The fraud investigators will require time to become familiar with the new tools and fraud scenarios being produced.

Although very early in the overall implementation, Kentucky has reacted to the impacts of the new system and implemented key organizational changes. Six (6) FTEs have been added to the Program Integrity group and Six (6) FTEs have been added to the Inspector General Office. These FTE additions were targeted to support the Medicaid implementation. Additional FTEs are expected to be added for the implementation of the SNAP and TANF programs.

RETURN ON INVESTMENT

Although the new Fraud Prevention System has been live since February of 2014, actual figures associated with return on investment have not been developed. Although Kentucky has a bright outlook on the benefits of the new fraud software solution, they have not had the opportunity to review actual results and determine the impacts and benefits realized from the implementation. Based on their early experiences, Kentucky considers cost recovery very difficult and that cost avoidance is a more effective goal to achieve.

KEY HIGHLIGHTS AND LESSONS LEARNED

Summarized below are the key highlights from the State of Kentucky research.

- The State has implemented a hosted software solution with SAS. State employee bandwidth and bench strength were the key factors supporting this decision.
- The scope of work includes three programs (Medicaid, SNAP, TANF) and a 3 year vendor contract price of $4,800,000. Licensing fees were an additional $864,000.
- The initial timeline for each implementation phase was planned at 13 months.
- It is too early to determine any return on investment. Cost recovery appears to be difficult to achieve. Cost avoidance is a more achievable goal.
- MOUs outlining data sharing agreements was the key element on gaining unwavering participation and collaboration on the project. Do not under estimate the effort and time required to establish these agreements between agencies.
- Enabling a Governance Structure and enforcing Project Management disciplines were important.
- The implementation will require full time support from the State to prepare and verify data used by the analytic software. Staffing impacts must be analyzed closely.
- There is a significant cost associated with investigating and chasing down fraud that has already occurred.
- The fraud prevention programs and processes are an ongoing and require full-time support and focus. Current results have produced thousands of leads with many being false positives that are not actionable. The software will require ongoing enhancement and tuning in order to produce more actionable results.
- Users will require time to become familiar with the new tools, scenarios, and different types of leads being produced.
- There were fewer data issues than expected with the phase 1 Medicaid implementation.
- From a contract perspective, would isolate the data and the analytics portion of the project into two separate efforts. The data readiness portion consumed too much of the overall implementation timeline.

3. State of North Carolina

OVERVIEW

North Carolina has an existing data analytics project named CJLEADS which began as a data sharing effort among criminal justice agencies. The Government Data Analytics Center (GDAC) has been managing the project since 2007. North Carolina reported that they believe most Agencies perform some type of fraud detection through legacy systems and manual business processes.

North Carolina's most recent fraud initiative was launched in the October of 2011 per request from the North Carolina Legislature. GDAC was provided a 2 year window for development of a new fraud analytics solution for the State.

PARTICIPANTS

Outlined below are the people who participated in the North Carolina case study interviews.

- Kay Meyer – Director, Government Data Analytics Center
- Carol Burroughs – Program Manager, NCFACTS

SOFTWARE SELECTION AND CONTRACT PROCUREMENT

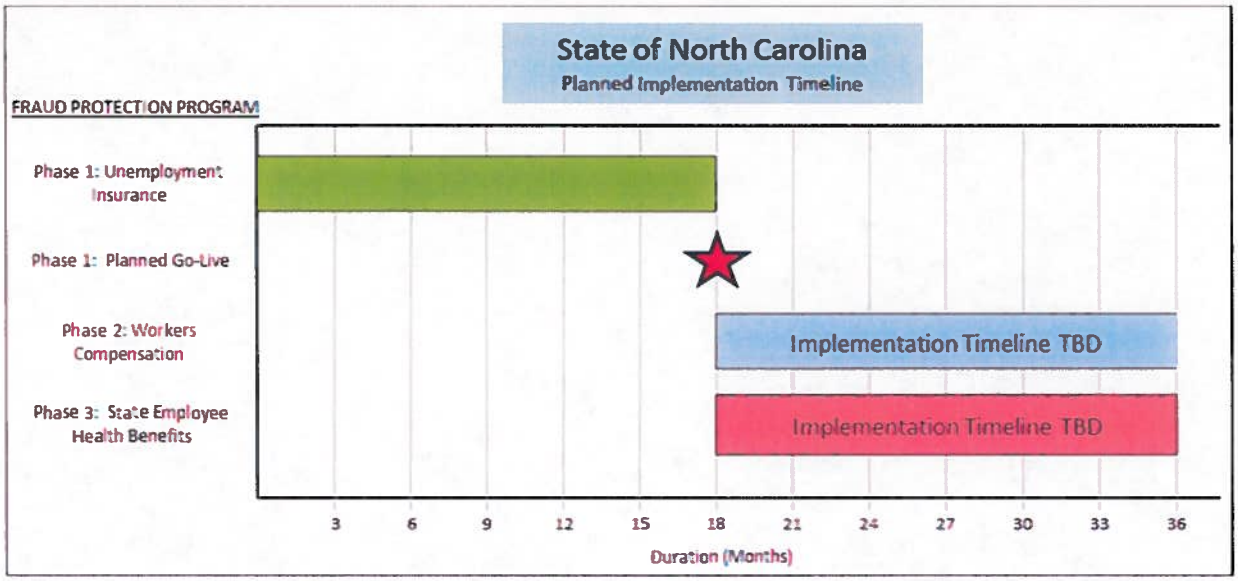
In October 2011, North Carolina GDAC commenced the initiative for additional fraud detection and improper payments. A formal procurement process was not required as North Carolina already had an enterprise license

agreement with SAS and their analytics software solution. The State elected to host the solution with SAS to mitigate risks associated with consistent employee turnover and loss of skills and knowledge to opportunities in the private sector marketplace

Prior to the start of the project, approximately one (1) year was spent marketing the NCFACTS project's purpose and goals to the Agencies to gain support and acceptance. Due to the existing contractual relationship with SAS, the scope of work was very generic and not formally documented. North Carolina eventually developed a phased implementation strategy consisting of the following programs.

- Phase 1 – Unemployment Insurance
- Phase 2 – Workers Compensation
- Phase 3 – State Employee Health Benefits

The implementation timelines included an estimated eighteen (18) calendar months for each program. The implementations will not run in parallel and have been planned to run in sequence in order to mitigate risks with State team member bandwidth and solution complexities.



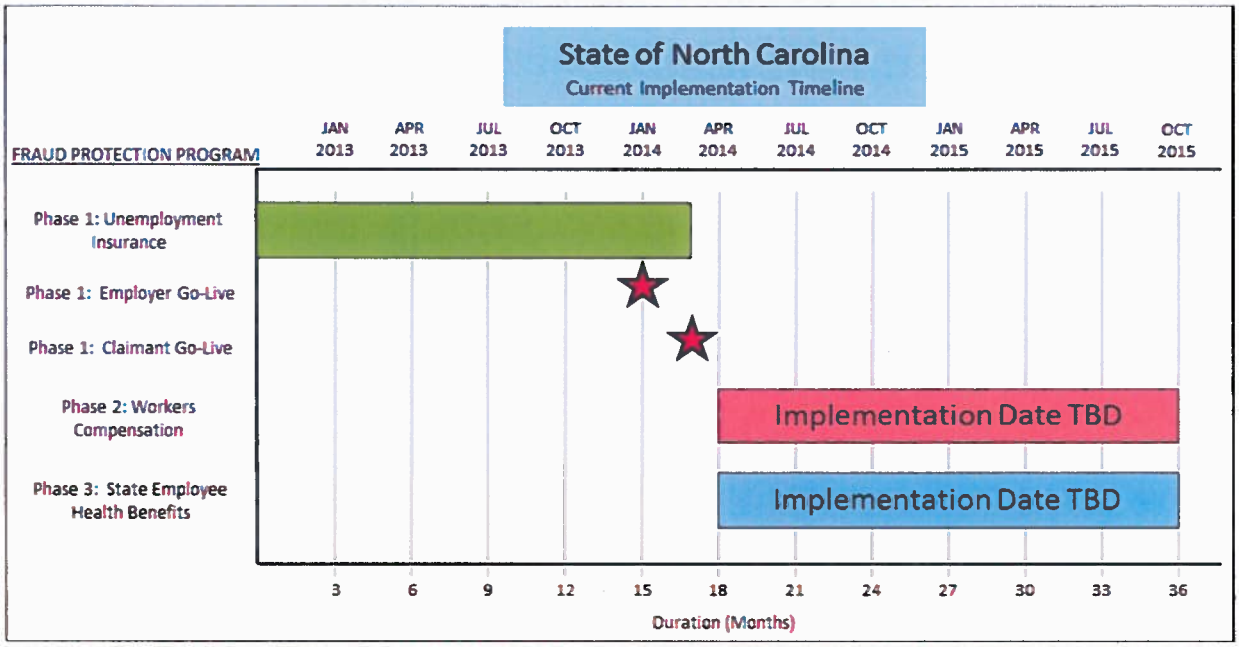
The contract cost for the implementation of the 3 programs included a one-time fee fixed price fee of $8,000,000, plus an additional $1,000,000 for yearly support and maintenance. A fixed bucket of 40,000 vendor hours were established for the hosted contract. The SAS corporate headquarters is based in North Carolina and they invested $5,000,000 into the project themselves. The current contract will expire in 2 years at which time North Carolina will need to negotiate new terms for the hosting agreement.

IMPLEMENTATION STATUS

The State of North Carolina Implemented the SAS Analytics software for Unemployment Insurance (Employer) in 12/2013 and Unemployment Insurance (Claimant) in 02/2014. The overall implementation took approximately 18 months in duration. Requirements gathering and development for phases 2 and 3 are in progress however specific implementation plans have not been finalized.

The implementation was difficult to achieve. Data conversion and cleanup was a painstaking process which was elevated to even greater degrees of difficulty as a result of old mainframe computing systems and lack of State institutional knowledge from both a data and technical perspective.

The diagram below illustrates the planned versus actual implementation timelines for the three (3) project phases.



The key highlights from the ongoing implementation project are outlined below.

- The project requires a significant amount of data governance to determine who owns the data, how it is protected, and how it is used. Data sharing was a complex issue for the implementation. Memorandums of Understanding (MOU) to gain agreement on the exchange and sharing of confidential data.

  Poor legacy system data quality increased implementation timelines.
- The project team consisted of State employees and Vendor consultants. With a hosted solution North Carolina has no involvement in the development of the SAS analytical tools. SAS was responsible for developing the software solution. North Carolina was responsible for ensuring that the source data was accurate and verifiable. They worked closely with the vendor team members on data definition and business process use.
- The State implementation team consisted of a Project Manager and 3 functional data analysts. Support from legacy system owners was also required.

POST GO-LIVE OPERATIONS

The State of North Carolina continues to operate, support, and use their existing fraud programs in parallel with the new fraud software solution. Overall, the volume of alerts has increased and the State end-users are overwhelmed with how to manage and prioritize the work load. Agencies end-users are not experienced with the dashboard data provided by the solution. A significant amount of assistance is required to learn how they should incorporate the new data analytics and leads into their existing fraud related business processes. Although the new fraud program solution has produced duplicates leads already identified through legacy systems, the SAS leads are enhanced and have provided a better understanding of the potential fraud and the depth of investigation required.

Data issues have been another problematic operational issue which has required rework and fine tuning.

The new software solution has improved the data analysis by providing more holistic view of the State data rather than a view from a silo perspective.

The overall support team has grown from four (4) FTEs to ten (10) FTEs.

Although very early in the overall implementation, North Carolina is currently evaluating current business operations to determine areas for improvement on how they manage the fraud alerts. The number of investigators may not need to be increased, however they may need reorganization to be better prepared to support the fraud leads. North Carolina believes additional areas of exposure have been generated as a result of the project as funds need to be returned to the Federal Government before the collection of monies has occurred.

RETURN ON INVESTMENT

Although the new Fraud Prevention System has been live since December of 2013, actual return on investment figures have not been developed. The State has not had the opportunity to review actual results and determine the impacts and benefits realized from the implementation of the new fraud software solution. Based on their early experiences, North Carolina considers cost recovery very difficult and that cost avoidance is a more effective goal to achieve.

KEY HIGHLIGHTS AND LESSONS LEARNED

Summarized below are the key highlights from the State of North Carolina research.

- The State has implemented a hosted software solution with SAS. Mitigating risks associated with consistent employee turnover and loss of skills and knowledge to opportunities in the private sector marketplace was the key factor to implement a hosted solution.
- The initial timeline to Phase 1 Unemployment Insurance was 18 months.
- It is too early to determine any return on investment. Cost recovery appears to be difficult to achieve. Cost avoidance is a more realistic goal.
- MOUs outlining data sharing agreements was the key element on gaining unwavering participation and collaboration on the project. Do not under estimate the effort and time required to establish these agreements between agencies.
- Project Management and Organizational Change Management are required component of the project.
- The implementation will require full time support from the State to prepare and verify data used by the analytic software.
- Do not start the project timeline until clean data is received from the source system data owners.
- Participating Agencies must be committed to the project and make it a priority.
- This is not a technology project. It is a people project.

4. State of Florida

State of Florida: The State of Florida has taken approaches that are similar to other states, where legacy systems provide fraud detection after a fraudulent overpayment has occurred. Florida has been recognized by the Federal Trade Commission as the number 1 state in the nation for identification theft. Florida state agencies are increasing their awareness of and prevention of identity theft by introducing programs designed to prevent fraud before payments are made. The Florida Department of Children and Families (DCF) and the Florida Department of Economic Opportunity (DEO) recognize that payments made as a result of identity theft are rarely recoverable, so an emphasis is placed on prevention.

Florida – DCF: The Florida Department of Children and Families (DCF) implemented the LexisNexis identity management and fraud detection service for all benefits eligibility including Medicaid, WIC, SNAP, TANF and others. This identification service is used to confirm an applicant's identity when applying for benefits by vetting information entered by an applicant against a national database maintained by the vendor. By

avoiding benefit payments to unqualified people, Florida can identify significant savings. The RFI and RFP process resulted in a 3-year contract for $3,000,000. Programming and configuration began September, 2012 and lasted 6 months. DCF staff implemented this functionality on a statewide basis by September, 2013. Avoided payments as of 4/14:

$3,000,000 avoided due to identity theft
$2,300,000 avoided because applicants were identified as deceased
$5,000,000 avoided because applicants were identified as incarcerated
$8,700,000 avoided when applicants opted out

Florida – DEO: The Florida Department of Economic Opportunity (DEO) uses the same identification service as DCF to detect fraud when clients apply for UI benefits. This system has been live since 10/13 and DEO reports a different degree of success. Of the applications identified as possibly fraudulent, 40% are subsequently found to be acceptable candidates. In addition to this effort, DEO created the Fraud Initiative Rating and Rules Engine (FIRRE) using the open-source software, OpenRefine. The decision to use open-source software was based on urgent need and lack of funding. FIRRE was first created as a pilot project. A proof of concept was presented in 4/13 and the design was implemented in 6/13. An Identity Theft Unit was subsequently established. This unit received $1,700,000 to further automate and expand the system. DEO estimates saving $60,000 monthly by preventing fraudulent payments due to use of this system.

IV. Agency Hosted versus Vendor Hosted Solutions

Using an Agency Hosted solution approach, the State will purchase a software license from the Vendor and install the software on State owned computing equipment and infrastructure network. The State is typically responsible for enhancing and maintaining the software, however can secure contract with the Vendor for these services.

Using a Vendor Hosted solution approach, the Vendor retains ownership of the software. The Vendor is responsible for installing the software and performing the required software maintenance. Enhancements to the software are secured through a services contract with the Vendor. The State does not have access to configure the software themselves.

The case study investigation identified three (3) unique reasons leading to a decision on whether to implement an Agency Hosted or Vendor Hosted solution.

1. The State of Michigan elected to purchase a software license for the software and maintain the software themselves. The deciding factor was data ownership and security concerns.
2. The State of Kentucky elected to host the software through the Vendor. This decision was based on the restrictions with State staff bandwidth, bench strength, knowledge, and skillset to support the solution in-house.
3. The State of North Carolina elected to host the software through the Vendor. This decision was made to mitigate risks associated with consistent employee turnover and loss of skills and knowledge to opportunities in the private sector marketplace. North Carolina was concerned that they would not be able to maintain a consistent and knowledgeable level of staff to maintain and enhance the solution themselves.

Each State indicated that cost was not a contributing factor into their decision on whether to license the software themselves or host the software solution with the Vendor.

The table below compares and contrasts the benefits of Agency Hosted and Vendor Hosted fraud prevention and detection solutions.

Measurement	Agency Hosted	Vendor Hosted
Data Ownership	Lower Risk	Higher Risk
Data Security	Lower Risk	Higher Risk
Initial Implementation Cost	Equal	Equal
Initial Implementation Duration	Longer Duration	Shorter Duration
Long-Term Support and Maintenance Cost	Lower Cost	Higher Cost
Required Staffing	Increased State Staffing	Decreased State Staffing

In order to make an informed decision, the State must perform an internal evaluation to determine IT strategic direction and risk adversity levels.

Suggested evaluation criteria would include the following.

- Data Ownership and Security
- Staff Availability
- Staff Skills and Knowledge
- Initial Implementation Costs
- Long-Term Maintenance and Support Costs

V. Findings on Funding Requirements and Law Changes

FUNDING REQUIREMENTS

It is estimated that it will cost between $4.5 and $5.8 million to implement the Fraud Prevention software solution that is recommended in the Case Study. Annual system maintenance costs are estimated at $1.5 million.

In the event that the recommendation is not accepted, estimated costs for the implementation of a Fraud Detection software solution is included in the table below.

Implementation Approach	Initial Implementation Cost	Annual System Maintenance Cost
Fraud Detection Agency Hosted (SNAP, TANF, UI) - 36 Months	$18,985,724	$2,078,908
Fraud Detection Agency Hosted (SNAP, TANF, UI) - 54 Months	$26,673,086	$2,078,908
Fraud Detection Vendor Hosted (SNAP, TANF, UI) - 36 Months	$14,479,224	$2,891,308
Fraud Detection Vendor Hosted (SNAP, TANF, UI) - 54 Months	$18,647,586	$2,891,308

- Cost Figures Represent both Vendor and State Costs to Demonstrate Total Cost of Ownership
- Vendor Costs Estimated between $8 and $12 million are based on Actual Costs from other States with Similar Objectives and are included in the figures above.

- The differences between the low and high implementation costs are caused by the length of time anticipated for implementation

LAW CHANGES

Our research did not identify the need to develop any law changes in order to implement an Enterprise Fraud Program. All States researched in this study did say they had challenges with arranging data sharing agreements necessary for Enterprise Fraud Programs. These States accomplished their data sharing requirements without law changes through the use of a Governor's Executive Order, data sharing agreements, and memorandums of understanding.

VI. Recommendations

Based on the research and investigation performed, the following recommendations are provided for consideration pending the approvals and plans for the State of Arkansas to pursue the procurement of new technology to support the prevention and detection of fraud.

1. In order to support greater collaboration amongst the State Agencies with fraud prevention and detection, it is recommended that a Statewide Fraud Governance Council be implemented to establish overall program policy, develop standards and procedures for data security and authorized data use, and guide the strategic direction for program growth and enhancement.
2. The Case Study did not focus on the features and functions of software solution options in the fraud prevention and detection marketplace. It is recommended that the State implement an extensive procurement process beginning with an RFI to gain an understanding of the solution options that are available.
3. In order to prevent schedule delays and vendor cost impacts, it is recommended that data sharing agreements amongst the State Agencies be developed and enabled prior to starting implementation activities.
4. In order to avoid staffing constraints and solution deployment complexities, it is recommended that the implementation plan reflect a sequential deployment of the pilot programs rather than a parallel or overlapping deployment of the pilot programs.
5. Business Operations will need to be evaluated for change. The new system will provide investigators with different types of fraud leads to research. The investigators will require time to become familiar with the new tools and fraud scenarios produced. It is recommended that a thorough Organizational Change Management program be developed and enabled as part of the project.
6. The implementation of new fraud technology will have an impact from both a support and use perspective. The new technology will require State personnel to support it. The new technology will generate additional fraud alerts that must be researched. In order to effectively manage and use the new technology, it is recommended that the State be prepared to perform an impact analysis for additional State positions.
7. Recovering monies from actual fraud that has been detected is challenging. There is a significant cost associated with investigating and chasing down fraud that has already occurred. Fraud prevention through identity management during front-end business processes is a recommended starting point for fraud technology.