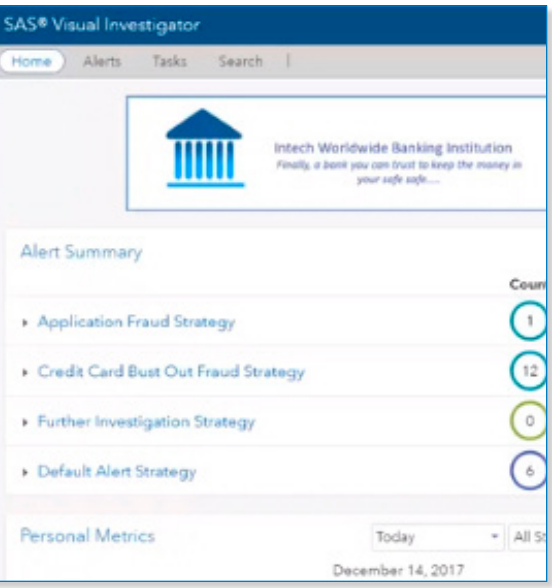
# SAS® Detection and Investigation for Banking




Fraud risk is escalating for banks and others providing financial services. Besides the proliferation of data breaches, consider the growing number of mobile devices generating banking transactions. New product offerings and technology advances present new risks – such as chip and pin technology for credit and debit cards. The advent of the chip card has ushered in a significant reduction in card fraud at point of sale, but brought a corresponding increase in card not present (CNP), digital and application fraud – especially using synthetic identities.

Much of the fraud perpetrated through false identities is difficult to detect, since synthetic identities create new transactional and customer profiles. The size of the fraud problem may be underestimated as many of these losses – especially those associated with synthetic identities – are charged off as a credit loss as opposed to a fraud loss.

Transaction monitoring has been a standard approach to detecting fraud for many years, but the nature of fraud in the era of data breaches and online anonymous banking has changed the rules. Increasingly, it's critical to detect a fraudster as early as possible in the relationship as identities and patterns are being created. Hence the need to use external public record data, network analytics and sophisticated models to identify criminals before they develop strong personas.

Unfortunately, few banks and other organizations opening relationships and doing business with customers via the internet have good tools, processes and procedures to ensure the identity of customers. Overall, addressing this type of fraud requires an expanded use of data, new rules and models, and a multilevel approach to fraud detection and prevention. Using a solution that can provide the technology and analytics to address all types of fraud becomes an appealing opportunity, allowing for more sophisticated detection methods, reduced costs and increased efficiencies.

## The Solution

SAS® Detection and Investigation for Banking is an end-to-end solution for detecting and preventing organized and first-party fraud. As part of SAS Enterprise Financial Crimes for Banking, the solution provides enhanced fraud detection and improved operational efficiency while decreasing the total cost of ownership.

The solution takes a unique, hybrid approach, using multiple techniques – automated business rules, predictive modeling, text mining, database searches, exception reporting, network link analysis, etc. – to detect and prevent fraud at the individual transaction, account, customer and/or network level. The solution gives you the distinct ability to uncover subtle or hidden relationships among entities that alone may seem innocuous, but when viewed at a network level may indicate first-party, bust-out fraud or associate collusion.

It scores and prioritizes alerts based on severity, then routes them to investigation units, where investigators can perform more in-depth reviews to determine if the transaction or any associated historical transactions are fraudulent. And we give you the flexibility to configure the system to meet your specific needs, as well as update models and adapt the system to address changes in fraud trends whenever necessary.

The solution includes:

- The power and scalability to handle large volumes of data.
- A category-specific workflow.
- Rapid model development and deployment capabilities, and the ability to update and refresh models and business rules as needed.
- Content management capabilities.
- Advanced analytics, including machine learning, artificial intelligence, text analytics, data mining and link analysis.
- A network visualization interface.
- Integration with an optional case management system.

## Benefits

### Detect more fraudulent activity and decrease losses due to fraud

- Process all data (not just a sample) through business rules and analytical models in real time or in batch so you can spot more suspicious activity with greater accuracy.
- Using machine learning and AI methods, uncover previously unknown fraud schemes.
- Detect repeat offenders and more accurately score incoming transactions by searching databases of known fraudsters and capturing all fraud outcomes, referrals and suspects within the system for reuse.
- Spot linked entities and crime rings – which can help stem larger losses – using a unique network visualization interface.
- Overcome poor data quality issues associated with imperfect matching and highly linked entities.
- Uncover application and online banking fraud using device data in conjunction with demographic data.

### Reduce false positives while increasing investigator efficiency

- Prioritize events before presenting to investigators by applying risk- and value-based scoring models.
- Enable investigators to work cases more effectively and focus on higher-value networks, which generate a higher ROI.
- Make the collection process more efficient by identifying those losses resulting from synthetic identities that have minimal or no chance of reconciliation.

### Gain a consolidated view of fraud risk

- Identify cross-brand/product fraud by seeing customer accounts and transactions for all lines of business.
- Stay on top of changes in fraud trends by improving models on an ongoing basis and continuously adapting the system.
- Better understand new fraud threats and prevent substantial losses early using social network diagrams and sophisticated data mining capabilities.

### Gain greater competitive advantage

- Provide legitimate customers with a better experience through fewer false positives for greater customer satisfaction.
- Discourage fraudsters from targeting your organization by employing more diligent and effective fraud detection methods.
- Satisfy greater regulatory demands with enhanced fraud management.

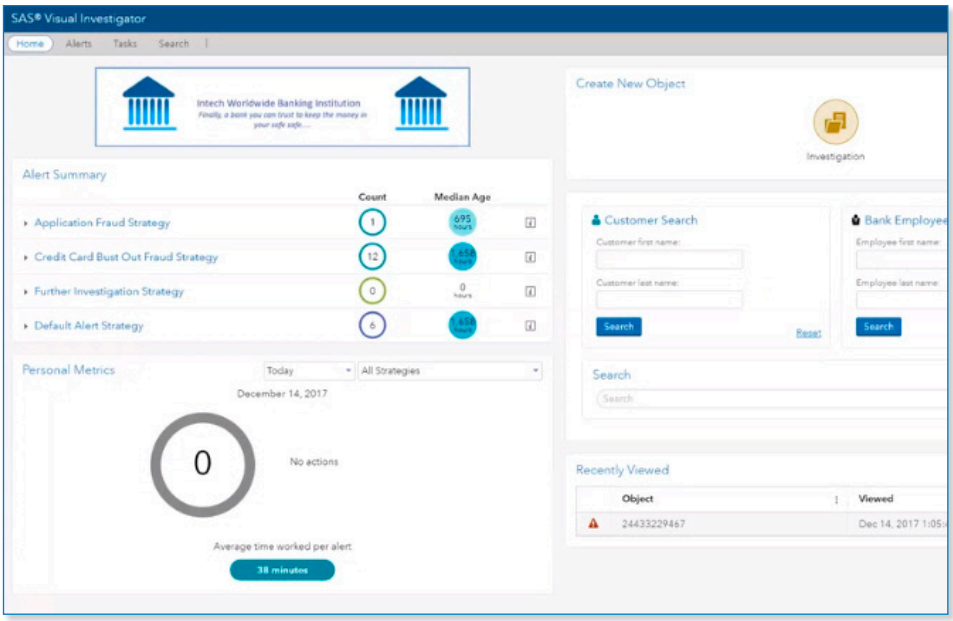
## Capabilities

### Data management

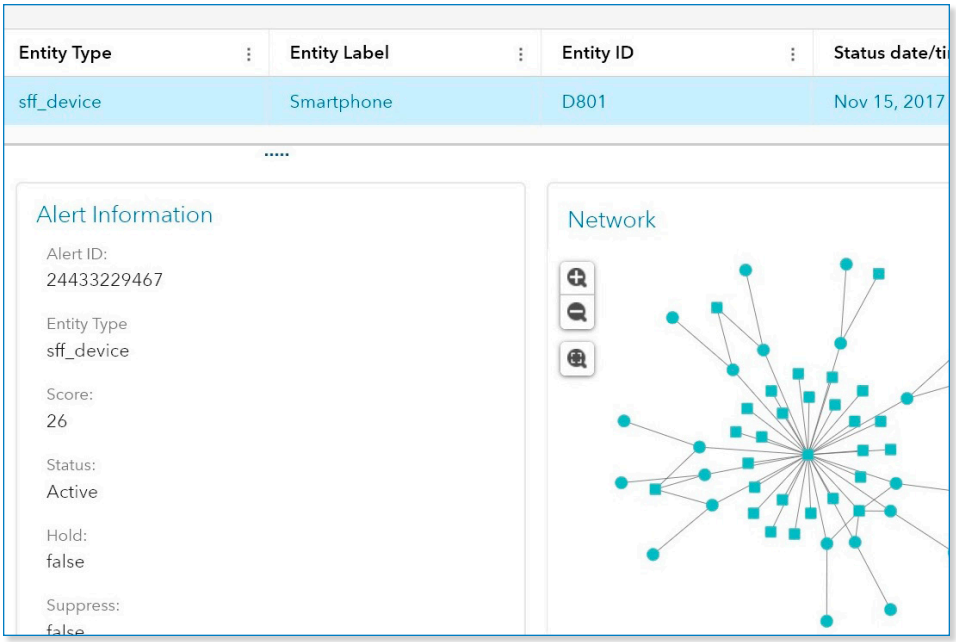
- Consolidate historical data from both internal and external sources for fraud analysis and investigation.
- Reduce or eliminate data inconsistencies or redundancies with automated, built-in data quality tools.
- Integrate the system seamlessly with third-party fraud applications.

### Rule and analytic model management

- Logically manage rules, models and alerts for investigators.
- Create and manage business rules, analytical models and known fraudster lists.
- Maintain simple or complex routing and suppression rules.




Alert summary home page.




Details of alert scorecard.

## Detection and alert generation

- Score transactions in real time with an online scoring engine that uses a combination of business rules, anomaly detection and advanced analytic techniques.
- Calculate the propensity for fraud at account opening, then rescore accounts with each transaction as new data gets captured.
- Go beyond fraud detection by deploying fraud analysis at account opening to prevent fraudsters from opening accounts in the first place.

## Alert management

- Assemble alerts from multiple monitoring systems, associate them with common accounts, and give investigators a holistic perspective on the risk of a particular account or individual.
- Calculate risk scores based on the activity's specific characteristics, including transparent reason codes.
- Prioritize alerts and route potentially fraudulent transactions to appropriate team members.
- Automatically assign work to investigators based on user-set rules and requirements.

## Social network analysis

- Identify linkages among seemingly unrelated transactions and uncover unknown relationships through a network visualization interface.
- Go beyond transaction and account views to analyze related activities and relationships at a network level.
- Automatically identify suspicious networked behavior in the data.
- Gain fast access to full details on transactions, all related parties and networks.
- Merge or delete network entities, and add annotations (text and images) to specific entities in a network.

## Workflow and case management

- Systematically facilitate investigations using a configurable workflow.
- Capture and display all information pertinent to a case, including interview notes and evidence needed for criminal or civil prosecution, restitution and collections.
- Assess your overall fraud exposure, including losses due to fraud and fraud detected or prevented.

## The SAS® Difference

Only SAS provides better fraud detection and greater operational efficiency with:

- A hybrid approach that combines rules, machine learning and artificial intelligence, predictive models and network analytics.
- Text analytics for analyzing unstructured data (e.g., from a call center).
- Social network analysis to uncover organized fraud rings that might otherwise take years to identify.
- A banking-specific data model, fraud engine, prepackaged heuristic rules, anomaly detection and predictive models to get you up and running quickly.
- The ability to develop profiles for all data available for analysis, including devices and IP addresses, plus all demographic information that allows for alerting on these attributes.
- Analytics to help you understand the actual impact on the bottom line.

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

- Assess investigative workloads, investigator efficiency and ROI more completely, and use that information to build a business case for expanding fraud investigation resources.

## Search and discovery

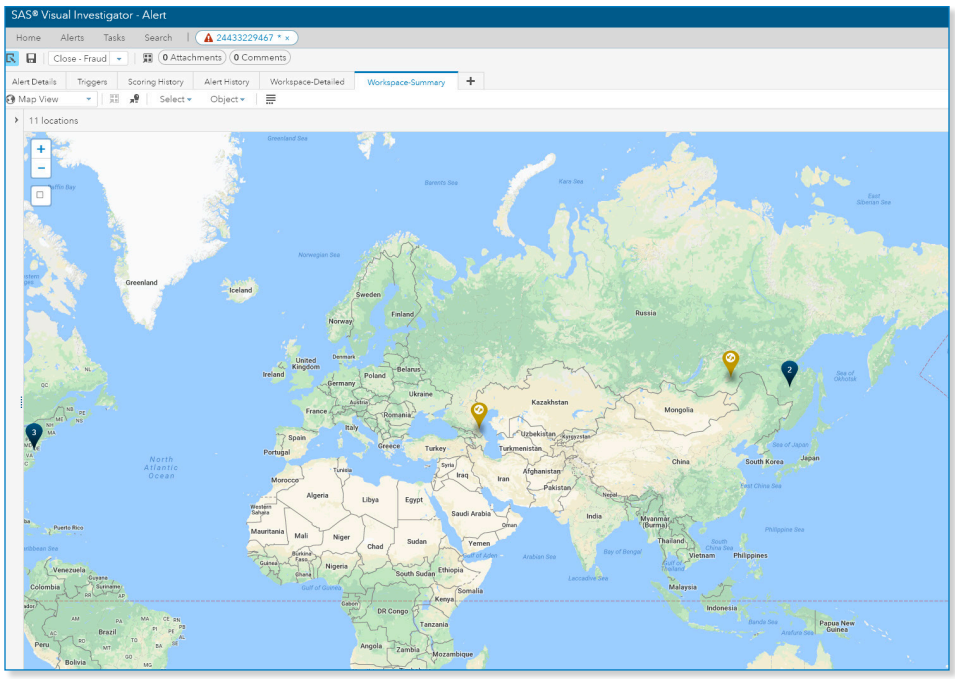
- Perform free-text, field-based or geospatial searches across all data (internal and external).
- Refine searches using interactive filters and facets that are customized for the SIU team.
- Construct complex queries through an intuitive interface without the need to understand programming syntax. For example, use fuzzy searching, proximity searching and field boosting while restricting searches to specific entity types, fields, comments or insights.

## Machine learning

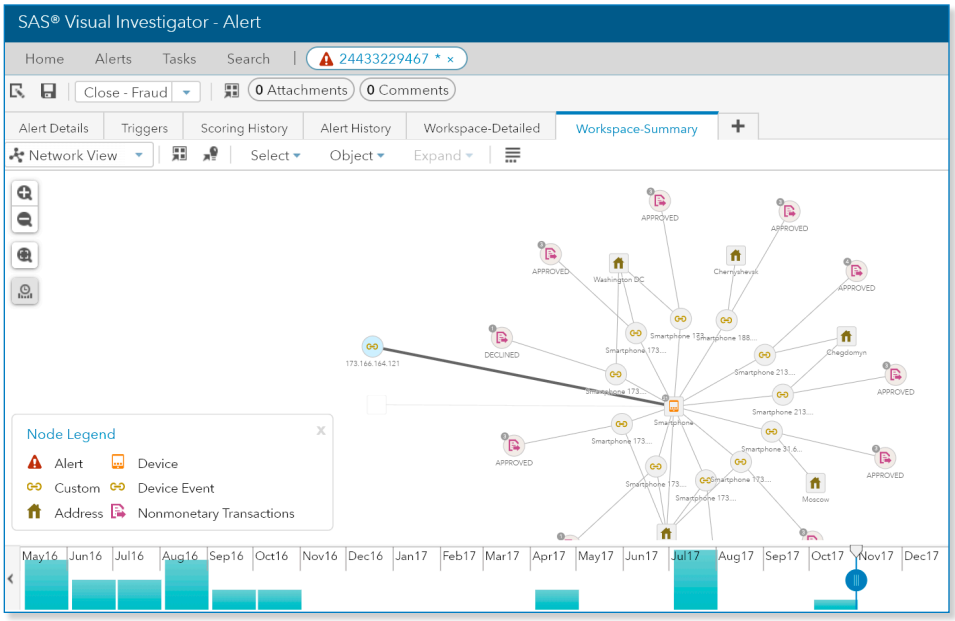
- Access a broad set of modern statistical, machine learning, deep learning and text analytics algorithms within a single environment.
- Improve fraud models by testing different approaches in a single run. Compare results of multiple supervised learning algorithms with standardized tests to reduce false positives.
- Employ multiple analytical capabilities, including clustering, several types of regression, random forests, gradient boosting models, support vector machines, natural language processing, topic detection and more.
- Perform continuous learning based on previous output results.

## Auditability

- Run reports and produce a complete audit trail for all alerts and investigations in accordance with compliance mandates.
- Show network evolutions and drill down into reports for more detail.




Map view of suspicious activity.




Network diagram of associated entities.

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

THE POWER TO KNOW.