UNDER THE SPOTLIGHT: INNOVATIVE VENDORS IN FINANCIAL CRIME CASE MANAGEMENT TECHNOLOGY

Joan McGowan
08 August 2017

This is an authorized excerpt of a Celent report profiling financial crime risk management investigative case management solutions. The reprint was prepared for SAS Institute, but the analysis has not been changed. For information about the full report, please contact info@celent.com.
CONTENTS

Executive Summary .................................................................................................................. 1
  Key Research Questions ........................................................................................................ 1
Introduction............................................................................................................................... 3
What Is Case Management? ..................................................................................................... 5
The Case for Integrated Investigative Case Management ......................................................... 7
Layering New Technologies on Old ......................................................................................... 10
  Technology Enablers of a Modern Solution ......................................................................... 11
Report Methodology................................................................................................................ 14
  Approach .............................................................................................................................. 14
  Limitations ........................................................................................................................... 14
Vendor Solution Profiles............................................................................................................ 15
SAS ........................................................................................................................................ 17
  Jack Henry & Associates ..................................................................................................... 20
Looking Forward ....................................................................................................................... 24
Leveraging Celent’s Expertise ................................................................................................... 26
  Support for Financial Institutions ......................................................................................... 26
  Support for Vendors ............................................................................................................. 26
Related Celent Research ......................................................................................................... 27
EXECUTIVE SUMMARY

KEY RESEARCH QUESTIONS

1. What's driving the changes in investigative case management technologies?
2. What are the key innovations in investigative case management technologies?
3. How will the life of the fraud investigator change and what benefits will banks realize?

The report explains why technology vendors have recently transformed their financial crime risk management (FCRM) investigative case management solutions. It examines how closely the upgrades and new solutions align to banks’ developing requirements, and answers, why now? What’s driving the changes in investigative case management technologies? What are the key innovations in investigative case management technologies? And how will the lives of the fraud investigation and compliance teams change?

The following vendors are reviewed in this report because they have either recently launched a new investigative case management solution or provided significant upgrades to their current systems. All have moved the needle in FCRM investigative case management with a focus on data-driven analysis, greater operational efficiencies, process automation, increased productivity, and reduced levels of risk.

- FIS Global
- IBM
- NICE Actimize
- Oracle
- Pegasystems (Pega)
- SAS / Jack Henry Associates

The report does not attempt to compare the different solutions but rather examines the route the vendors are taking and the alignment of their solutions to the banks’ requirements. What the vendors do have in common is that they have prioritized efforts on the build out of investigative case management with more automation and AI capabilities. The ability to automate access to risk data and to use analytics to interpret that data is essential for a fraud investigator to be able to accurately investigate and report on a suspicious activity.

Vendors are clear that they believe a centralized investigative case management platform is a step closer to an enterprisewide FCRM platform, which should remain the goal of the bank. Celent argues that a centralized investigative case management platform can be the point of risk data integration, freeing up investment dollars and resources earmarked for integration of legacy detection systems.

By deploying such a platform, a bank can take advantage of newer technologies to reduce false positives, streamline processes, automate routine tasks and lower-level alerts, improve productivity, reduce regulatory risk, and abate fraudulent attacks. If done
correctly, the ROI of a centralized investigative case management platform can be considerable.

The vendors discussed in the report demonstrate outstanding efforts on multiple dimensions of investigative case management innovation. For example, FIS Global offers a highly intuitive user case management interface; Actimize and Pega deploy robotic process automation (RPA) to automate rote work and the resolution of low-level alerts; IBM is using Watson to identify key metrics and patterns from prior cases to reaggregate and reduce false positives; SAS Viya platform provides the ability to analyze data where it is parked and has partnered with Jack Henry Associates to offer their solution to institutions under $30 billion in assets; and Oracle has a strong entity network and relationship analysis and correlation tool.
INTRODUCTION

From insider threats to borderless attacks, from anti-money laundering (AML) and tax evasion to bribery and corruption, from check fraud to cyberfraud, financial crimes are committed across a wide and complicated range of bank products, channels, and geographies. Fraudsters add distance and complexity to their attacks to make them more difficult to detect and mitigate.

Although banks recognize the complexity of such crimes, they still operate on the premise that crime maps to the structure of the bank. Siloed legacy detection software, batch processing of data, poor data quality, coding static business rules and models, and overlapping operating practices and processes all greatly hinder the proper investigation of suspicious activities related to fraud and AML.

Banks did go down the path of trying to integrate their financial crimes systems on a single platform, but few succeeded. At the same time, banks practiced an open policy of staffing investigations and compliance. Both have proven to be challenging, costly, frustrating for staff and customers, and unsustainable. Crime continues to plague the industry, as do the consequences of regulatory sanctions and fines.

Since 2009, financial institutions have processed about $12 billion in fines, penalties, and forfeitures for violations of Bank Secrecy Act/AML regulations, and Foreign Corrupt Practices Act.

Figure 1: Amount Collected in Fines and Penalties for the Violation of Financial Crime by US Federal Agencies from 2009 to 2015


The US Government Accountability Office (GAO) calculated that from January 2009 to December 2015, federal agencies assessed about $5.2 billion for BSA/AML violations,
$27 million for FCPA violations, and about $6.8 billion for violations of US sanctions program requirements.

Such heavy fines can hit the bank’s balance sheets and reputation hard. Banks and vendors have to rethink their approach to financial crime management and look to modern data-driven technologies, deployed on a centralized investigative case management platform, to be able to streamline, automate and better manage fraud and AML activities, and control burgeoning costs.
WHAT IS CASE MANAGEMENT?

Case management is the coordination and investigation of bundles of information, artefacts, activities, relationships, and customer communications required to handle, resolve, and report a fraud and or AML suspicious activity case. Case management systems support the complex workflow and processes that begin with the triggering of an alert and ends with the resolution, reporting, and auditing of a case. Figure 2 shows a high level overview of an FCRM investigative case management process.

Figure 2: FCRM Investigative Case Management Process

Top line components that make up a bank’s investigative case management solution include alert management, case investigation and analysis, user interface, workflow, reporting, audit, and compliance, as shown in Figure 3.

Figure 3: FCRM Investigative Case Management Top Line Components

Source: Celent
A well-designed financial crime investigative case management platform will operate across fraud types and subcategories such as fraud (deposit, check, ACH, wire, internal fraud, and payments), AML, trade compliance, and corporate security. It will have the capability to extract data from multiple internal systems and external sources and apply intelligent automation, entity analytics, and machine learning to improve accuracy and speed of investigation, and to reduce overall financial crime risks.
THE CASE FOR INTEGRATED INVESTIGATIVE CASE MANAGEMENT

Although the convergence of banks’ detection systems has been pitched mercilessly by vendors and industry pundits over the past decade, few banks have achieved an integrated financial crime platform. Not too dissimilar to the failed CRM approach of the early 2000s, banks have stumbled over the convergence of large numbers of detection systems that have evolved as point solutions. Some of the larger banks report more than 30 AML and fraud detection systems across their organization. These systems have remained siloed along business lines and shaped their own data standards, data models, procedures, and controls for detection and case management of suspicious activities.

The Problem with Managing Multiple Detection Systems

Operating one-off detection systems means that banks have to contend with incomplete and inconsistent information, lack of common standards and processes, repetition of tasks across LOBs, high error rates, high false positives, poor customer experience, spurious suspicious activity reports (SARs), and frustrated fraud investigators and compliance managers.

In the meanwhile, fraudsters are taking advantage of new technology to hide their crimes. Bank legacy detection systems have themselves become drivers of fraud, money laundering, reputational risk, and noncompliance. Financial crime and the consequential penalties by the regulators continue to soar.

As banks continued to struggle to detect crime across products, channels, and geographies they began to inflate their risk, compliance, and legal staff in the hope of preventing crime at the investigation stage. But the lack of consistency across case management platforms and the high levels of false positives mean fraud investigators typically spend half their time triaging low-level alerts and collecting and correlating information from across multiple systems in order to close alerts.

Current Technologies Hamper the Job of Investigators

Discussions with bank investigators show that typically over half their day is spent on the manual task of gathering data, and 25% of their time is taken up with putting together narratives for SARs/CTRs and BSA.¹ The leaves little time to focus on the more

¹Currency Transaction Reports (CTR), Bank Secrecy Act (BSA)
specialized job of forensic analysis, decisioning, and resolving a range of complex fraud and AML activities.

Investigators are highly skilled; they have deep knowledge of information security, information systems, and risk businesses. They are well paid and scarce. The time spent by investigators on triaging false positives and manually reviewing millions of transactions is frustrating, wasteful, and a gift to the fraudster.

Banks continue to face crime and punishment. Table 1 shows a list of recent violations by a cross-section of banks and the heavy fines imposed by regulators. This is but a small sample of the numerous fines levied over the last several years.

Table 1: Examples of Recent Violations and Regulatory Fines

<table>
<thead>
<tr>
<th>BANK</th>
<th>REGULATOR</th>
<th>FINE</th>
<th>CRIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNP PARIBAS</td>
<td>French Prudential Supervision and Resolution Authority (ACPR)</td>
<td>$11 million (€10 million)</td>
<td>June 2017: Fined for inadequate AML controls and lack of dedicated staff in the prevention of money laundering and financing of terrorism.</td>
</tr>
<tr>
<td>DEUTSCHE BANK</td>
<td>UK Financial Conduct Authority (FCA)</td>
<td>$204 million</td>
<td>January 2017: Fined for serious anti-money laundering control failings and exposing the UK’s financial system to the risks of financial crime.</td>
</tr>
<tr>
<td>DEUTSCHE BANK NEW YORK BRANCH</td>
<td>New York State Department of Financial Services (NYSFSD)</td>
<td>$425 million</td>
<td>January 2017: Fined because it did not catch a money laundering scheme that moved $10 billion out of Russia.</td>
</tr>
<tr>
<td>BANK INTESA SANPAOLO</td>
<td>NYSFSD</td>
<td>$235 million</td>
<td>December 2016: Fined for repeated violations of AML laws and Bank Secrecy Act. The bank failed to identify suspicious transactions involving shell companies and trained employees to handle Iranian transactions so they could not easily be tied to sanctioned entities.</td>
</tr>
</tbody>
</table>

Source: Publically available data

Inefficiencies, relentless fraud, and dwindling revenue necessitate the use of technology to control costs across compliance. Banks have to automate the routine work involved in case management to free up investigators’ time to focus on the analysis of high-level risk activities. The goal is to enable your investigators to become proactive in the deterrent of financial crime.
The High Cost of False Positives

Investigative case management is triggered by alerts generated across different transaction monitoring systems (detection systems). The age of many of these systems and their reliance on hard rules and simple models that can only view a subset of data, often not in real time, cannot capture the complexity of transactional networks and hidden links between nefarious actors.

Further exacerbating the job of the investigator are the limited rules and preset scenarios and thresholds that, through an abundance of caution, are set low and result in the detection of a large number of activities that are not suspicious. The stats on the number of false positives generated by bank detection systems fluctuate between 75% and 95%, which is exceptionally high and costly.

*False positives generated by bank detection systems fluctuate between 75% and 95%.*

Fraud investigators are fully reliant on the integrity of the alerts generated by the different detection systems. The knock-on effect of such high false positives is time wasted on triaging and case managing false alerts that become non-substantive SARs.

In the process of triaging and then investigating an alert, it is common practice to suspend the transaction or account in question. In the case of a false positive alert, this can be very irritating for the customer, who is now blocked from completing the transaction. Typically, the customer walks away, and this often results in a lost sale to a merchant.

False positives create operational overheads, frustrate investigators, irritate customers, and cause the bank to miss real alerts hidden by the vast number of false alarms that have to be managed. High false positives remain a big concern to banks and regulators. IBM, profiled later in the vendor section of this report, is one of a few firms that are focused on tackling false positives: it’s using Watson to supercharge their reduction.

The reduction of false positives is the kick start for an effective central investigative case management platform that will proffer a more complete and accurate picture of risks. Investigators can then focus their specialized skill set on the investigation of high-level and complex risk cases, in the knowledge that they are valid targets of investigation.
LAYERING NEW TECHNOLOGIES ON OLD

Over the past couple of years several technology vendors have focused their efforts on developing an enterprise FCRM investigative case management system with new technology-enabled capabilities. These solutions are profiled in the next section.

Typically, banks take a three stage approach to obtaining a centralized case management platform. The stages evolve around the separate integration of fraud-related and AML-related detection systems that, by stage three, will feed into a central investigative case management platform.

Figure 4 shows the build of the stages to attaining a single case management platform. Most banks are on the cusp of stage two.

Figure 4: Three Stages to Integrated Financial Crime Management; Most Banks Are on the Cusp of Stage Two

- Lower operational and overhead costs from synergies and rationalization of systems, processes, technologies, and people.
- Lower hardware, software, maintenance, support, and development costs.
- Consistency of standards and controls leading to greater transparency and stronger governance.
- Increased throughput and productivity leads to reduced errors, and reduced risks. Robotic automation of low-level alerts (false positives) enables investigators to focus...
their efforts on evidence gathering, analysis, and resolution of high-level risk activities.

- Lower false positives will reduce friction with customers whose accounts are suspended pending an unwarranted investigation.
- Reduced monetary losses as confirmed suspicious activities are more quickly identified and prevented.
- Transparency of evidence improving the audit work of compliance officers and regulators. Regulators require insight into data lineage and model validation.
- Effective case management of suspicious activities will go a long way to ease the frustration and fatigue of investigators, compliance officers, law enforcement, and regulators.

**TECHNOLOGY ENABLERS OF A MODERN SOLUTION**

Technology-enabled capabilities for an effective investigative case management system includes the ability to automatically extract and correlate risk information; automate manual and routine processes; and enable advanced analytics in Know Your Customer (KYC), surveillance, fraud and AML detection, and case resolution.

**Key Research Question 2**

What are the key innovations in investigative case management technologies?

Technology-enabled capabilities for an effective investigative case management system includes the ability to automatically extract and correlate risk information; automate manual and routine processes; and enable advanced analytics in KYC, surveillance, fraud and AML detection, and case resolution.

**RPA** is a low-cost technology that enables the automation of processes that currently require human involvement. It’s a collection of configurable tools within an enterprise management framework aimed at integrating systems by replicating the actions of the user, interpreting interfaces, transforming data, and initiating and responding to events. RPA tools seek to mimic the role of the human while making the process more automatic and less prone to error.

When coupled with machine learning and natural language processing (NLP), RPA can carry out simple, judgment-based activities in the resolution of cases or filing of SARs and CTRs. Attended robots can aid the investigator in more complex risk cases, improving productivity and efficiency.

**Secondary analytics** such as statistical models, text mining algorithms, entity resolution, network analytics, and supervised and unsupervised learning methods can be layered onto FCRM models. This will enhance the interpretation of the data. Entity analytics is critical in showing relationships, ultimate beneficial ownership (UBO), and related activities.

**Machine learning and artificial intelligence** can support the above advanced analytics to offer superior insights, which is essential for conducting due diligence and surveillance analysis. Self-learning methods can not only help refine patterns and fine tune models, but also to define robotic processes to automate judgment calls on routine alerts.
Dynamic workflow, based on machine learning, can update rules to change the workflow process when an attribute within the case changes. Crimes are complex and do not follow set patterns; the ability to change direction is essential.

Natural language generation (NLG) tools, developed using text analytic models, can remove the onus from investigators of manually typing narratives for regulatory e-filing of SARs and CTRs. NLG can configure and generate reports based on large volumes of data and transactions. Also, it solves the problem of fat fingers.

The key technology capabilities required for an enterprise FCRM investigative case management platform are illustrated in Figure 5.

Figure 5: A Well-Designed Investigative Case Management Will Include Advanced Technology Capabilities

An effective centralized investigative management platform will provide:

- Governance around procedures and controls that align to the bank’s risk profile.
- A unified view of information captured from bundles of information across detection systems and internal and external data sources.
- Continued gap analysis and statistical fine tuning, based on self-learning of transaction monitoring scenarios that determine risk scoring and alert type.
- Graphical user interface that is intuitive, configurable, and highly visual, offers dynamic workspaces and communication tools, and avoids the need to toggle across different systems.
- Entity analytics to discover and correlate like and related entities across large and disparate collections of data.
- Robotic process automation to complete routine tasks and to make judgment calls on low-level alerts, freeing up the time of the investigator to be able to focus on high risk cases.
- Dynamic workflows that are self-learning and can adapt with changing attributes of a case.
- Automation of regulatory reporting using natural language generation and text analytic models.
- Transparency across FCRM processes. Governance and regulators require evidence that shows lineage and model validation.
A combination of failed integrated FCRM initiatives, kludgy detection systems, challenging data environments, continued high false positives, operational inefficiencies and the associated high costs of maintaining and upgrading such systems, clever criminals, a growing threat landscape, punitive fines, a mountain of regulatory paperwork, and disgruntled investigators and compliance staff have brought banks and vendors to the table.

The next section of the report looks at seven technology vendors that have recently launched or are in the process of launching new and innovative technologies for case management of fraud and AML. All have moved the needle in FCRM investigative case management with a focus on data-driven analysis, greater operational efficiencies, process automation, increased productivity, and reduced levels of risk.

- FIS Global
- IBM
- NICE Actimize
- Oracle
- Pegasystems
- SAS / Jack Henry Associates

There is no standout vendor; they excel in different capabilities. For example, FIS Global offers a highly intuitive user case management interface; NICE Actimize and Pega deploy RPA to automate rote work and the resolution of low-level alerts; IBM is using Watson to identify key metrics and patterns from prior cases to reaggregate and reduce false positives; SAS Viya platform provides the ability to analyze data where it is parked; SAS has partnered with Jack Henry Associates to offer its Visual Investigator product to banks under $30 billion in assets; and Oracle has a strong entity network and relationship analysis and correlation tool.

The information provided in the next section of the report will help banks to see where they are today, show what new technologies are on offer, and describe how those technologies align with their immediate and future requirements.
REPORT METHODOLOGY

APPROACH
To analyze the new capabilities of investigative case management solutions for the banking marketplace, Celent invited vendors to respond to detailed questions through RFIs, interviews, and briefings. The information requested covered the capabilities provided in the solution, the technology and architecture, the service delivery options, and roadmaps. Seven firms were selected because they have recently developed a financial crime shared investigative case management platform with innovative technologies.

Vendors had an opportunity to review their profiles for factual accuracy. Some of the vendors profiled in this report are Celent clients, and some are not. No preference was given to Celent clients.

LIMITATIONS
Celent believes that this study provides valuable insights into current offerings in FCRM investigation management solutions. However, readers are encouraged to consider these results in the following context. The vendors self-reported, and while this information was supplemented with publicly available information where possible, Celent did not independently confirm the details provided by the participants.
The following tables compare the solutions profiled in this report.

Table 2: Component Availability by Vendor.

<table>
<thead>
<tr>
<th>Feature</th>
<th>FISGLOBAL</th>
<th>IBM</th>
<th>NICE ACTIMIZE</th>
<th>ORACLE</th>
<th>PEGASYSTEMS</th>
<th>SAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROBOTIC PROCESS AUTOMATION</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ENTITY RESOLUTION ANALYTICS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SOCIAL NETWORK ANALYTICS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>BIG DATA ANALYSIS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DATA AGGREGATION</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MACHINE LEARNING</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ARTIFICIAL INTELLIGENCE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DYNAMIC WORKFLOW</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NATURAL LANGUAGE GENERATION</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ONE-STOP GRAPHICAL UI</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Source: Celent, vendor responses
Table 3: Deployment and Service Options by Vendor.

<table>
<thead>
<tr>
<th></th>
<th>FIS GLOBAL</th>
<th>IBM</th>
<th>NICE ACTIMIZE</th>
<th>ORACLE</th>
<th>PEGASYSTEMS</th>
<th>SAS *</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON-PREMISE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HOSTED</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CLOUD</td>
<td>ASP**</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MANAGED SERVICE OF INVESTIGATIONS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>STAND-ALONE SOLUTION</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PART OF FCRM PLATFORM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Source: Celent, vendor responses
*SAS partners with Jack Henry Associates for distribution to Jack Henry’s smaller bank and credit union clients.
**FIS Global offers an ASP service for its solution.
SAS Institute is a privately owned company headquartered in Cary, North Carolina and is the largest independent vendor in the business intelligence market. It is a leader in business analytics software and services and markets software applications including business intelligence, data integration, risk and fraud management, financial intelligence, and IT management. It has 14,158 employees, with offices in 58 countries serving 83,000 clients worldwide.

SAS has an exclusive partnership with Jack Henry & Associates to market SAS Visual Investigator case management capabilities to Jack Henry’s bank and credit union clients under $30 billion in assets. SAS client base has historically been banks in tier 1 and 2. The ability to downstream Visual Investigator will provide Jack Henry’s clients access to multiple sources of risk data and advanced analytics on a single alert and case management platform.

In June 2017, SAS Visual Investigator was ported to the new SAS Viya platform. Viya is a cloud-native and open platform. SAS Viya data analytics methods and services can be accessed through SAS, Python, Java, and Lua interfaces, and REST APIs and microservices. With the introduction of an open platform, Viya extends its capabilities in interactive discovery, investigations and reporting, statistics, data mining, machine learning, streaming data analytics, forecasting, optimization, and econometrics.

Lowering the high bar for SAS modeling requirements, business analysts, data scientists, and software developers can simultaneously derive insights from the same data. Important to banks and credit unions, which struggle with data management issues, is the ability to run analytic models where the data is parked or where the data is created, initiating alerts and defining which data is important to store and route forward.

Visual Investigator addresses case management through data integration, authoring of rules and models, identification of patterns, unknown relationships, and objects of interest through follow the money visuals. Investigators can author scenarios to detect anomalies and suspicious events, manage prioritized alerts, and conduct targeted investigations.

SAS Visual Investigator includes a number of innovative and emerging technologies:

- Text and geospatial search and analysis.
- Data analysis where data resides.
- Entity and network analytics.
- Data visualization.
- Single interactive user interface.
- Automated decisions and dynamic workflow.
- Text analytics and natural language generation.
- Automated decisions and dynamic workflow.

**Surveillance and alert creation:** From the user interface investigators can author scenarios using a rule builder and decision table to create or adjust scenarios and scores. For advanced SAS users, SAS code can be used to create more complex scenarios rules through a scenario authoring interface. SAS legacy case management
tools works with Visual Investigator by pulling prep data sets via an API to be used in its Scenario Administrator. Decisions upon the alerts can be made automatically or manually as the activity occurs.

**Alert management:** Alerts can be automatically triaged based on analysis and through business rules-driven workflow. SAS BPM workflow capabilities are part of Visual Investigator product and provide the user with the ability to refine, automate, and audit workflows if there is change in a scenario profile or case attribute, for example. Within the alert management product, investigators have the ability to:

- Prioritize alerts.
- Visualize alerts in different views to gain context.
- Enhance alerts by adding entities and integrating and connecting data.
- Escalate by routing alerts or changing their priorities.
- Create manual alerts.
- Manage multiple alert domains.
- Designate an alert to prompt a deeper investigation.

**Case investigation:** When a case is created the workflow attributes of the alert, including the runtime due dates, are set as part of the case. This enforces task deadlines. As part of the evidence-gathering process, investigators can perform free-text or geospatial searches across internal and external data. Search results can be refined using interactive filters and facets. For example, investigators can carry out a field-based search for a specific entity type, such as first name and surname for an individual or a license plate number to locate a particular vehicle. Other examples of more intricate searches include a form-based targeted search to locate a specific account number based on a financial product, and average daily balance, in a specified location; or a search for a customer who triggered a structuring scenario based on cash activity.

A selection tool scan can be used to highlight and collate objects for further case investigation.

**Entity analytics:** Link analysis shows entity relationships, their closeness, and influences. The screen visually illustrates patterns and interactions across relationships between people, transactions, accounts, places, thing and events over time and across multiple dimensions. A Network Viewer tool enables the investigator to see entire social networks and the flow of transactions. Investigators can interactively explore the network and network layout, develop communities, and identify hidden relationships. Areas of potential interest can be highlighted for further investigation.

Figure 22 visually depicts the social network connections and relationships of Frank Peyton, a customer suspected of fraudulent activities.
Figure 22: Investigators Can View Entire Social Networks, Expand or Trim the Network, Explore Communities and Individual Relationships, and Manipulate the Network Layout

Node decorators help investigators identify entities at a glance and node icons can highlight useful information as part of their investigation and evidence documentation. For example, a node icon can highlight customer accounts held at different institutions.

Visual Investigator’s Insights module is an interface that captures views of the workspace and search visualizations (e.g., maps, timelines, grids, and networks), as well as notes and images documented by the investigator. Interactive workspaces provide investigators with the ability to gather data, manipulate, and interact with visualization components as part of an investigation. Investigators can take static clips of views as forensic evidence to be included in the case. Figure 23 shows a network visual of a fraud investigation view that can be saved and documented as part of the case.
Text analytics and NLG: SAS Viya supports text analytics and NLG and natural language summarization. Text analytics can be used to analyze regulatory filing narratives, perform entity extraction and resolution, topic generation, and categorization.

Administration: Managers have access to an open data model to meet different or changing surveillance strategies and business requirements. Using a light workflow, managers can configure and manage alerts, cases and investigations. They can prioritize investigator activities, monitor productivity, and balance of workloads. To help with daily performance, managers have access to Visual Investigator case management features including dynamic forms, attachments, comments, and task management.

Jack Henry & Associates
Jack Henry & Associates (Jack Henry) was founded in 1976 to support community banks with in-house data processing systems. Today, the company sells and supports more than 300 products and services that enable financial institutions to process financial transactions, and automate their businesses. Jack Henry’s 6,000 employees serve approximately 10,500 clients with products and services delivered through three primary brands: Jack Henry Banking focuses on the US community and mid-tier banks, Symitar focuses on credit unions of all sizes, and ProfitStars focuses on the US and international financial institutions.

In the community bank space operational efficiency is critical. Small banks typically have one investigator officer and one BSA officer; unlike the bigger banks, they do not have the resources to hire more officers. More often than not, the investigator has come up through the bank’s ranks; they understand the business and have seen most types of fraud, but they are not experienced in data science. Therefore, Jack Henry investigation case management solutions need to offer ease of access to advanced and intuitive analytics, agile workflow, and an intuitive graphically interface.
Jack Henry’s partnership with SAS creates a new Enterprise Risk Mitigation (ERM) solution. The solution provides risk identification and management to the mid-tier and community banks and credit unions. The solution is part of Jack Henry’s strategy to converge financial crime products. Jack Henry sees ERM as an answer to providing more complex and predictive analytics to smaller institutions. Modules offered on the ERM platform will include:

- AML
- eFraud
- Fraud
- Card Fraud Services

SAS Visual Investigator does not require SAS processing language expertise and can be used by smaller firms that do have the wherewithal to manage and analyze large volumes of structured and unstructured data. Jack Henry has partnered with SAS to use Visual Investigator, Scenario Administrator, and Visual Analytics platforms positioned as a single solution.

Jack Henry is currently beta testing SAS Visual Investigator with its clients. Its goal is to go live end of 2017. Figure 24 outlines the products that will make up Jack Henry’s ERM solution. Visual Investigator will be a central platform to feed alerts and attached risk for investigators to disposition.

Figure 24: Jack Henry Enterprise Risk Management Solution Is Product-Based and Underpinned by SAS Visual Investigator

Source: Jack Henry & Associates

One of the biggest problems faced by smaller banks is the high false positives raised by older legacy systems. Jack Henry will contribute large amounts of bank data (its clients account for 20% of US direct deposit accounts data), while SAS provides regression models and better model value to improve false positives. Visual reporting and in memory analytics will guide Jack Henry clients to better identify patterns and reasons for false positives.
Jack Henry clients will also have access to a sandbox, as part of the Scenario Administrator, so that users can play with live data and can tune models without impacting production. Adding to the Scenario Administrator module, Jack Henry will offer prebuilt commonly used risk scenarios. The first set of scenarios to go live will be for AML alert management.

Visual Investigator will be integrated with Jack Henry’s systems data, including cores and teller systems, online banking, mobile, cybersecurity, and cyber-research team data. The solution will adopt Viya capabilities to manage external searches. It will search and pull data from across systems, databases, devices, and device IDs. Together with the ability to do complex external relationship searches, investigators will have access to greater and more accurate case insights and relationships.

A move from Excel spreadsheets to visual graphics that are updated as an event changes or a new event occurs will improve productivity, produce more accurate risk results, and avoid user frustrations with having to step outside the system to manipulate and import worksheets. Furthermore, investigators will no longer have to toggle from screen to screen; cases can be managed on a single interface with one-click access to transaction, account, and customer information, including check images and card signatures, etc.

Jack Henry will maintain its own products that add value to Visual Investigators’ case management capabilities such as Enterprise Workflow. If there is a fraudulent attempt on a dormant account, Enterprise Workflow can automatically send a request to the branch manager of the account to contact the customer to validate whether it is a dormant account with a fraud attempt. This is a popular tool used by both Jack Henry banking and credit union clients.

**Deployment options:** SAS Visual Investigator is a cloud-native, multitenant solution providing clients with several ways to deploy the solution.

1. On-premise private cloud or native Linux-based installations. Clients can host Visual Investigator either on their internal private cloud infrastructure (OpenStack, VMWare), on containers such as Docker or on a native Linux-based server or on a Linux cluster.
2. Clients can deploy Visual Investigator to a number of public cloud providers such as Amazon AWS, Google and Microsoft Azure.
3. Partner-based solution hosting such as deploying Visual Investigator on Jack Henry’s private cloud. Intriguingly, one of Jack Henry’s backup facilities for its cloud deployments is built 175 feet below ground and inside Branson Mountain, Missouri. The facility is enclosed under a dome and two layers of granite-like shale.

Regardless of deployment options, clients have the ability to configure and deploy Visual Investigator themselves, with help from SAS training and consulting services.

**Roadmap:** SAS’ roadmap items include:

1. *Mobile Investigator*, which will provide the ability for clients to develop and deploy mobile investigative applications.
2. Upgrades to SAS Exploratory Analysis tool to include new interactive visualization components, investigative sandbox, and unstructured text and entity analysis components.
3. A predictive modeling and machine learning workbench will leverage SAS fraud and compliance modeling.
4. Artificial intelligence and bots that learn from investigator interactions and investigation dispositions, as well as uncovering patterns of interest.

Jack Henry’s plan is to go live with Visual Investigator Q4, 2017. It will phase its rollout of fraud modules onto the Visual Investigator case management platform, starting with an AML module:

1. AML module.
2. eFraud module including online, ach, wire, P2P, etc.
3. Fraud module including deposit checks, employee fraud, etc.
4. Cards fraud module.

**Strengths:** Through SAS Viya platform capabilities, investigators now have easier access to advanced SAS data analytic techniques. Simpler visualization workflow design provides interactive visualization and search components to help build, gather, explore, visualize, and manipulate data for forensic analysis and complex investigations.

SAS’ partnership with Jack Henry means that the smaller bank and credit union communities should soon be able to leverage new and emerging data analysis technologies. One of the differentiators offered by the platform to both SAS and Jack Henry clients is the ability to run analytic models where the data is parked or where the data is created, initiating alerts and defining which data is important to store and route forward. This approach reduces data management efforts currently required to extract risk data from multiple sources and normalize that data in a separate data mart.
In a challenging environment where the industry has to balance regulations with fighting crime while containing costs, banks are seeking advanced FCRM technology.

The current approach of running siloed detection and case management systems are expensive and challenging, and often cannot deliver on changing requirements for financial crime management and regulations. Banks recognize that they have to address operational production inefficiencies and optimize the total cost of monitoring, investigations, and compliance activities. To drive efficiencies and effectiveness in financial crime operations, banks have no choice but to adopt newer technologies.

By deploying modern technologies to a centralized investigative case management platform, banks will realize operational efficiencies, increased productivity, greater transparency, improved governance and compliance, reduced fraud, and happier staff. Effective case management of suspicious activities will go a long way to ease the frustration of investigators, compliance officers, law enforcement, and regulators.

To be considered a good investment, an investigative case management platform must serve as the point of integration and analysis for risk data. Technology capabilities need to enable data-driven visual analysis of multiple sources of risk data, dynamic configuration of workflow and controls, and automation of manual and routine processes. Ultimately, the platform must position the investigator to be proactive in the deterrent of financial crime.

Key technology requirements of a well-designed investigative case management platform include:

- Robotic process automation.
- Secondary analytics such as statistical models, behavioural models, text mining algorithms, entity resolution, and network analytics.
- Machine learning and artificial intelligence.
- Business intelligence and dynamic workflow.
- Text analytics and natural language generation.

The vendors covered in the report are actively updating their case management technology and have taken different approaches to their platform design. FIS and Jack Henry take a product-based approach to building out their case management platforms.
they are both in the process of porting fraud and AML modules onto a centralized case management platform. Jack Henry has the advantage of leveraging a SAS analytics platform. IBM, Oracle, Pega, and SAS have repurposed their horizontal capabilities to customize their investigation management technologies for banks. NICE Actimize covers both approaches of offering innovative technologies that are purpose built for financial crimes.

Banks should work closely with their technology partners to align requirements and technologies. A centralized case management solution can become the engine of financial crime risk management.

Was this report useful to you? Please send any comments, questions, or suggestions for upcoming research topics to info@celent.com.
LEVERAGING CELENT’S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

SUPPORT FOR FINANCIAL INSTITUTIONS
Typical projects we support related to operational risk management include:

**Vendor short listing and selection.** We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

**Business practice evaluations.** We spend time evaluating your business processes. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

**IT and business strategy creation.** We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

SUPPORT FOR VENDORS
We provide services that help you refine your product and service offerings. Examples include:

**Product and service strategy evaluation.** We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

**Market messaging and collateral review.** Based on our extensive experience with your potential clients, we assess your marketing and sales materials — including your website and any collateral.
RELATED CELENT RESEARCH

Innovation in Compliance Technology: Emerging Themes and Vendor Solutions
June 2017

Risk Management Business and IT Outlook 2017: Traversing the Politics of Identity, Industrialization, and Innovation
April 2017

Bank of America: In Pursuit of Operational Risk and Compliance Excellence
April 2017

How to Become a Trusted Partner of a Bank, Part 2: A Proactive Approach by Third Parties to Risk Management
February 2017

Banker’s Guide to Third Party Risk Management: Strategic, Complex, and Liable
December 2016

Treating Cyber-Risk as an Operational Risk: Governance, Framework, Processes, and Technologies
October 2016

Risk Outlook for Banking: Calmer Times
June 2016

Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency
August 2016

Connected Due Diligence: Optimizing the Management of Supply Chain Risk
November 2015

Connected Due Diligence: Why the Industry Needs Mutualized KYC
November 2015

Emerging Solutions in Anti-Money Laundering Technology
May 2015

Emergence of a Utility Model: The Case of KYC On-Boarding Solutions
September 2014
For more information please contact info@celent.com or:

<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>EUROPE</th>
<th>ASIA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USA</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Clarendon Street, 12th Floor Boston, MA 02116</td>
<td>28, avenue Victor Hugo Paris Cedex 16</td>
<td>The Imperial Hotel Tower, 13th Floor 1-1-1 Uchisawai-cho Chiyoda-ku, Tokyo 100-0011</td>
</tr>
<tr>
<td>Tel.: +1.617.262.3120</td>
<td>Tel.: +33.1.73.04.46.20</td>
<td>Tel: +81.3.3500.3023</td>
</tr>
<tr>
<td>Fax: +1.617.262.3121</td>
<td>Fax: +33.1.45.02.30.01</td>
<td>Fax: +81.3.3500.3059</td>
</tr>
<tr>
<td><strong>USA</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1166 Avenue of the Americas New York, NY 10036</td>
<td>55 Baker Street London W1U 8EW</td>
<td>Beijing Kerry Centre South Tower, 15th Floor 1 Guanghua Road Chaoyang, Beijing 100022</td>
</tr>
<tr>
<td>Tel.: +1.212.541.8100</td>
<td>Tel.: +44.20.7333.8333</td>
<td>Tel: +86.10.8520.0350</td>
</tr>
<tr>
<td>Fax: +1.212.541.8957</td>
<td>Fax: +44.20.7333.8334</td>
<td>Fax: +86.10.8520.0349</td>
</tr>
<tr>
<td><strong>USA</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Four Embarcadero Center, Suite 1100 San Francisco, CA 94111</td>
<td>Galleria San Babila 4B Milan 20122</td>
<td>Asia Square Tower 1 Singapore 018960</td>
</tr>
<tr>
<td>Tel.: +1.415.743.7900</td>
<td>Tel.: +39.02.305.771</td>
<td>Tel: +65.9188.3998</td>
</tr>
<tr>
<td>Fax: +1.415.743.7950</td>
<td>Fax: +39.02.303.040.44</td>
<td>Fax: +65.6327.5406</td>
</tr>
<tr>
<td><strong>Brazil</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Av. Doutor Chucri Zaidan, 920 – 4º andar Market Place Tower I São Paulo SP 04578-903</td>
<td>Paseo de la Castellana 216 Pl. 13 Madrid 28046</td>
<td>Youngpoong Building, 22nd Floor 33 Seorin-dong, Jongno-gu Seoul 110-752</td>
</tr>
<tr>
<td>Tel.: +55.11.5501.1100</td>
<td>Tel.: +34.91.531.79.00</td>
<td>Tel: +82.10.3019.1417</td>
</tr>
<tr>
<td>Fax: +55.11.5501.1110</td>
<td>Fax: +34.91.531.79.09</td>
<td>Fax: +82.2.3999.5534</td>
</tr>
<tr>
<td><strong>Canada</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1081 McGill College Avenue Montréal, Québec H3A 3T5</td>
<td>Tessinerplatz 5 Zurich 8027</td>
<td></td>
</tr>
<tr>
<td>Tel.: +1.514.499.0461</td>
<td>Tel.: +41.44.5533.333</td>
<td></td>
</tr>
</tbody>
</table>