DATA ANALYTICS FOR PAYMENT ACCURACY, PROGRAM INTEGRITY & EFFICIENCY

BEST PRACTICES IN GOVERNMENT
GREG HENDERSON, SAS SECURITY INTELLIGENCE PRACTICE
TOPICS

- Key Trends
- Enterprise Approach
- Hybrid Detection Analytics
- Operationalizing Analytics
“More people tolerate fraud and are softer about punishment”. The coalition estimates **$80 Billion in US insurance fraud annually**.

The General Accounting Office (GAO) estimates that fraud in healthcare ranges from **$70 billion to $700 billion per year**. Others experts estimate anywhere between **3% and 10%** of the $2 trillion heath care budget.

The General Accounting Office (GAO) estimates that fraud in healthcare ranges from **$70 billion to $700 billion per year**. Others experts estimate anywhere between **3% and 10%** of the $2 trillion heath care budget.

July 22, 2010, President Obama signs the Improper Payments Elimination and Recovery Act (IPERA) which will help **reduce wasteful, improper payments by $50 billion** between by 2012.
THE IMPACT OF FRAUD ON GOVERNMENT

TOTAL DEFICIT = $8.6 TRILLION

U.S. Federal Budget Surplus/Deficit
FY2000-2014

SOURCE: www.whitehouse.gov/omb/budget/historicals
THE IMPACT OF FRAUD ON GOVERNMENT

TOTAL DEFICIT = $1.5 TRILLION

U.S. Federal Budget Surplus/Deficit FY2000-2014

KEY TRENDS

- **Schemes and Methods**
  - Far more sophisticated, organized, patient, share info
  - Engage insiders to understand detection environment
  - Hit multiple program areas at the same time
  - Continuously evolve strategies

- **Current Controls**
  - Silo’d by fraud type and program – no sharing of data
  - Focus primarily on transaction data – no holistic view
  - Rely on rules and basic outlier detection
  - Detection focused – not proactive
# Improper Payments

## Key Trends

- **Reducing cost** of combating fraud, abuse and improper payments: 68%
- Increasing **agility** to deal with new types of fraud and abuse: 62%
- **Improving efficiency and ROI** auditor/investigator: 61%
- Enabling personnel to address problems **ahead of payments**: 60%
- **Reducing improper payments** and setting more accurate target loss rate: 60%
- Increasing payment integrity **without harming process performance**: 59%
- Gaining **enterprise view of fraud**, abuse and improper payment risk: 57%
- **Predicting** the likelihood of fraudulent events or behavior: 56%
- **Eliminating false positives** and improving focus on outliers: 52%
- Using information to collaborate across federal, state and local agencies: 51%

Source: TechWeb Research  
322 respondents working in Federal, state or local government
PAYMENT INTEGRITY

BEST PRACTICE 1: ENTERPRISE APPROACH

- Leverage enterprise data for improved detection
- Provide a common platform for fraud detection, prevention and investigation across all program areas
- Increase agility and decrease costs
ENTERPRISE APPROACH

COMMON DATA ACCESS LAYER

CONSOLIDATED VIEW OF DATA FOR CROSS-PROGRAM AUDIT / DETECTION

Injured Worker  Unemployment  Health Care  Welfare  Food Assist  Tax / Revenue  License & Register  Justice  Housing

DATA

GOVERNMENT PROGRAMS

CITIZEN JOHN DOE
ENTERPRISE APPROACH

COMMON TECHNOLOGY PLATFORM

COMMON TECHNOLOGY FRAMEWORK

CONSOLIDATED VIEW OF DATA FOR CROSS-PROGRAM AUDIT / DETECTION

GOVERNMENT PROGRAMS

DATA

DATA

INJURED WORKER

UNEMPLOYMENT

HEALTH CARE

WELFARE

FOOD ASSIST

TAX / REVENUE

LICENSE & REGISTER

JUSTICE

HOUSING

CITIZEN JOHN DOE
ENTERPRISE APPROACH

COORDINATED INVESTIGATIONS

Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit

COMMON TECHNOLOGY FRAMEWORK

CONSOLIDATED VIEW OF DATA FOR CROSS-PROGRAM AUDIT / DETECTION

Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit
Investigative Unit

DATA CONSOLIDATED VIEW OF DATA FOR CROSS-PROGRAM AUDIT / DETECTION

GOVERNMENT PROGRAMS

Injured Worker
Unemployment
Health Care
Welfare
Food Assistance
Tax / Revenue
License & Register
Justice
Housing

CITIZEN JOHN DOE

DATA
DATA

Copyright © 2012, SAS Institute Inc. All rights reserved.
CASE STUDY

LOUISIANA ENTERPRISE FRAUD INITIATIVE

Highlights

• First state to institute a state-wide approach to fighting fraud
• Initially focused on Unemployment Insurance
• “Quick Start” methodology resulted in $12M in identified savings within first 100 days

Business Problem

The LA Workforce Commission was faced with the challenge of uncovering employer and employee workers compensation fraud. For employers, that often takes the form of misclassification of employees to avoid paying appropriate premiums. For employees, it can be collecting disability compensation while working somewhere else. Future target areas include fraud in insurance, child care and Medicaid and the identification of waste and improper payments, which are not necessarily criminal.

Approach

Louisiana will use software from SAS, to crack down on fraud and reduce waste and improper payments. By reducing fraud losses, the state can save money, create a more favorable economic environment, while protecting workers.

SAS software, including the SAS Fraud Framework for Government, will eventually be available to all state agencies. However, the initial phase of the project will target fraud within the Workers Compensation and Unemployment Insurance programs of the Louisiana Workforce Commission.

Results

In less than 100 days, LA Workforce Commission identified and recovered over $1.2M in unpaid premiums, and identified over $12M of additional evaded premiums.
BEST PRACTICE 2: ADVANCED ANALYTICS APPROACH

- Combine multiple analytic techniques into aggregate entity level risk scores
- Allows for reduction of both false-positives and false negatives
  - Different techniques detect different kinds of behavior
  - Aggregating results provides checks and balances
- Sophisticated schemes require sophisticated analytics
- Prioritize alerts to investigators are working the most high value cases first
PAYMENT INTEGRITY  

HYBRID ANALYTICS

Enterprise Data

Suitable for known patterns

Rules
Flag improper claims based on known abuses
Examples:
- DRG/CPT Mismatch
- Procedure not appropriate for demographic
- Unbundling
- Deceased recipient or provider

Suitable for unknown patterns

Anomaly Detection
Detect individual and aggregated abnormal behaviors
Examples:
- Excessive claims compared to peers
- Bill amount consistently exceeds norm
- Unusual driving distances for specialty
- Abnormal volume of upcoded procedures

Suitable for complex patterns

Predictive Models
Predictive assessment against known fraud cases
Examples:
- Billing patterns similar to known fraud cases
- Predicted diagnosis does not match actual
- Like provider/network growth rate (velocity)
- Unexplained change in behavior

Suitable for associative link patterns

Link Analysis
Knowledge discovery through associative link analysis
Examples:
- Provider association to known fraud
- Collusive provider / supplier relationships
- Suspicious referrals to linked providers
- Linked suspicious addresses or phone

Providers | Recipients

Facilities | Claims

Referrals | Audit Flags

Intra-Agency | 3rd Party Data

Hybrid Approach
Proactively applies all 4 techniques at provider, recipient, facility, and network levels
PAYMENT INTEGRITY

HYBRID ANALYTICS

Opportunistic / Mistakes

Average Fraud & Improper Payments

Criminal Offender

Organized Criminal Gangs

Business Rules

Anomaly Detection

Predictive Models / Advanced Analytics

Social Network Analysis

Text Mining

The Tentatives

Mistakes

Systemic Issues

Revenge Seekers

Game Players

Exploiters

High Volume Low Loss

Low Volume High Loss
**CASE STUDY**

**LOS ANGELES COUNTY DEPT OF SOCIAL SERVICES**

**Business Problem**

The Department of Social Services of a large US County was being hit by fraud, waste, and abuse across their public assistance programs. The County engaged SAS to pilot the SAS Fraud Framework to determine if the data analytics and visualization solution could assist in proactively detecting both opportunistic and organized fraud in the Childcare program.

**Approach**

SAS subjected 6 years of historical data from 5 different source systems (including claims, payments, application, 3rd party, and fraud case data) to the predictive capabilities of the SAS Fraud Framework. Client investigators evaluated the solution results during a 3 week validation period against 3 main categories of cost avoidance: investigative efficiency, earlier detection of fraudulent providers & participants, and incremental detection of fraudulent providers & participants.

**Results**

The pilot resulted in a business case and deployment roadmap for full implementation,

- **Investigative Efficiency:** $3.0M (saved across 40 investigators)
- **Earlier Detection:** $1.6M
- **Incremental Detection:** $26.5M
TAX FRAUD  BELGIAN TAX AUTHORITY

CHALLENGES

• VAT Carousel Fraud causing annual losses of €1B+
• Organized fraud rings increasing
• High velocity attacks resulted in large losses quickly
• Overwhelmed with data
• Limited investigative resources

SOLUTION (SAS® Fraud Framework For Government™)

• Utilized Hybrid Analytics and early detection techniques on enterprise data to detect and disrupt fraud rings faster

PROFILE

• 600,000 taxpayers
• 500,000 tax returns
• 24,000,000 transactions
• 27 EU Countries
• 600 Investigators
TAX FRAUD  BELGIAN TAX AUTHORITY

PRELIMINARY RESULTS
• Decreased carousel fraud losses by 98%
• Estimated savings of €1B+ per year
• 80% accuracy on analytical models
• Ultra-early detection prevents most losses and avoids recoveries
• Substantial increase in investigator productivity

NEXT STEPS
• Improved data sharing amongst EU member states
• Expand into other tax areas
• Continue to refine and improve analytical models

APPROACH
• Utilize all available data about companies
• Apply rules, anomaly detection, predictive models and network analysis
• Sophisticated non-linear score aggregation
• Optimize resources through case prioritization and automation
BEST PRACTICE 3: OPERATIONALIZE ANALYTICS

- Prevention vs. Detection
- Continuous Monitoring vs. Random Audits
- Process Efficiency
  - Better Leads / Alerts
  - Case Prioritization
  - Streamlined Investigation Tools / Processes
PAYMENT INTEGRITY

OPERATIONALIZE ANALYTICS

Alert Generation Process

- Business Rules
- Alert Administration
- SAS® Social Network Analysis
  - Network Rules
  - Network Analytics

Analytics
- Anomaly Detection
- Predictive Modeling

Learn and Improve Cycle
- Case Management
- Alert Management & BI / Reporting

Intelligent Fraud Repository

Exploratory Data Analysis & Transformation

Fraud Data Staging

Operational Data Sources
- Transactions
- Entities
- Internal Data
- External Data

Operational Data Sources
- Staging
- Intelligent Fraud Repository

Operational Data Sources
- Data Sources
- Data Analysis & Transformation

Operational Data Sources
- Data Sources
- Data Analysis & Transformation
Business Problem

State provides coverage for more than 2.5 million workers employed by 171,000 employers. Employer fraud and abuse occurs when employers underreport hours, report hours in an improper risk class with lower premium rates, or don’t register or pay at all. L&I audits employers' business records to make sure they report accurately and pay the premiums owed. The audit function is core to determining where abusive or fraudulent behavior is taking place across a workers' compensation system that collects premiums and pays out over $1.4 B annually.

Approach

The solution is used to detect employers that are evading payment of workers compensation taxes for their employees. SAS Fraud Framework for Government is a part of the Department’s fraud solution for workers compensation premium evasion. The SAS Fraud Framework solution was developed out of the successful proof of concepts of several other state fraud detection implementations.

Results

SAS Solutions OnDemand is working to consolidate 30 different data sources and create a single view of employers to better analyze, detect and combat workers’ compensation fraud. The Department conservatively estimates a savings of $11 million to $14 million in the first year of recovered premiums.
CASE STUDY  US INTERNAL REVENUE SERVICE

Business Problem

IRS needed a robust system to assist with their capabilities to detect, resolve and prevent criminal and civil non-compliance which would reduce the tax gap and be line with the IRS enterprise architecture.

SAS Approach

The SAS Fraud Framework for Tax will use data mining and modeling, predictive analytics, fraud scheme detection, real-time fraud scoring, workload management and work stream identification based on fraud score card analysis, as well as the ability to incorporate real-time business rule changes.

Highlights

• Reduce the issuance of fraudulent tax refunds.
• Discover new types of fraud, including criminal fraud rings using social network analysis.
• Increase collections and close the tax gap.
• Dashboard reporting and case management integration

Results

• The IRS Return Review Program (RRP) is using the SAS Fraud Framework is an upstream system for the IRS’ Customer Account Data Engine (CADE), the system that processes individual and business tax returns.
• RRP is used to maximize fraud detection at the time tax returns are filed to eliminate the issuing of questionable refunds. Tax filings are the input for the RRP, and the system's output is sent to different work streams, from audit analysts to various case management systems.
• Tax credit fraud amounts to roughly $20-30 billion. Frequent instances of this type of fraud range from child adoption or earned income tax credits to ghost tax return preparers. For the latter, social network analysis can help identify ghost preparer fraud rings by building probabilistic models.
CLOSING THOUGHTS

- Sophisticated schemes require sophisticated detection techniques
- Taking an enterprise approach greatly enhances detection and provides economies of scale
- Improper payment detection and prevention needs to be an integrated part of the operational process
- Investigators need to be equipped with modern technology to maximize efficiency and effectiveness
FRAUD AND SECURITY INTELLIGENCE

QUESTIONS?
QUESTIONS?