WHITE PAPER

Keeping Fraud Detection Software Aligned With the Latest Threats

Why it matters – and how next-generation software strengthens your defense against fraud

sas

THE POWER TO KNOW.

Contents

Fraud and Financial Crimes Are on the Rise – and Taking a Big Toll

Fraud and financial crimes weren't considered serious and widespread issues until the 1980s. Since then, instances of fraud and financial crimes have become commonplace. Now banks and financial institutions, national security and law enforcement organizations, government agencies, and insurance companies are looking beyond traditional approaches to combat increasingly complex and higher levels of fraud and financial crime.

Fraud and financial crimes cost governments and businesses millions of dollars annually. For example:

- When banks fail to contain financial crime, they are hit with both crime-related losses and fines imposed by regulators and law enforcement agencies. Fines can run into hundreds of millions of dollars or more.
- US government officials estimated that Hurricane Katrina resulted in about $500 million of fraud related to federal funding.[1]
- According to the ACFE's 2018 Report to the Nations, more than $7 billion was lost to occupational fraud.[2]

But the biggest risks often extend beyond financial impacts to include damage to corporate brands from association with fraud – whether it's due to transnational organized-crime rings, scandals related to corruption, or data breaches that put customer data at risk.

Reducing fraud is the top priority for banks. Our research shows that 70 percent of banks say their FCIUs are focused on reducing fraud loss.[3]

Fraud Schemes Are Continuously Evolving

Despite investments in staff and anti-fraud software, fraudulent activity continues to fly under the radar, as fraud types and strategies rapidly evolve. It's hard for organizations to keep anti-fraud software current and able to detect new and emerging threats. Consider the following industry examples of how fraud is evolving.

Bank fraud and financial crimes

The explosive growth of digital communications has helped make cybercrime one of today's fastest-growing and sophisticated industries. Financial institutions are battling highly organized, transnational criminal groups operating across established crime networks to commit fraud, launder money, and finance terrorist groups and criminal gangs.

A study by Longitude Research found that traditional approaches to combating financial crime are no longer sufficient.[4] Banks are rising to the challenge by investing heavily in staff and technologies to run their financial crimes intelligence units (FCIUs). Their FCIUs conduct ongoing organizationwide threat assessments, and feed the results into their central intelligence systems to help them build a full picture of the magnitude of financial crime risks. This process enables banks to formulate strategic policy decisions to combat the threat of highly organized and sophisticated financial crimes.

Insurance fraud

The insurance industry has seen a huge surge in both new fraud types (e.g., application) and the scale and sophistication of fraud schemes, as illustrated by recent trends in disaster, smartphone and auto insurance claims fraud.

Disaster-related fraud

Examples of disasters – both natural and man-made – occur all too frequently today. Recent examples include 9/11, the Asian tsunami (2004) that affected 14 countries; and Hurricane Katrina (2005). In 2017 with hurricanes Harvey, Irma and Maria, FEMA paid out $8.7 billion to policyholders, the third-highest total in the program's history – with Hurricane Florence striking another blow in 2018.[5] Unethical people and organized crime rings view these events as opportunities to gain financially through fraudulent insurance claims. Most disaster fraud happens through charitable solicitations, contractors and vendors, price gouging, and false insurance claims.

Smartphone insurance fraud

The widespread adoption of smartphones has given rise to cellphone insurance fraud. In these cases, people eager to get their hands on the latest iPhone® make fraudulent claims against the insurance on their existing phones (for example, by claiming they lost their device) as a way to save money on the cost of the new phone. Insurance companies that purchased a fraud system around the year 2000 have likely had to spend money adapting it for this type of insurance, as well as to detect smartphone-related insurance fraud.

In New York, it is estimated that one in three auto insurance claims involve fraudulent practices.[6]

Auto insurance fraud

Auto insurance fraud continues to be one of the most widely perpetrated types of fraud. But it has evolved in recent years. For instance, the deep recession caused by the global banking crisis in 2007-08 gave rise to "crash and buy" fraud, in which drivers without insurance are involved in accidents, but do not report them until they have purchased auto insurance.[7] Once insured, they file a claim to cover the cost of repairs or replacement. While this type of fraud is not new, insurance companies have seen dramatic spikes in instances since 2007. Anti-fraud applications must be adapted to detect these new tactics so that insurance companies can avoid related financial losses.

Health care fraud

Health care fraud includes health insurance fraud, drug fraud and medical fraud – and it's big business that often involves organized crime rings. It's widely cited that Medicare fraud alone totals at least $60 billion annually in the US. And fraudsters are continuing to evolve their schemes to successfully avoid detection systems. In fact, in July 2016, the operator of one of Florida's wealthiest health care networks was arrested on charges of orchestrating the nation's biggest Medicare fraud scheme, worth $1 billion.[8]

Health care fraud is notoriously difficult to detect, as noted by Gary Cantrell, Deputy Inspector General for Investigations for the OIG in the US Department of Health and Human Services. "Fraud schemes can recur over long periods of time, or emerge as new schemes develop," he said. "For example, billing for home health services that are not received is a recurring fraud scheme. By its very nature, this fraud is difficult to detect if both the patient and physician conspire with a fraudulent home health agency to bill for services that were not rendered. An emerging variation of this theme is a beneficiary who receives adult daycare services billed as home health services. Not only is the billing of these services misrepresented, but the services are neither allowed nor medically necessary."[9]

Adapting Fraud Detection Software to Identify New Threats

As these examples suggest, organizations must continuously adapt their fraud detection software to be able to detect new types of fraud. And the cost of doing so must be built into the total cost of ownership (TCO) for the software. TCO is an estimate of the software's direct and indirect costs. The goal of calculating TCO is to look at the various costs involved in the use of a solution over its lifetime.

To calculate an accurate TCO, all of the costs associated with a given software solution must be considered. The problem is, some are often unknown or overlooked at the start of an implementation project. For example, the most common mistake when calculating TCO is using only upfront costs along with the annual maintenance, which would typically result in a TCO chart similar to Figure 1.

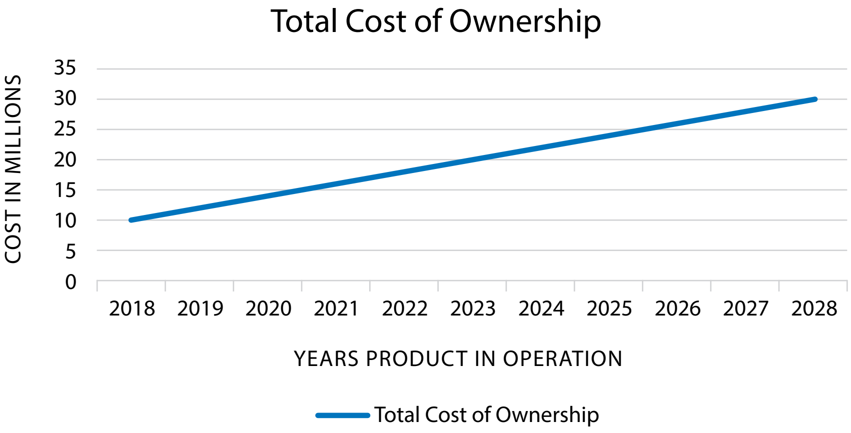


Figure 1: Cost of software over 10 years using only upfront costs and annual maintenance.

This approach does not take into consideration some of the key factors that can influence the overall cost of the software over its life span – most notably, how easy it is to adapt the software to meet changing business needs (such as detecting new types of fraud described above). To understand what kinds of changes must be planned for during the life span of a fraud application, you should answer the following questions:

- Can we adapt the application to monitor for new types of fraud that we're not yet aware of?
- Can we change how the data is shown to analysts to improve their efficiency?
- Can we adapt the application to alter the data that is recorded as part of an investigation?
- How do I monitor analyst efficiency, determine inefficiencies and adjust the system to make improvements?
- What happens if the available number of analysts changes?
- How easy is it to accommodate new and/or additional data sources?

If the answer to any of these questions is to bring in an outside "forward deployed engineer" to make software changes, then the TCO for the software changes dramatically, as shown in Figure 2. This is because whenever a change must be made to the software, costs spike for that year, as the customer must pay the vendor to make the changes. This single factor can dramatically increase the TCO for fraud detection software.

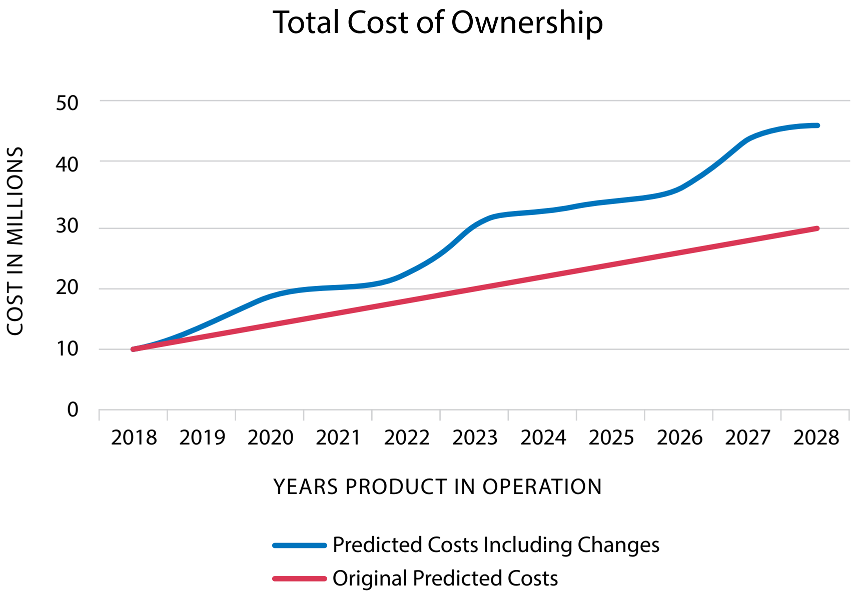


Figure 2: Cost of ownership of software when changes are made by the vendor.

SAS: Delivering Configurable Solutions With Next-Generation Fraud Analytics

Given these challenges, SAS has created next-generation fraud solutions that empower end users to keep their software current and able to detect new and emerging threats.

SAS® Visual Investigator is a cloud-ready investigation and incident management system that combines large, disparate, structured and unstructured data sources. Users can manage their rules and models for detecting threats; define, create, triage and manage alerts; perform detailed investigations; and customize the framework to meet their individual and organizational needs.

Unlike other intelligence analysis and investigation solutions, SAS Visual Investigator can be easily configured and adapted by internal IT resources to detect new and evolving types of fraud. An open, data-driven approach to system administration helps organizations configure their critical capabilities and respond to new trends and business problems.

Let's take a closer look at key areas of functionality and configurability built into the SAS Visual Investigator solution. Throughout the examples, we'll use an insurance fraud example for purposes of illustration.

Alerts

Using SAS Visual Investigator, users can define the scenarios they will use to look for fraud within their data. They can then apply these scenarios to incoming data to automatically generate alerts for analysts regarding what to investigate for fraud.

Alerts provide valuable information associated with a known entity (a set of data that relates to an object that is visualized and searchable within SAS Visual Investigator) within the system; examples of entities include a person, an insurance policy or a service claim provider. The software tracks all activity associated with an alert and enriches existing alerts with new entity information as it is created or captured (rather than creating duplicate alerts).

Queues and strategies

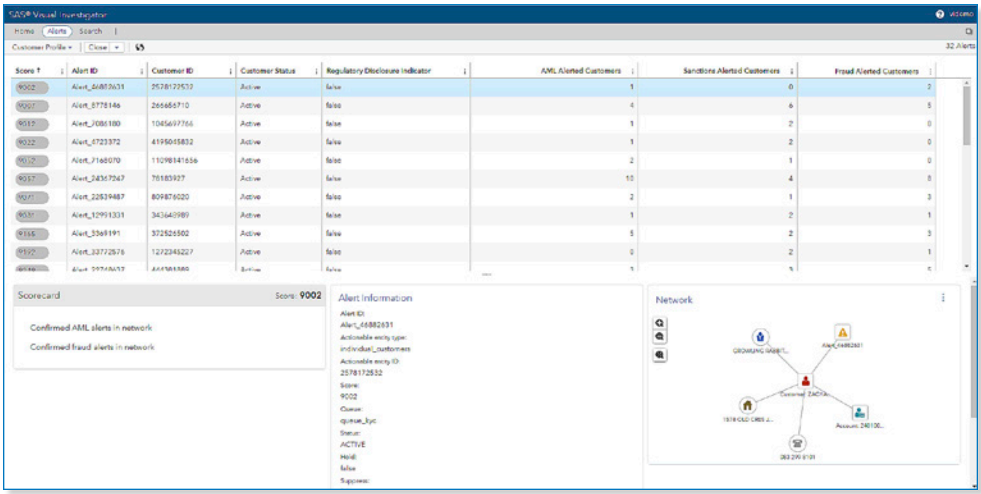
A strategy, in the context of SAS Visual Investigator, is simply a way to perform surveillance to address a particular business problem. Strategies give users a way of dividing up and managing surveillance across a boundary that they choose. They determine what is shown to an analyst, how the work is prioritized, and what can be done to an alert. The main purpose of strategies is to manage alerts and prioritize triage activities.

Within a strategy, SAS Visual Investigator prioritizes alerts using queues. The queue in which an alert shows up is determined by "queue priority" and the rules defined for that queue. The strategy-queue hierarchy is extremely flexible and adaptable with regard to the number of analysts and investigators it can support simultaneously, as well as the variety of fraud detection methods it provides to them. For example, for a large fraud investigation unit that contains staff members specializing in specific types of fraud, it can support a separate strategy for each fraud type (for example, claims fraud versus provider fraud) where specialists work in their respective strategy. Within each strategy, organizations can use multiple queues to determine the prioritization, or severity, of suspected fraud activity.

This ability to prioritize alerts by queues would be critical in the event of a disaster. After a hurricane, the number of home insurance claims rises dramatically, which can overwhelm the limited resources of insurance firms. With SAS Visual Investigator, companies can triage and efficiently manage workloads while providing better service to customers – for example, by adjusting prioritization, placing lower-priority claims on hold and allocating resources optimally.

Alert triage

As shown in Figure 3, SAS Visual Investigator has an alert triage page providing analysts with a listing of alerts, including a summary for each alert. Armed with this at-a-glance information, business users can decide on the disposition for the alert as quickly as possible.



Score	Alert ID	Customer ID	Customer Status	Regulatory Disclosure Indicator	AML Alerted Customers	Sanctions Alerted Customers	Fraud Alerted Customers
9002	Alert_46882631	2578172532	Active	false	1	0	2
9007	Alert_8778146	266656710	Active	false	4	6	5
9012	Alert_7086180	1045697766	Active	false	1	2	0
9022	Alert_4723372	4195045832	Active	false	1	2	0
9032	Alert_7168070	11098141656	Active	false	2	1	0
9057	Alert_24367247	78183927	Active	false	10	4	8
9071	Alert_22539487	809876020	Active	false	2	1	3
9081	Alert_12991331	343648989	Active	false	1	2	1
9155	Alert_3369191	372526502	Active	false	5	2	3
9192	Alert_33772576	1272345227	Active	false	0	2	1

Scorecard Score: 9002

Confirmed AML alerts in network

Confirmed fraud alerts in network

Alert Information

Alert ID:
Alert_46882631
Actionable entity type:
individual_customers
Actionable entity ID:
2578172532
Score:
9002
Queue:
queue_kyc
Status:
ACTIVE
Hold:
false
Suppress:

Figure 3:The alert triage page with SAS Visual Investigator.

Organizations can configure and adapt almost everything shown on this page to meet their needs, including:

- **The alert strategies**. As the types and frequencies of fraud exposure change, so can the alert strategies.
- **The disposition actions that can be performed on an alert**. These can be adjusted for the different types of fraud.
- **The data shown in the grid**. The data columns are defined at the strategy level.
- **The summary view of the alert shown**. This summary view (at the bottom of the page) can be changed using the page builder component (more on this later).

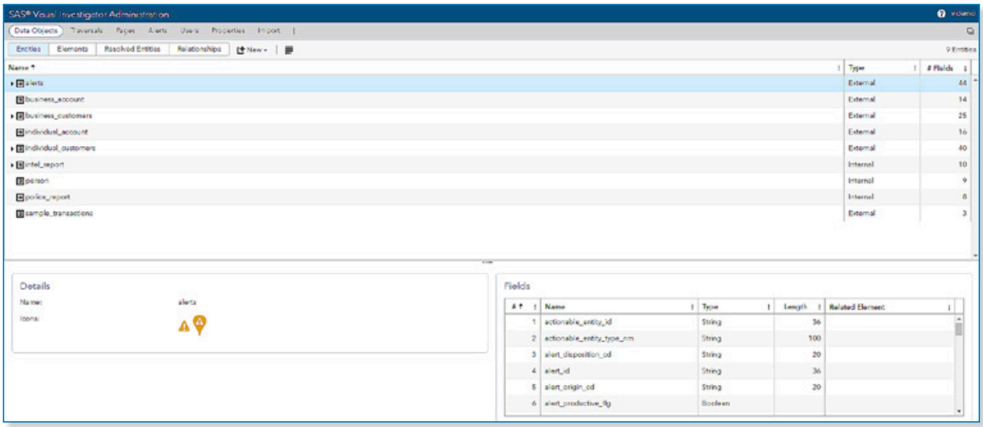
Having the ability to make these kinds of changes allows an organization to adjust what is presented to analysts, who can then focus on what's most important and work with optimal efficiency. Equally important, as new types of fraud emerge, users can adapt the triage functionality within SAS Visual Investigator to respond appropriately.

Easy access to new data sources

Modern information technology is generating and collecting unprecedented amounts of new data that can be used for fraud detection and investigation. For example, the Internet of Things (IoT) includes data generated by cars, cellphones, mobile applications and other devices with sensors – big data that enables investigators to perform more comprehensive fraud detection and investigation.

SAS Visual Investigator lets users include as few or as many data sources as they wish in their analyses. It's easy to incorporate a new data source – even for business users – thus eliminating the need for costly software engineers. You can control access to data sources via group membership, ensuring that the security of the data is preserved.

In addition, an administrator within SAS Visual Investigator can define the entity types that are available to users of the system. For example, in an RDBMS, an insurance company may have multiple tables that relate to each customer. SAS Visual Investigator can group these tables together to show customer details. Figure 4 shows the screen where users define the entity types that will be available to analysts.



Name	Type	# Fields
alerts	External	44
business_account	External	14
business_customers	External	25
individual_account	External	16
individual_customers	External	40
intel_report	Internal	10
person	Internal	9
police_report	Internal	8
sample_transactions	External	3

Name: alerts
Icons: ⚠

#	Name	Type	Length	Related Element
1	actionable_entity_id	String	36	
2	actionable_entity_type_nm	String	100	
3	alert_disposition_cd	String	20	
4	alert_id	String	36	
5	alert_origin_cd	String	20	
6	alert_productive_flg	Boolean		

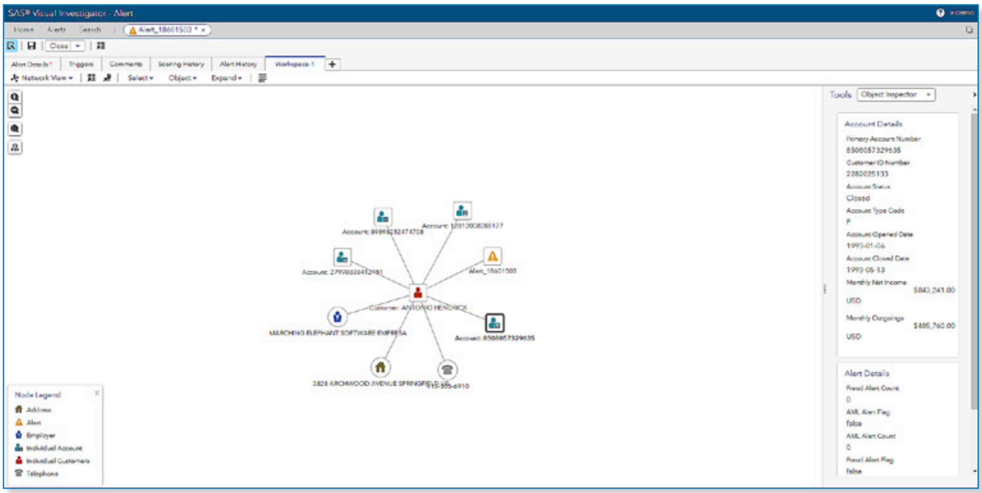
Figure 4: Administering the entity types available within SAS Visual Investigator.

As new data sources become available, the administrator can simply create a new entity type to represent them. When creating the new entity type, the administrator provides details about where the data resides, points at the data, and decides which parts to consume and how to present this within SAS Visual Investigator. For example, if a new source of data is available to an insurance company, the administrator can configure an entity type for this data source, index the data, and immediately make the new data available to analysts for investigative use.

Relationship visualization

The administration module within SAS Visual Investigator allows users to define how the different entity types modeled within the system relate to one another. For example, an insurance policy typically has a one-to-many relationship to claims. You can extract these relationships from the data using foreign keys or bridge tables.

As shown in Figure 5, SAS Visual Investigator analyzes and visualizes the relationships between entity types and represents them visually as a social network. This visualization helps analysts explore networks faster and see hidden relationships, which helps with investigations.



Account Details

Primary Account Number
8506057329635
Customer ID Number
2282025133
Account Status
Closed
Account Type Code
P
Account Opened Date
1993-01-06
Account Closed Date
1993-05-13
Monthly Net Income
$840,241.00
USD
Monthly Outgoings
$485,760.00
USD

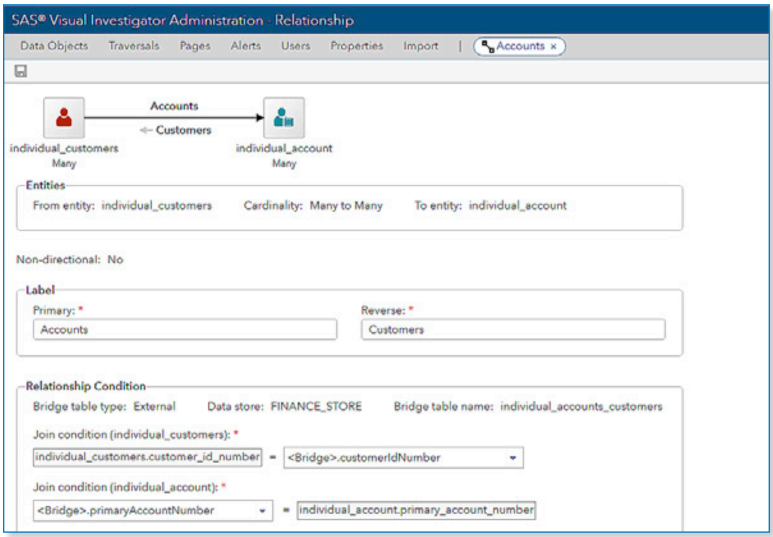
Alert Details

Fraud Alert Count
0
AML Alert Flag
false
AML Alert Count
0
Fraud Alert Flag
false

Figure 5: Social network exploration with SAS Visual Investigator.

In addition to allowing users to visually explore a social network, the software enables administrators to choose how to present the data when viewing entities. For example, when analysts view an insurance policy, they can see all the related claims. And when viewing a customer entity, they can see the related policies and claims.

As shown in Figure 6, they can also visualize the relationships between two entity types. For example, in an insurance solution, there might be entities on medical providers and medical bills. The administrator of the system can define how these are linked together within the underlying data. The creation of this relationship between the provider and the provider's medical bills enables the administrator to configure the display of the provider entity so that it displays the provider's respective bills. This enriches an investigation, as the analyst can automatically include medical bills when an alert is created on a particular provider.



Entities

From entity: individual_customers   Cardinality: Many to Many   To entity: individual_account

Non-directional: No

Label

Primary: * Accounts

Reverse: * Customers

Relationship Condition

Bridge table type: External   Data store: FINANCE_STORE   Bridge table name: individual_accounts_customers

Join condition (individual_customers): *
individual_customers.customer_id_number = <Bridge>.customerIdNumber

Join condition (individual_account): *
<Bridge>.primaryAccountNumber = individual_account.primary_account_number

Figure 6: Creating a new relationship within SAS Visual Investigator.

Social network visualization through entity resolution

Analysts can also use SAS Visual Investigator to create and visualize social networks using entity resolution. Entity resolution is the process of trying to extract unique entities from the contents of others. When these entities are found, links are created back to the source entity.

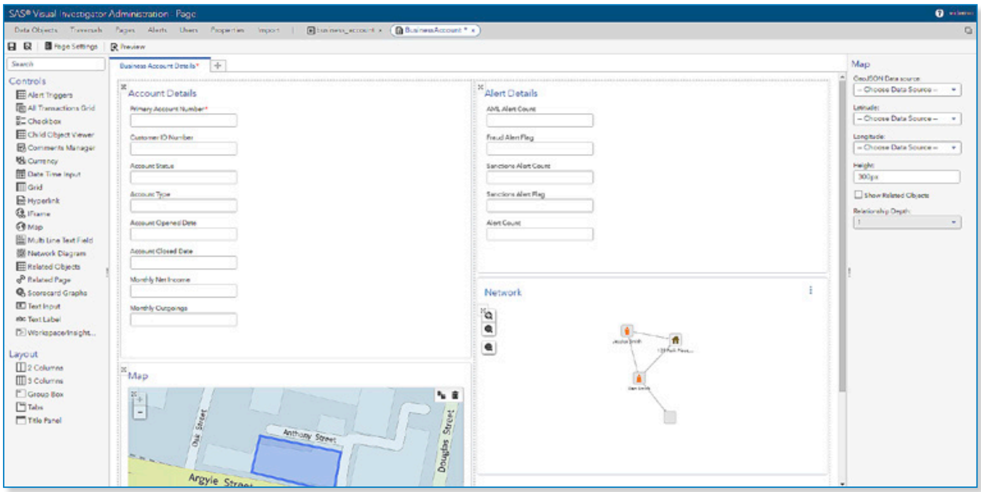
For example, an insurance claim related to an automobile crash might refer to multiple people, such as the drivers and passengers of any cars involved. The entity resolution process within SAS Visual Investigator uses rules defined by an administrator. These rules determine how to uniquely identify these entities.

By changing the entity resolution rules within the administration section of SAS Visual Investigator, administrators can adapt the solution as data sources change. If a new data source becomes available, the administrator can control analysis of the new data and the entities it contains.

Drag-and-drop page builder capabilities

Because fraud methods are constantly changing, the data that must be analyzed to detect fraud will change over the lifetime of any fraud detection software. Ease of data access – and control of how users present data to analysts – is central to an anti-fraud solution's success. These variables directly affect the efficiency of analysts investigating alerts.

SAS Visual Investigator addresses these needs by enabling administrators to define the pages shown for configured entity types. The page builder component of SAS Visual Investigator provides an intuitive, drag-and-drop interface that makes it easy to design a page. As shown in Figure 7, the left panel provides access to the different controls available for use on the pages.

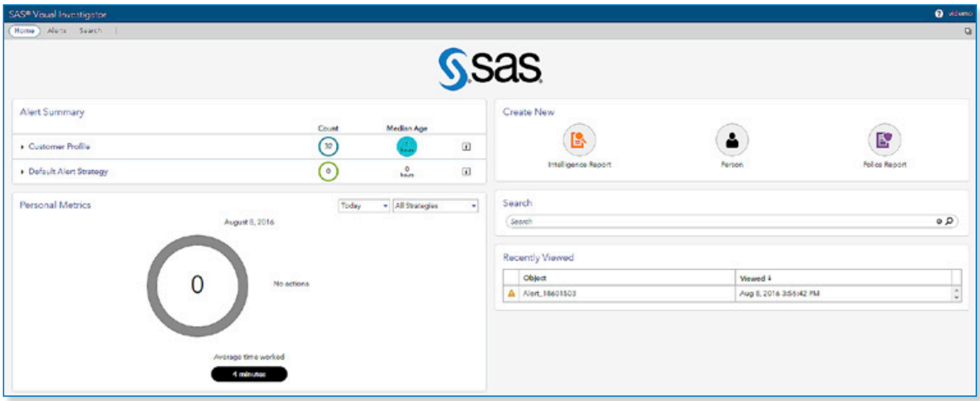


Map
GeoJSON Data source: -- Choose Data Source --
Latitude: -- Choose Data Source --
Longitude: -- Choose Data Source --
Height: 300px
□ Show Related Objects
Relationship Depth: 1

Figure 7: Using page builder to design a page for an entity within SAS Visual Investigator.

Homepage

The homepage of SAS Visual Investigator provides users with access to important information and functionality. They can configure it to provide instant access to recently viewed entities. As these entities are opened, the software reminds users of where they last stopped working so they can resume work efficiently. You can also configure the homepage using the page builder administration interface.



	Count	Median Age
Customer Profile	10	1 hours
Default Alert Strategy	0	0 hours

	Object	Viewed
⚠	Alert_18601503	Aug 8, 2016 3:56:42 PM

Figure 8: Designing a homepage within SAS Visual Investigator.

Conclusion

Fraud across all industries is constantly changing and evolving, so it's critical to easily adapt anti-fraud software to detect new kinds of threats. SAS Visual Investigator is the foundation of the next generation of SAS software for combating fraud. This solution empowers organizations – including business users – to adapt software as needs change, eliminating the need to hire costly outside consultants to do this work. Our software design not only reduces the TCO for fraud detection software, but also increases agility in response to new threats.

To learn more, visit sas.com/vi.

End Notes

[1] Alpert, Bruce, "Katrina brought billions of dollars – and quite a bit of fraud." nola.com/katrina/index.ssf/2015/08/katrina_brought_good_and_evil.html

[2] Association of Certified Fraud Examiners, Report to the Nations – 2018 Global Study on Occupational Fraud and Abuse, 2018.

[3] "Combating Financial Crime: The Increasing Importance of Financial Crimes Intelligence Units in Banking," Longitude Research/SAS, June 2016. sas.com/en_us/whitepapers/combating-financial-crime-108356.html

[4] Ibid.

[5] CNN, "Hurricane Florence is the latest setback to struggling flood insurance program." https://www.cnn.com/2018/09/14/politics/hurricane-florence-national-flood-insurance/index.html

[6] Tidball, Christopher, "Counting the cost of America's insurance fraud epidemic." propertycasualty360.com/2015/04/15/counting-the-cost-of-americas-insurance-fraud-epid?slreturn=1467934248

[7] Johnson, Denise, "Insurance Scams and Fraud Trends to Watch in 2014," Claims Journal, 23 Jan. 2014. claimsjournal.com/news/national/2014/01/23/243336.htm

[8] Miami Herald, "Feds break up $1 billion Medicare scam in Miami – biggest in U.S. history," July 22, 2016. miamiherald.com/news/local/community/miami-dade/article91231277.html#storylink=cpy

[9] U.S. Department of Health & Human Services Office of Inspector General, Testimony Before the United States House of Representatives Committee on Ways and Means: Subcommittee on Oversight; "Fraud in Medicare." oig.hhs.gov/testimony/docs/2015/cantrell-032415.pdf

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

THE POWER TO KNOW®