Paper SAS6781-2016

# Evolving Fraud Types: Can Your Application Keep Up?

Gordon Robinson, SAS Institute Inc.

## ABSTRACT

Does the rapidly changing fraud and compliance landscape make it difficult to adapt your applications to meet your current needs? Fraudsters are constantly evolving and your applications need to be able to keep up. No two businesses are ever the same. They all have different business drivers, customer needs, market demands, and strategic objectives. Using SAS® Visual Investigator, business units can quickly adapt to their ever-changing needs and deliver what end users and customers need to be effective investigators. Using the administrative tools provided, users can quickly and easily adapt the pages and data structures that underpin applications to fit their needs.

## INTRODUCTION

The total cost of ownership (TCO) of software is something that is inherently difficult to predict and something that frankly most people get wrong. Given the need to regularly adapt investigation software to changing fraud schemes, SAS® has developed a solution that reduces the complexity, ultimately reducing the TCO. This paper looks at the factors that impact TCO and some of the more common mistakes and assumptions that are made.

## EVOLVING FRAUD

Insurance fraud was not seen as a big deal until the 1980s. In the intervening period, the types of fraud committed have evolved dramatically and continue to change. The following examples cover some types of fraud that have either emerged or increased in frequency over the last 10 to 15 years.

For each example, the owner of anti-fraud software would need to consider how they would have adapted the product accordingly.

### DISASTER FRAUD

Natural or manmade disasters often bring out the best in humans. Unfortunately the flip side of this is true and they often bring out the worst. Disaster fraud is a good example of this.

This type of fraud can be grouped into 5 main categories (Satti 2015):

- Charitable Solicitation—The act of soliciting funds by posing as a charitable organization
- Contractor and Vendor Fraud—The act of posing as a vendor, worker, or repairman to collect payments but never completing the associated task
- Price Gouging—Increasing the price of goods within a disaster zone
- Property Insurance Fraud—Reporting fraudulent claims for property damage within a disaster zone
- Forgery—The act of pretending to be someone you are not for financial gain

Since the turn of the century, we have seen an increase in the number of disasters around the world. The following are just a few examples of these:

- 9/11 (*September 11, 2001)*—coordinated terrorist attacks by Al-Qaeda on the United States
- Asian Tsunami (*December 26, 2004)*—Indian Ocean earthquake off the west coast of Sumatra, Indonesia, affecting 14 countries, primarily Indonesia, followed by Sri Lanka, India, and Thailand
- Hurricane Katrina (*August 2005)*—the fifth hurricane of the 2005 Atlantic hurricane season, the costliest natural disaster, as well as one of the five deadliest hurricanes in the history of the

United States, causing severe destruction along the Gulf coast from central Florida to Texas (USDOJ:DFTF n.d.)

With global warming bringing changing weather patterns, and an increasingly volatile world, disaster fraud is something that is likely to continue to grow. As it grows, fraudsters will find new ways of trying to gain financially through fraudulent insurance claims.

### SMARTPHONE INSURANCE FRAUD

The emergence of smartphones over the past 10 to 15 years has led to cell phone insurance fraud becoming a problem. People eager to get their hands on the latest iPhone will make fraudulent claims on the insurance on their existing phones to save money on the cost of the new phone.

Insurance for cell phones has only really emerged within this time period. Anyone buying a fraud system around the turn of the century might not have accounted for this type of insurance or fraud.

### AUTO INSURANCE FRAUD

Auto insurance fraud continues to be one of the main types of fraud perpetuated. The deep recession caused by the banking crisis in 2007 led to changes in how this type of fraud is committed. In particular, it led to the growth of the "Crash and Buy" scenario. Drivers would crash their cars but not report it for a few days until they had subsequently purchased insurance. Whilst this type of fraud was not new, the frequency of occurrences spiked dramatically. Anti-fraud applications need to be able to adapt to these types of changes.

## TOTAL COST OF OWNERSHIP OF SOFTWARE

Wikipedia defines the total cost of ownership as the following:

**Total cost of ownership (TCO) is a financial estimate intended to help buyers and owners determine the direct and indirect costs of a product or system.**

The goal of calculating the TCO is to look at the various costs involved in the use of a product over the period of its lifetime. The problem most people have when trying to calculate this is knowing what all the costs will be for the product, as some of them might be unknown at the start of the project.

The most common mistake in calculating TCO is to only use upfront costs along with the annual maintenance. This is a naïve approach to calculating TCO and would lead to a chart similar to that below.

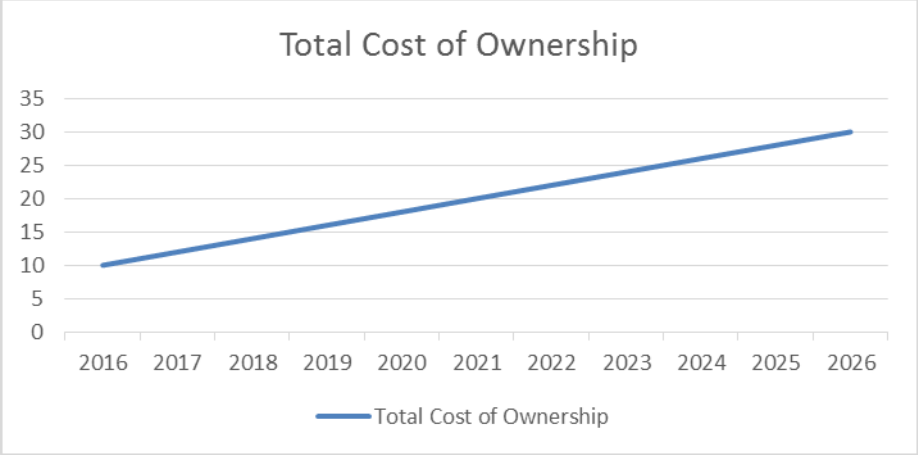


**Figure 1. Cost of Software over 10 Years Using Only Upfront Costs and Annual Maintenance**

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. One of these key factors is how easy it is to adapt the software to the changing business needs of the organization.

The following list gives some questions that are likely to arise during the life span of an insurance fraud application:

- Can we adapt the application to monitor for new types of fraud?
- Can we change how the data is shown to analysts in an attempt to improve their efficiency?
- Can the application be adapted 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 or difficult is it to accommodate new and/or additional data sources?

If the answer to any of the above requires that the customer needs to call on a "Forward Deployed Engineer" to make the changes, then the nice linear graph suddenly changes to be more like what is shown below.

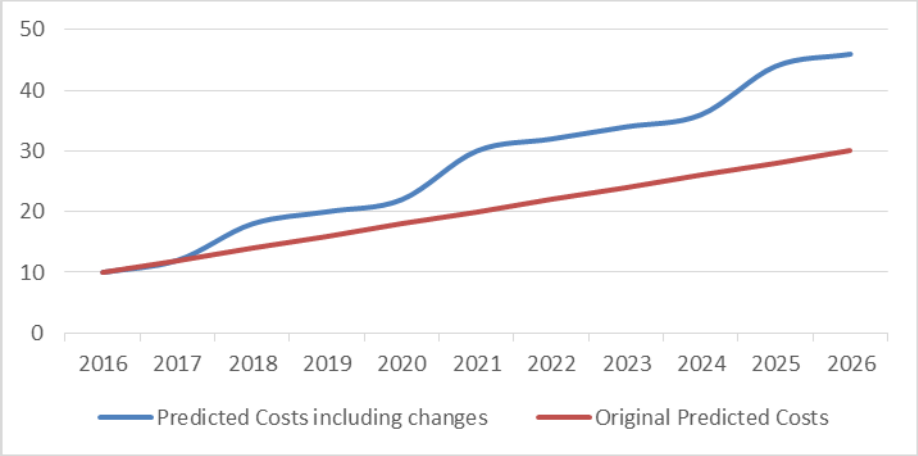


**Figure 2. Cost of Ownership of Software When Changes Are Made by the Vendor**

Whenever a change is required to be made to the software, the customer sees a spike in the costs for that year, as they have to pay for the vendor to make the changes. Even adding only this factor will lead to a fairly dramatic increase in the TCO for the product.

## HOW CAN SAS HELP?

SAS is investing heavily into advancing fraud analytics with its next generation of products.

On the authoring and surveillance side, SAS® Visual Scenario Designer has been through multiple releases and is in production at numerous insurance institutions around the world.

On the triage and investigation side, the forthcoming SAS® Visual Investigator is sure to stir up the software market. This product should be a game changer for analysts and investigators.

The aim of both of these products is to put the power to adapt to changing business needs into the hands of the end user. By doing so, we aim to reduce the necessity to call on professional service providers for enhancements, thus reducing the spikes in the cost of ownership.

## SAS VISUAL SCENARIO DESIGNER

SAS Visual Scenario Designer was developed to enable users to quickly identify patterns of interest, rare events, and anomalies interactively. It empowers the end user to make changes to the models and scenarios that they use to detect fraud and to understand how these changes would impact the workloads of their analysts.

The use of SAS Visual Scenario Designer has been covered in various papers and demos and while it isn't the focus of this paper, it is important to understand how upfront surveillance feeds downstream applications.

## SAS VISUAL INVESTIGATOR

SAS Visual Investigator is our new offering in the triage and investigation space. It has been designed from the outset to be configurable to allow it to be adapted to meet different and ever-changing business needs of customers. Designing for analyst efficiency has been a core focus of SAS efforts.

### ALERTS

SAS Visual Scenario Designer's strength is that it allows the end user to define the scenarios that will be used to look for fraud within their data. SAS Visual Investigator takes the output from this process and surfaces alerts to the analysts to allow them to investigate for fraud. SAS Visual Investigator provides an open API, which means that it can be integrated with alert generation processes other than that provided by SAS Visual Scenario Designer.

Alerts are associated with a known entity within the system, for example, a person, an insurance policy, or service claim provider. The system tracks all activity associated with an alert and enriches existing alerts with new entity information as it occurs, rather than create duplicative alerts. For example, it is not possible to have more than one alert on an insurance policy. I can, however, track that multiple rules fired, that the alert priority has changed, or that additional rules and activities have occurred related to an existing alert.

### QUEUES AND STRATEGIES

A strategy can simply be thought of as a way to perform surveillance for a particular business problem. Strategies give us a way of dividing up and managing surveillance across a customer-chosen boundary. They determine what is shown to an analyst, how the work is prioritized, and what can be done to an alert. Their main purpose is for alert management and prioritizing triage activities.

Within a strategy, alerts are prioritized by queues. The queue in which an alert shows up is determined by "queue priority" and rules defined for that queue. When an alert is first generated, it is associated with a specific queue.

The strategy-queue hierarchy is extremely flexible and adaptable depending on the number of analysts and investigators, and the variety of fraud for which the system is being used. A large fraud investigation unit (FIU) might contain staff members specializing in specific types of fraud. This large FIU might desire a strategy for each fraud type—for example, claims fraud versus provider fraud—where specialists work in their respective strategy. Within each strategy, multiple queues determine the prioritization, or severity, of suspected fraud activity.

A good example of where this would be useful is in the event of a disaster. After a hurricane, the number of insurance claims will rise dramatically. Being able to adjust the priorities of queues, to put some of them on hold, and to allocate resource between them would be invaluable to be able to cope with the workload.

### ALERT TRIAGE

Below is an example of the alert triage page within SAS Visual Investigator. The aim of this page is to provide analysts with a listing of the alerts—including a summary for each alert—with the goal of them being able to make a decision regarding the disposition for the alert as quickly as possible.

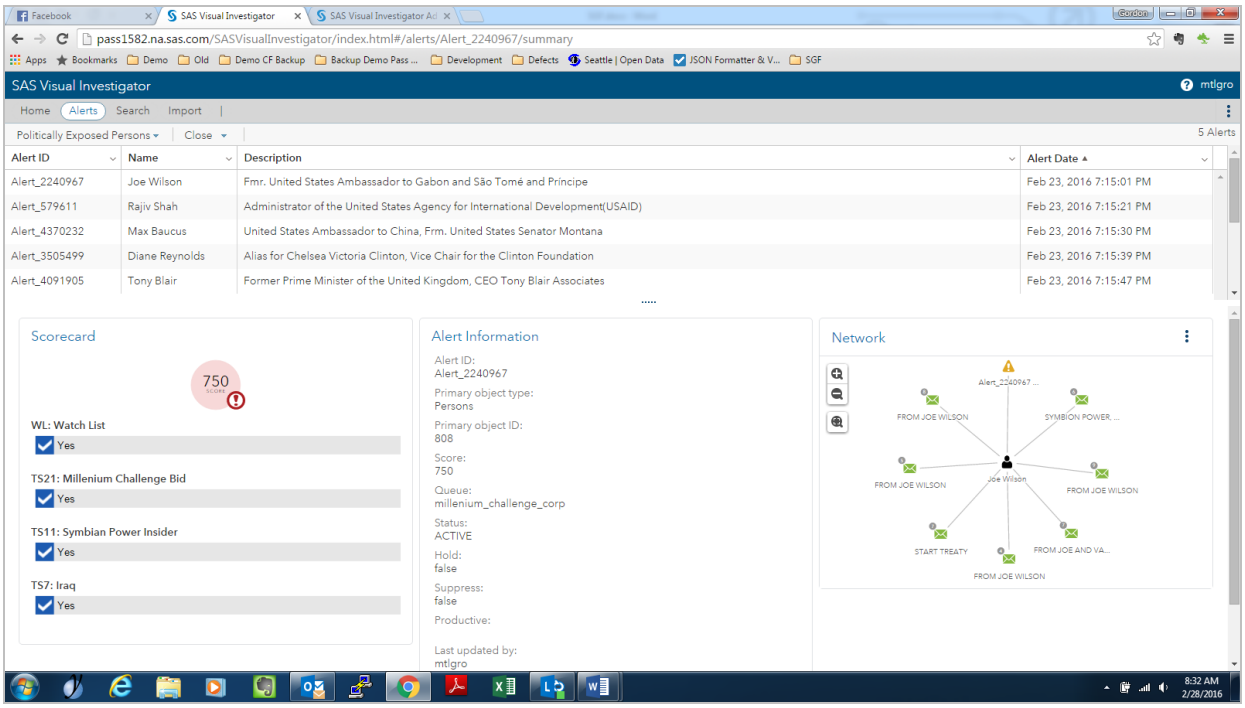


**Figure 3. The Alert Triage Page within SAS Visual Investigator**

Almost everything that you see on this page can be configured and adapted to the needs of the business. This includes the following:

- The alert strategies that are listed—as the types and frequencies of fraud exposure change, so too 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 that is shown in the grid—the data columns are defined at the strategy level.
- The summary view of the alert shown at the bottom of the page—changing this summary view is done through the page builder component to be discussed later.

Having the ability to make all of these changes means that the business can adjust what is presented to the analysts, ensuring that the business can maximize their efficiency. As new types of fraud emerge, so too can the triage functionality within SAS Visual Investigator.

## DATA SOURCES

The world we live in has changed fairly dramatically over the past 10 to 15 years with the evolution of technology and in particular the Internet. The potential data sources that can be used for fraud detection and investigations have increased during this time. For example:

- Social Media—Being able to access social media data enhances fraud investigators' abilities to investigate a person.
- Internet of Things (IoT)—As we generate more and more data from items like our cars, cell phones, mobile applications, and other devices with sensors, we increase the amount of data that can be used for fraud detection and investigations.

SAS Visual Investigator has been developed to allow it to utilize as few or as many data sources as the customer wishes. The process of incorporating a new data source has been designed to allow for a business-level user to do this rather than requiring expensive software engineers.

A document type within SAS Visual Investigator is a collection of data that is related to one object/entity. For example, an insurance fraud solution within SAS Visual Investigator would likely have documents on the following:

- Policies
- Claims
- Customers

SAS Visual Investigator includes an administration module, which includes, among other things, the ability to administer data sources. The screen below focuses on defining the document types that will be available to the analysts.

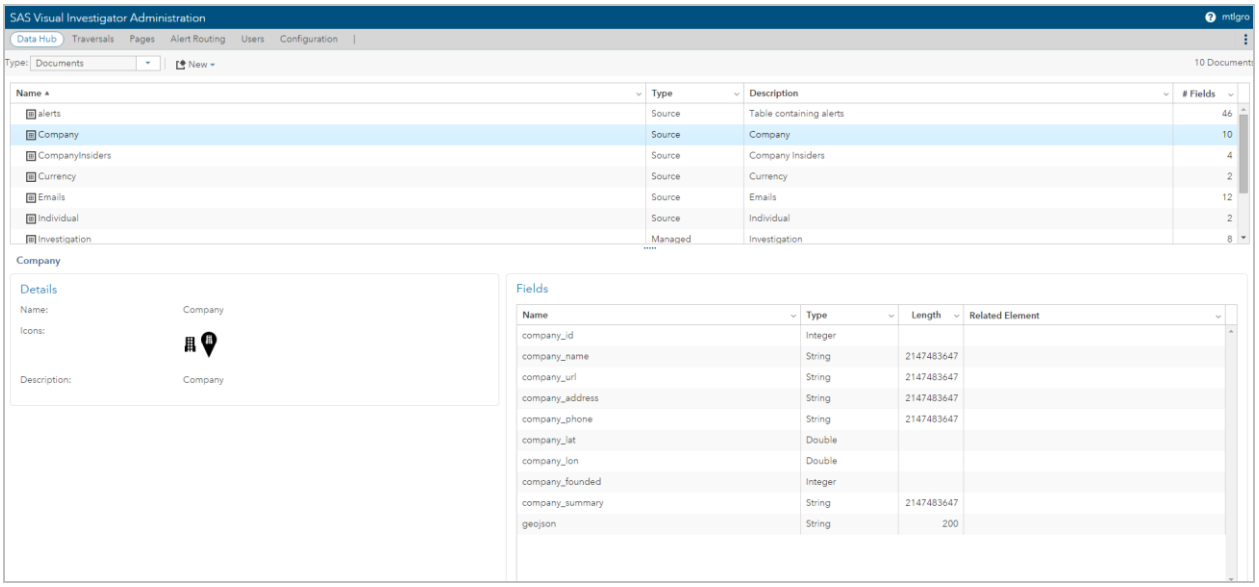


**Figure 4. Administering the Document Types Available within SAS Visual Investigator**

As new data sources become available, the administrator can simply create a new document type to represent it. When creating the new document type, the administrator is asked for details about where the data resides. Once the administrator has pointed at the data, it is simply a case of deciding which parts of the data he or she wants to consume and how he or she wants to present this within SAS Visual Investigator.

For example, if a medical bills data source was to become available, then the administrator could create a document type for this. Once this has been configured, and the data indexed, the medical bill documents would be available to the analysts to aid with their investigations.

## RELATIONSHIPS

The administration module within SAS Visual Investigator allows users to define how the different document types modeled within the system relate to each other. For example, an insurance policy would have a one-to-many relationship to insurance claims.

These relationships can be extracted from the data through the use of foreign keys or bridge tables.

Configuring relationships between the document types results in a social network being created. SAS Visual Investigator provides analysts with the ability to explore the resulting network. Figure 5 shows an example of a network diagram being explored by an analyst:

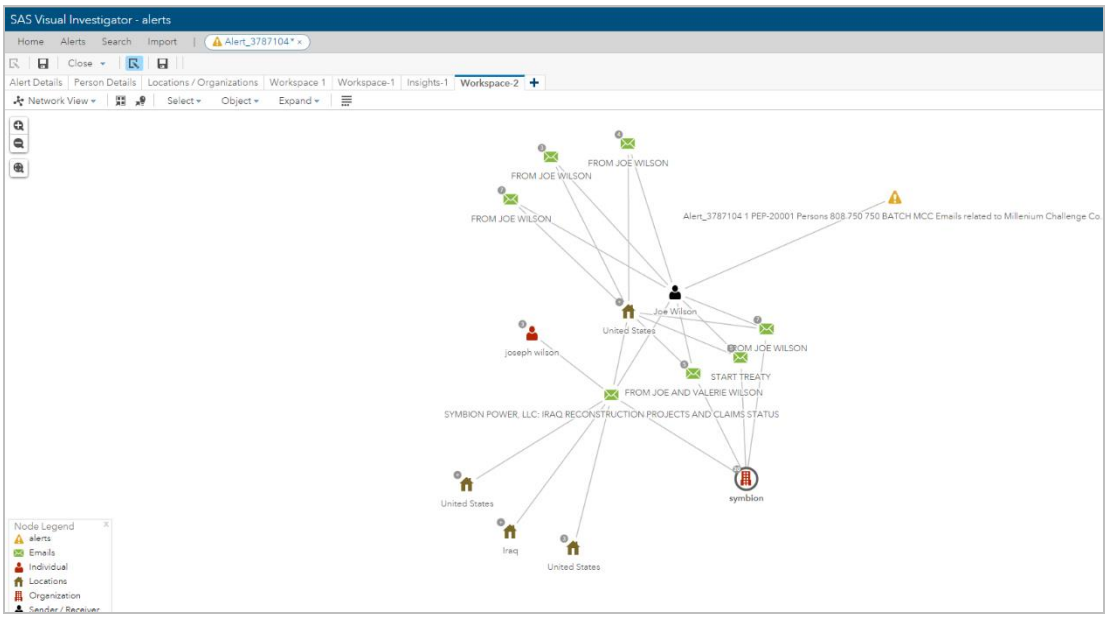


**Figure 5. Social Network Exploration within SAS Visual Investigator**

Whilst allowing the user to explore the social network within the network diagram, the relationship also allows the administrator of the system to choose how he or she wishes to present the data when viewing documents. For example, the system enables the following scenarios:

- When an analyst views an insurance policy, he or she can see all of the related claims.
- When viewing a customer document, the analyst can see the related policies and claims.

SAS Visual Investigator administration also allows for the creation of relationships between two document types.

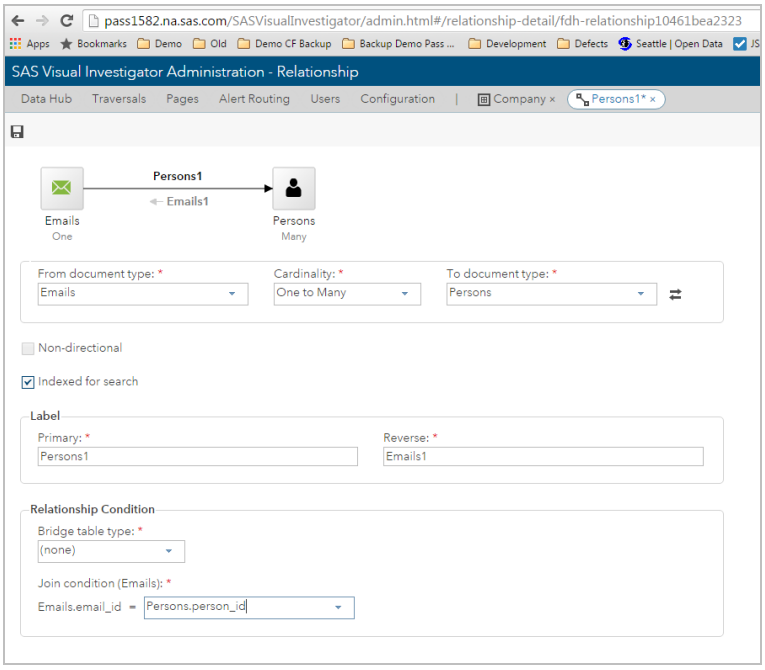


**Figure 6. Creating a New Relationship within SAS Visual Investigator**

In an insurance solution there might be documents on medical providers and medical bills. The administrator of the system would be able to define how these are linked together within the underlying data.

The creation of this relationship between the provider and the provider's medical bills would mean that the administrator could configure the display of the provider document to display the provider's respective bills. This enriches an analyst's investigation by automatically including medical bills when an alert is created on a particular provider.

**ENTITY RESOLUTION**

A second option within SAS Visual Investigator for creating social networks is through the use of entity resolution.

Entity resolution is the process of trying to identify unique entities across documents within SAS Visual Investigator. Once an entity has been resolved, SAS Visual Investigator will create a searchable record linked back to the documents from which it originated. These entities can then be included in and investigated from the network diagram, as if they were documents.

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

Having the ability to change the entity resolution rules within the administration section of SAS Visual Investigator allows the administrator to adapt the solution as data changes. If a new data source becomes available, the administrator can control how the data in that document is analyzed to determine the entities contained within it.

**PAGE BUILDER**

Key to a successful anti-fraud solution is the ability to control how data is presented to the analysts. How easy it is to access required data will have a direct impact on the efficiency of analysts using the system.

The data that a user needs to be able to access quickly will vary amongst the different types of fraud. The data that the analyst needs to see should be expected to change over the lifetime of the application as the types of fraud evolve.

The administration section of SAS Visual Investigator allows administrators of the system to define the pages that are shown for the configured document types. The page builder component of SAS Visual Investigator administration is used to design a page.

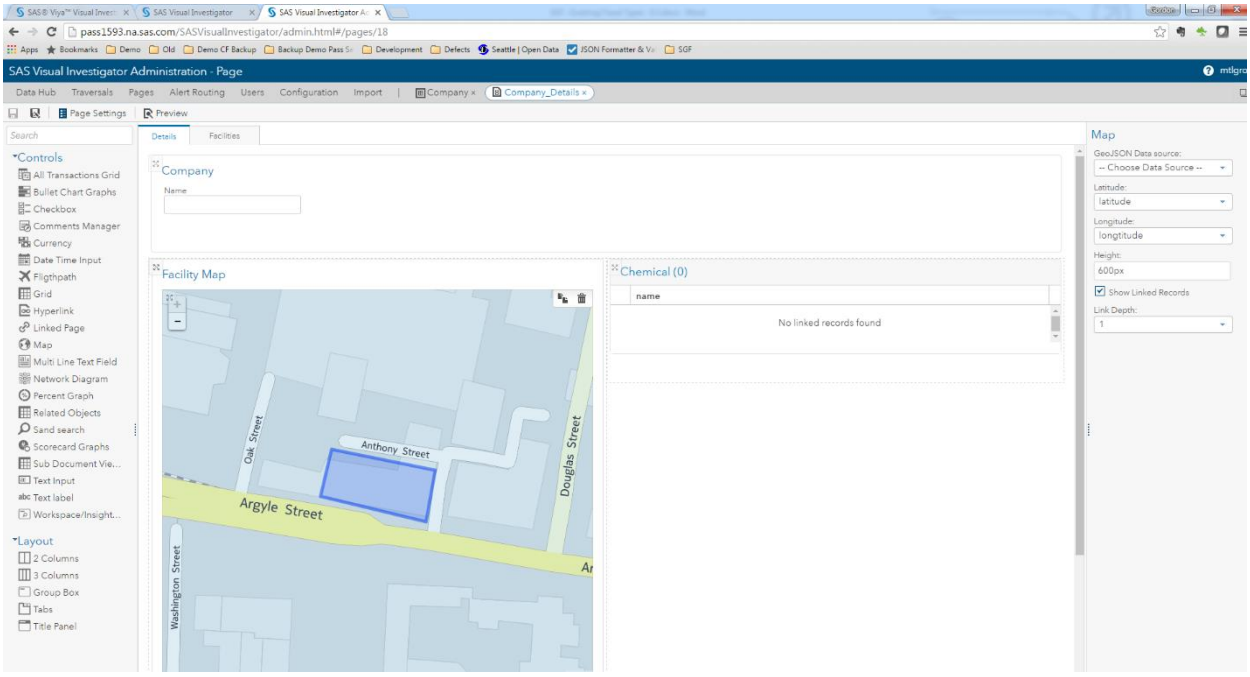


**Figure 7. Using Page Builder to Design a Page for a Document within SAS Visual Investigator**

Designing a page is done via a drag and drop interface. The left panel provides access to the different controls available for use on the pages. The right panel allows the user to select any properties associated with a selected control. The middle section is a representation of the page. The administrator can design the page by simply dragging controls into the middle section. Layout controls, such as a 2-column layout control can be used to control the positioning of controls on the page.

## HOME PAGE

The home page of SAS Visual Investigator is the landing page that a user comes to when the user first signs in to the application. The key function of this page is to provide the user with access to important information and functionality. For example, one option on the home page is to provide access to recently viewed documents. Being able to recover work from the position in which the user left it last could be efficient for an analyst.

The home page is also configured using the page builder administration interface. One difference is that the user is presented with a different set of controls when designing the home page.

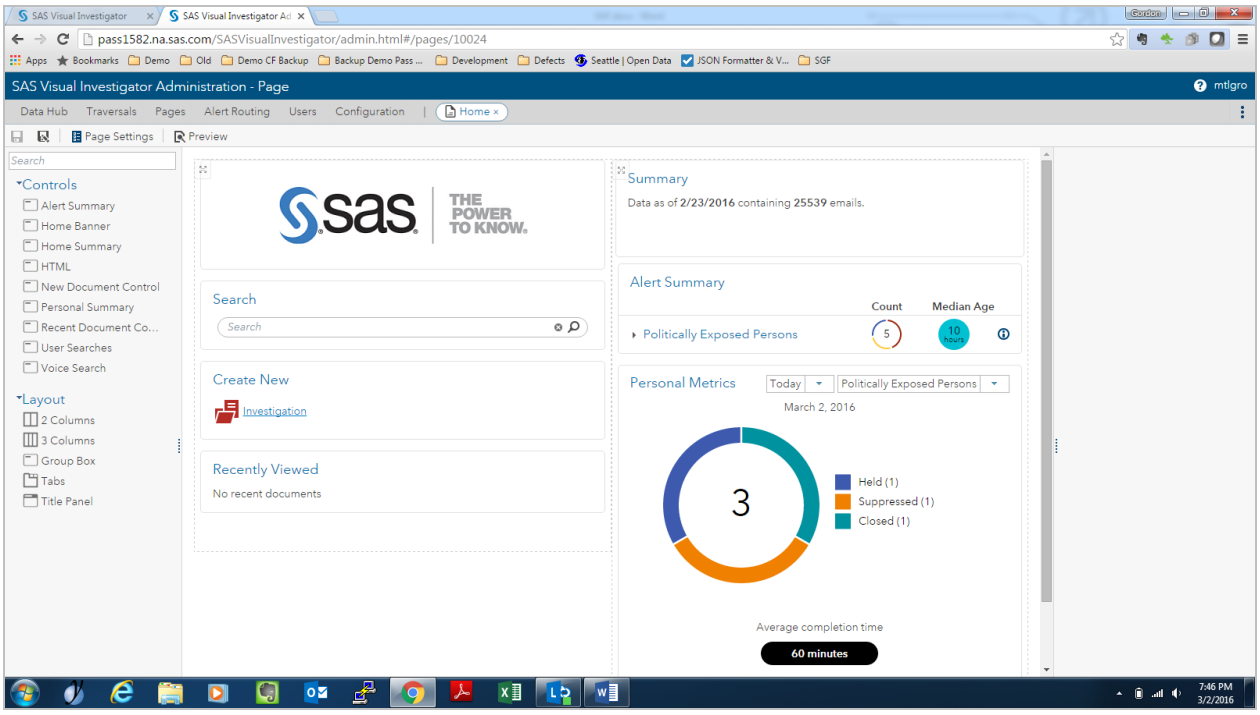


**Figure 8. Designing a Home Page within SAS Visual Investigator**

## CONCLUSION

In an environment where types of fraud are constantly changing and evolving, it is critical that any anti-fraud software application can adapt and keep up.

SAS Visual Scenario Designer and SAS Visual Investigator are the next generation of software from SAS that will be used to combat fraud. The combination of these products puts the power to adapt into the hands of the customers who use them.

This power is not only a market differentiator for SAS, but it reduces the need to hire software engineers and consultants to make implementation changes and thus reduces the total cost of ownership for the customer.

## REFERENCES

United States Department of Justice (USDOJ) Disaster Fraud Task Force, “Disaster Fraud Task Force (DFTF) | Department of Justice,” justice.gov, USDOJ, n.d. Available https://www.justice.gov/criminal-disasters.

Satti, Brooke, “Disaster Fraud: Criminals Capitalizing On Catastrophes,” securityintelligence.com, Security Intelligence, 13 Oct. 2015. Available https://securityintelligence.com/disaster-fraud-criminals-capitalizing-on-catastrophes/.

Johnson, Denise, “Insurance Scams and Fraud Trends to Watch in 2014,” claimsjournal.com, Claims Journal, 23 Jan, 2014. Available http://www.claimsjournal.com/news/national/2014/01/23/243336.htm.

Coalition Against Insurance Fraud (CAIF), “The State of Insurance Fraud Technology,” insurancefraud.org, Coalition Against Insurance Fraud, Sep. 2014. Available http://www.insurancefraud.org/downloads/technology_study-2014.pdf.

Violino, Bob, “Fraud Detection: A Method to the Data Source Madness; Insurers, including Nationwide, CNA and MetLife, are leveraging a rowing number of data sources and applying high-performance analytics to help detect patterns of fraud as early as possible,” insurancefraud.org, Insurance Networking News, Jan. 2014. Available http://www.insurancefraud.org/downloads/articles/InsuranceNetworkingNews_01-14-2.pdf.

## CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Gordon Robinson
SAS Institute Inc.
919 531 3038
gordon.robinson@sas.com