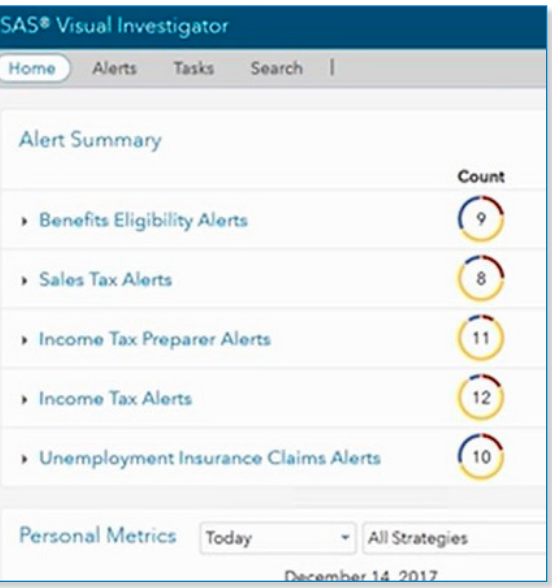
SAS® Detection and Investigation for Government



Governments, like all organizations, are vulnerable to fraudsters who attempt to cheat and abuse the system. Each year, billions of tax revenues paid by hardworking citizens are lost due to fraud, abuse and improper payments.

These payments have a real impact – hundreds of billions of dollars in the US alone. Fraud, waste and abuse spending at the US federal level increased from $137 billion in fiscal year 2015 to $144 billion in fiscal year 2016, with Medicare and Medicaid leading with $66 billion in 2016.[1] In the UK, applying a global average loss rate to GDP would imply total losses of GBP 125 billion (US$176 billion) each year. Reducing such losses by 40 percent would free up more than GBP 50 billion each year. This sum is more than the UK government spent on defense or education in 2016.[2]

Directives aimed at increasing the transparency of improper payments (for instance, in the US government) state that when the government makes payments, it must make every effort to confirm that the right recipient is receiving the right payment for the right reason at the right time. Unfortunately, the methodologies typically employed by government agencies to detect fraud and reduce improper payments are not keeping pace with fraudsters' tactics.

The nature of government programs requires collecting and processing enormous amounts of information. One of the biggest challenges for these systems is the integrity of the data itself. Data authentication, verification, standardization, integration and matching are required first steps to implementing an effective analytical fraud, waste and abuse solution. Without a trustworthy, single version of the truth, auditors and analysts cannot adequately protect government funds from improper payments.

The Solution

SAS Detection and Investigation for Government helps governments detect and prevent both opportunistic and professional fraud through improved data effectiveness and analytics. You can standardize, integrate and authenticate data and consolidate program integrity activities. By harnessing your quantitative and qualitative data, you can better identify fraudulent activity and stop payments before they're made.

Analytics helps government investigators identify abnormalities and patterns that may indicate fraudulent activity, for instance, by finding patterns and aberrations using visualization and analysis techniques. SAS calculates the propensity for fraud at each stage of a process with a fraud analytical engine that uses multiple techniques, including:

- Automated business rules.
- Predictive modeling.
- Machine learning.
- Text mining.
- Search and discovery within databases.
- Exception reporting.
- Network link analysis.
- Artificial intelligence.

---

1 Adelaide O'Brien, *Moving Beyond Recovery to Prevention in Fraud and Abuse in Federal Programs*, IDC, September 2017.

2 *The Financial Cost of Fraud 2017*, Crowe Clark Whitehill.

With SAS, an online dashboard of key indicators and statistics provides access to information on improper payments, such as payment error rates by agency and program, and listings of the most egregious offenders. The solution routes alerts for potentially fraudulent activities to integrity teams, where investigators use case management tools to rapidly investigate. Once investigators score and prioritize activities based on severity, they may perform a more in-depth review of activity characteristics (including any associated historical activities) to decide if an activity is fraudulent.

The SAS solution is an end-to-end framework for detecting, preventing and managing all types of improper payments. It includes components for detection, alert management and case management, along with a category-specific workflow, content management and advanced analytics that uses machine learning, artificial intelligence and social network analytics. The SAS approach provides enhanced fraud detection and improved operational efficiency while decreasing false positive alerts.

Benefits

Detect fraudulent activity more precisely

- Insert analytical models into the process, in addition to rules engines.
- Process all transactions (not just a sample) through rules and analytical models.

Apply machine learning and artificial intelligence

- Use customized models to detect previously unknown schemes.
- Spot linked entities and crime rings, which can help stem larger losses.

Decrease fraud losses

- Prevent fraud before payments are made using online, real-time scoring.
- Detect repeat offenders and more accurately score fraudulent activity by searching databases of known fraudsters and capturing all fraud outcomes, referrals and suspects.
- Detect insider or collusive behavior by integrating staff data and audit records that show who handled which transactions.

Reduce costs to detect and investigate fraud

- Greatly reduce false positives.
- Improve investigation efficiency with advanced case management tools.
- Increase ROI per investigator by prioritizing higher-value networks and conducting more efficient and accurate investigations.

Gain a consolidated view of fraud risk

- Improve models on an ongoing basis and adapt the system continuously to address changes in fraud trends.
- Better understand new threats and prevent substantial losses early using social network diagrams and sophisticated data mining capabilities.

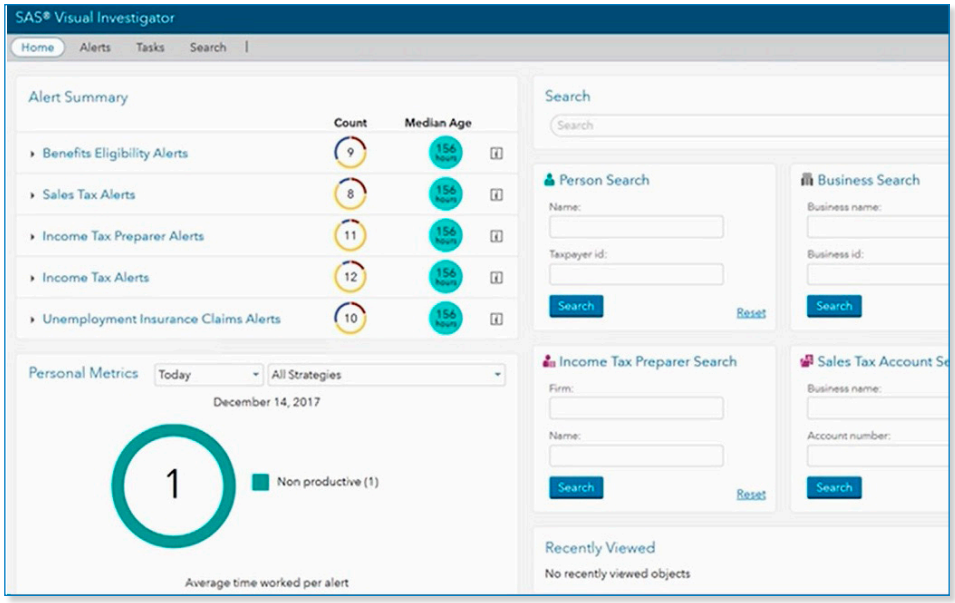
Improve transparency and increase accountability

- Measure – not estimate – your improper payment rates precisely, and determine how they change over time.
- Build sophisticated detection models that are easy to understand and explain.

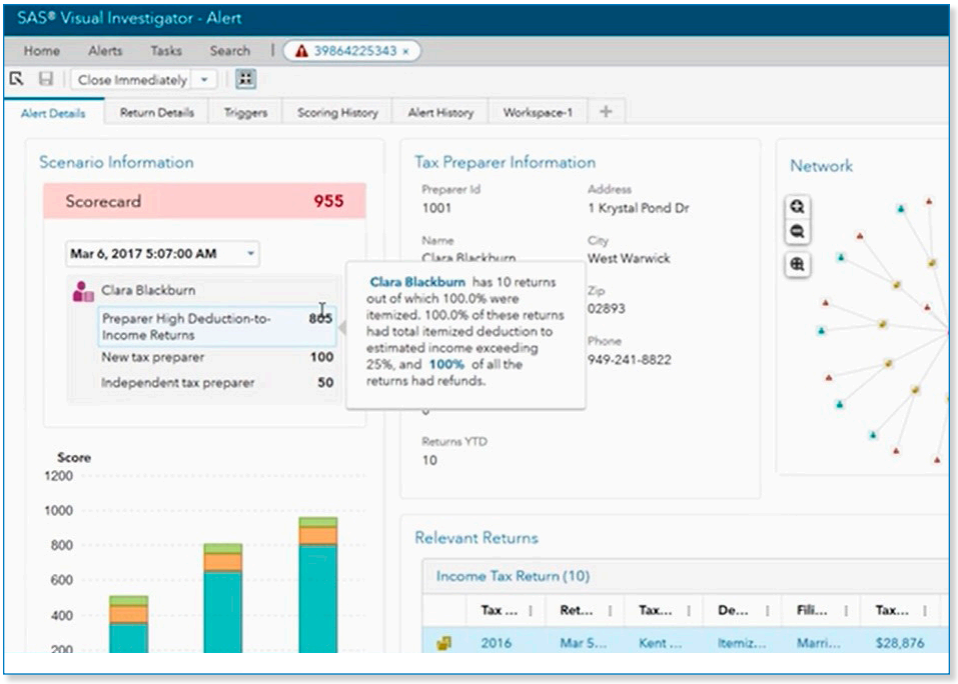
Capabilities

Data integration and business rule deployment

Data is the lifeblood of any fraud solution. SAS Detection and Investigation for Government can extract relevant data from different systems, unstructured text and third-party data sources. It can also import business rules for known fraud, waste and abuse schemes from existing rules engines.



Fraud alert summary screen.



Drill down into details of fraud alerts.

Search and discovery

The solution gives you the freedom to perform free-text, field-based or geospatial searches across all data (internal and external).

- Refine searches using interactive filters and facets that are built for investigators.
- Build complex queries through an intuitive interface without the need to understand programming. For example, use fuzzy searching, proximity searching and field boosting while restricting searches to specific entity types, fields, comments or insights.

Advanced analytics, machine learning and AI, and model deployment

SAS enhances the value of existing business rules by enabling the discovery of emerging suspicious activity that would otherwise go undetected. Activities identified as suspicious are scored using advanced predictive modeling techniques. The resulting scores are then used to prioritize the order in which suspicious transactions should be investigated. By deploying review capabilities as early in the payment process as possible, you can maximize your ability to stop fraudulent or abusive transactions before payments are made.

- Improve fraud models by testing different approaches in a single run and comparing results of multiple supervised learning algorithms with standardized tests. This helps to reduce false positives.
- Analytical capabilities include clustering, several types of regression, random forests, gradient boosting models, support vector machines, natural language processing, topic detection and more.
- Continuous improvement emerges from previous output results.

Detection and alert generation

These components enable the systematic detection of suspicious activity using a fraud scoring engine that employs a combination of analytic techniques to determine the likelihood of fraud. The detection and alert components:

- Score transactions in real time with an online scoring engine that lets you detect fraudulent activity using a combination of business rules, anomaly detection and advanced analytical techniques.
- Use historical data to gain a deep understanding of behavior, allowing you to determine if a payment makes sense in the context of past actions.

Alert management

The alert management component assembles alerts from multiple monitoring systems, associates them with common individuals and provides investigators with a more complete perspective on the risk of an individual. It also includes:

- Risk score calculation: Each alert is assigned a risk score based on the specific characteristics of the activity, with transparent reason codes.
- Alert prioritization: Prioritizes and routes potentially fraudulent transactions to appropriate team members, resulting in greater efficiency, increased detection rates and reduced losses.
- Work assignment: Auditors can appoint automated alert assignments to various investigators or analysts based on rules and requirements set by the user.

Social network analysis

Investigators can detect and prevent organized fraud by going beyond individual transaction and account views to analyze all related activities and relationships at a network dimension. In addition, the solution:

- Improves investigator efficiency: Produce complete dossiers of networks surrounding a case using an intuitive interface that provides fast access to all details, related parties and networks.
- Uncovers previously unknown relationships: Using a unique network visualization interface, the solution gives investigators the ability to identify linkages among seemingly unrelated claims.
- Produces independent and combined fraud scores: Assess overall risk on an individual, claim and/or network basis.

Intelligent case management

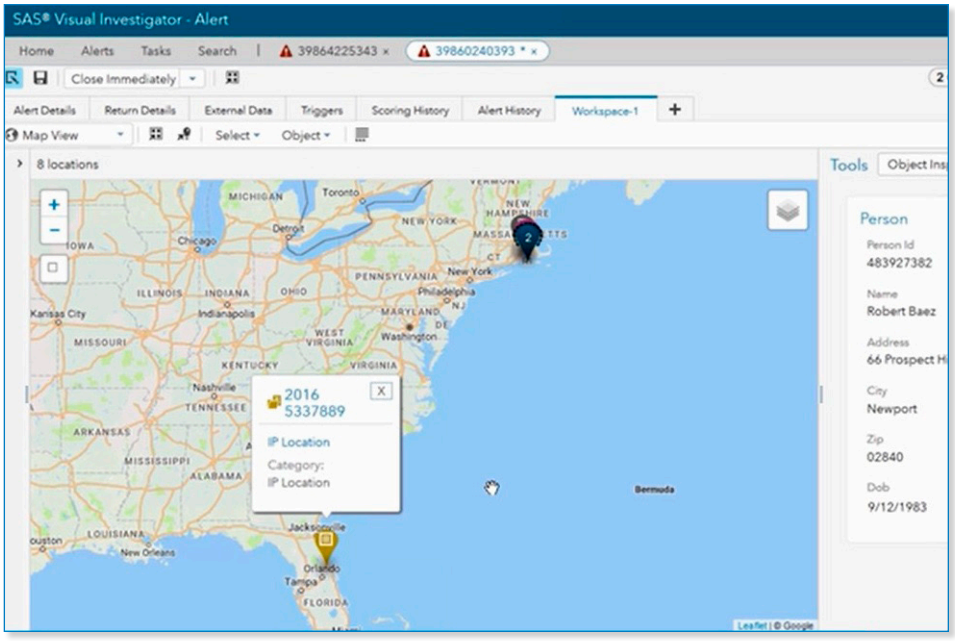
Once an alert has been triaged and requires further investigation, the case management functionality provides a systematic means to investigate, capture and display all information pertinent to a case. You can:

- Store fraudulent activity information, including interview notes and evidence needed for criminal or civil prosecution, restitution and collections.
- Assess your overall fraud exposure, including losses due to fraud, as well as fraud detected or prevented.
- Use a configurable workflow for the management and resolution of cases.

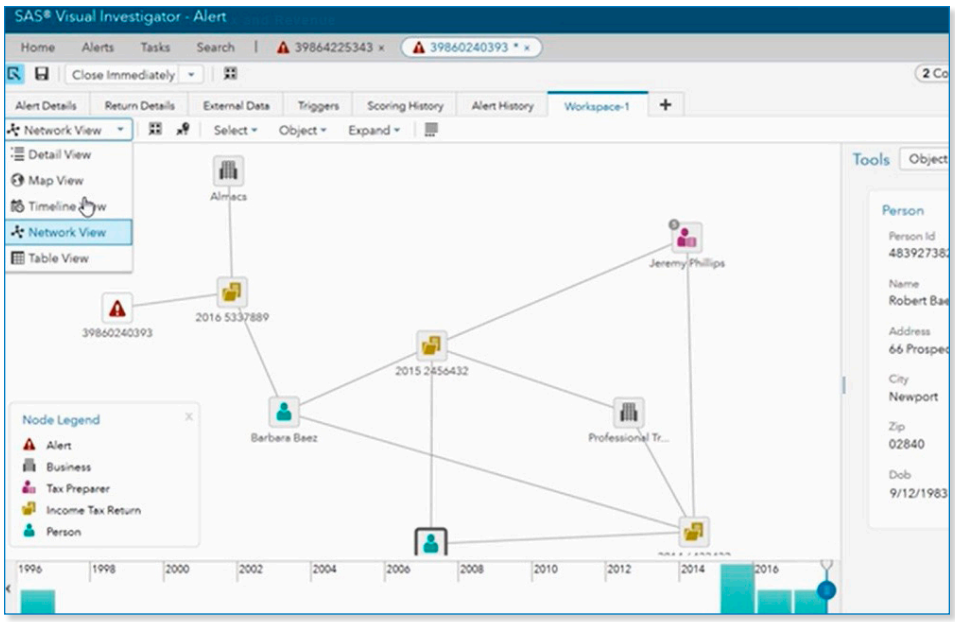
Hosting and analytical services

SAS offers complete hosting services, with the solution installed and administered at the SAS hosting site, eliminating the need for your staff to oversee the system. This deployment method typically has a faster implementation period, translating into faster and more significant ROI. If you prefer to install and host the solution on-site, SAS will assist with the implementation and provide industry-leading training.

To learn more about SAS Detection and Investigation for Government, download white papers, view screenshots and see other related material, please visit sas.com/detect-investigate-gov.



Use geospatial analysis to detect suspicious transactions.



Identify networks of behavior and how they change over time.

To contact your local SAS office, please visit: sas.com/offices