CELENT

INSURANCE FRAUD-DETECTION SOLUTIONS: HEALTH INSURANCE, 2022 EDITION

A Celent SolutionScape, powered by VendorMatch

This is an authorized reprint of a Celent report granted to SAS®. The report was written by Celent and was not sponsored by SAS®. For more information, please contact Celent (info@celent.com)

Andrew Schwartz and Fabio Sarrico

September 30, 2022

CONTENTS

EXECUTIVE SUMMARY

A claims fraud-detection system helps insurance providers identify fraudulant claims, at both the individual and organizational levels. It is typically used by claims teams. There are a variety of business benefits that can be achieved from claims fraud-detection solutions, but two of the primary goals are:

- Improving the carrier's loss ratio by identifying illegitimate claims.
- Enhancing the overall customer experience by giving providers the confidence to quickly indemnify claims that are deemed valid.

This report provides an overview of fraud-detection solutions for health insurance providers. The report profiles 5 claims fraud-detection solutions providing an overview of their functionality, customer base, technology, SaaS capabilities, implementation, pricing, and support.

Celent asked firms that provide claims fraud-detection solution for health insurers to enter information about their company and products into Celent's free digital catalog, VendorMatch (https://www.celent.com/vendormatch). This report presents certain extracts of that information. Additional details about each product are available in VendorMatch, subject to VendorMatch's terms of use.

This report aims to help health insurers define their claims fraud-detection solution requirements if they are looking to select a partner. It can be used as the first step toward creating a short list of vendors for evaluation. Insurers continue to have a broad spectrum of systems and vendors to consider when looking for a solution to fit their needs. Insurers can leverage their access to the authors through analyst access calls to learn more about the vendors.

© CELENT

INTRODUCTION

The origins of insurance can be traced back to the beginning of recorded civilization. Some historians cite Babylon, circa 4000-3000 BC, as having the first-known instance of an insurance policy. Loans were granted to merchants with the stipulation that if their shipment was lost at sea the loan did not need to be repaid. Over the next millennia, countless generations of businesspeople and regular citizens alike would benefit from the protections provided by insurance. However, for as long as the insurance business has existed, so has its "evil twin," insurance fraud.

Health insurance fraud is defined as providing false or misleading information to a health insurance provider to unlawfully obtain benefits. It can be perpetrated by the policyholder, medical provider, or a third party. According to the Coalition Against Insurance Fraud, 10% of all losses are estimated to be fraudulent.[1]

Insurance companies should be cognizant of the fact that more minor incidences of fraud may be more rampant than they think. This is evidenced by a poll from the Insurance Research Council in 24% of respondents in the United States believe it is acceptable to inflate an insurance claim to make up for their deductible.[2] And that is just those who were not too embarrassed to admit it. Hence, it is reasonable to opine that some healthcare providers believe it is acceptable for to behave dishonestly with insurance companies.

Some examples of health care fraud are:

Medical Providers:

- Billing for services not performed by either entirely fabricating a claim or padding legitimate claims with services that did not take place
- Double billing by submitting multiple claims for the same service
- Upcoding by charging for more expensive services than were actually provided
- Conducting unnecessary procedures to generate revenue
- Falsifying a patient's diagnosis to justify conducting a procedure or service that is not necessary

[1] https://www.propertycasualty360.com/2022/05/17/fraud-in-disaster-claims-cost-insurers-as-much-as-9-2b-in-2021/

[2] http://www.insurancejournal.com/news/national/2013/03/20/285243.htm

- Accepting kickbacks for patient referrals
- Unbundling by billing for each stage of a procedure as it is were a separate one to increase reimbursement costs

Policyholders:

- Forging or altering medical bills
- Using a false or expired identification card to receive medical services or medications
- Giving a medical insurance card to an individual who is not designated for its use
- Doctor shopping by visiting multiple providers to get desired medical prescriptions or services done

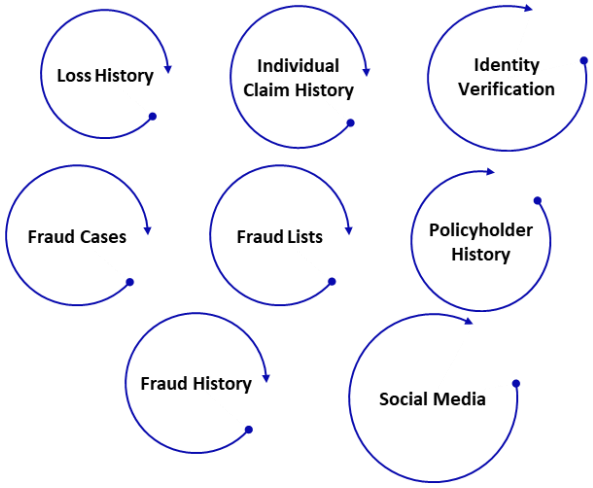
Trends Impacting Health Insurance Fraud

Celent believes there are two major trends that are impacting how insurers are detecting and responding to fraud in the health insurance space. Accordingly, today's leading vendors in the fraud-detection space have made valiant strides over the last several years to provide solutions that support providers.

Use and Application of Data

To make machine learning models work effectively, fraud-detection models need to access high-quality data from myriad sources. As such, leading fraud-detection tools are leveraging new data sources and applications of data to improve fraud detection. By integrating with a variety of available internal and external data sources, providers can have a more complete picture of the claim, which will allow them to make more informed assessments about its veracity. Having access to this data in real time will allow providers to prudently make claims decisions and create an improved customer experience. The future benefit of having AI/ML models ingest the data stems from iterative feedback loops that may optimize processes and provide insight into fraud factors.

Figure 1: Data Points that May Inform Fraud Detection

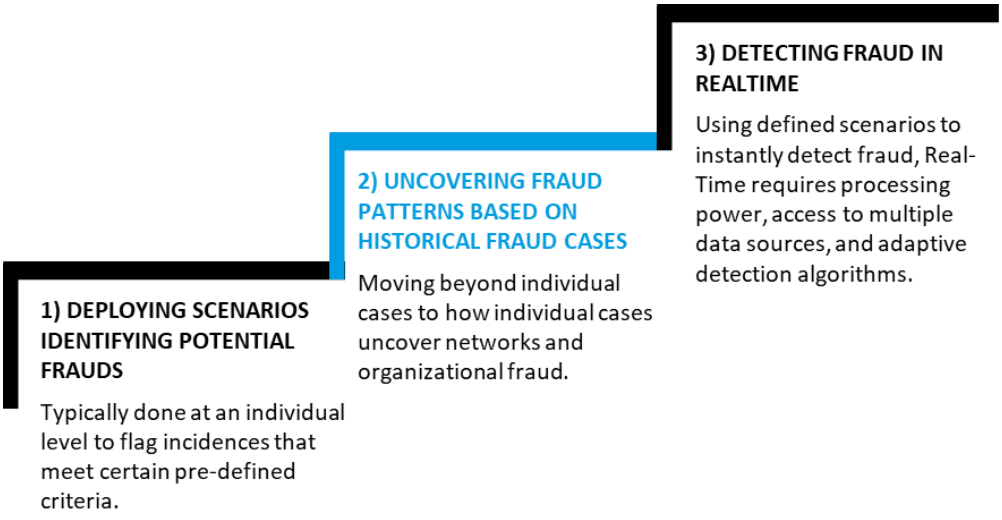


Source: Celent

Automation of Decisions

Today's advanced fraud tools are going beyond simply providing information for an adjuster employee to decipher. Directionally, they are moving from showing what happened to making intelligent automated decisions based on the fraud model. Figure 3 illustrates the evolution of modern fraud-detection tools. The tools are moving from deploying scenarios to identify potential frauds at an individual level to uncovering larger fraud patterns based on historical cases to, in their most advanced state, using defined scenarios to detect fraud in real time.

Figure 2: Evolution of AI in Fraud-Detection Tools



Source: Celent

KEY RESOURCES AND CAPABILITIES OF A FRAUD-DETECTION PLATFORM

In the simplest terms, the goals of a fraud-detection tool are to detect and flag suspicious claims. To do so, most fraud-detection solutions have a baseline set of features and functions. Below is a table of common functionality.

Table 1: Fraud-Detection Solution Features and Functions

FUNCTION	FEATURES
Data	• Ability to aggregate historical data from different internal databases. • Ability to integrate with external data capture tools (IoT, wearables, sensors, etc.). • Ability to consolidate data coming from external databases. • Data quality checking tools. • Automatic data adjustment prompts (unstructured, inconsistent, or redundant data).
Model Configuration	• Reusable, sharable rules, variables, and models. • Rules, variables, and models repository (searchable, version controlled). • Ability to compare multiple scenarios/models. • Real time fraud scoring. • Ability to create multivariable-based algorithms. • Ability to schedule model run-time. • Ability to prioritize model updates and model results (for instance, when multiple results are displayed on a shareable dashboard).
Claims fraud-detection techniques and claims-related models	• Claims fraud pattern identification. • Anomaly detection.

FUNCTION	FEATURES
	• Social network analysis. • Claims severity modeling. • Claims frequency modeling. • Claims settlement optimization.
Investigator features	• Ability to design and update monitoring dashboards. • Ability to assign/share fraud cases with other investigators. • Ability to check fraud case logs (status changes, audit trails, etc.).

Source: Celent

REPORT METHODOLOGY

Approach

To analyze the capabilities of health insurance fraud-detection solutions, Celent invited a broad set of vendors to participate in this year's report. Not all vendors chose to participate. There was no cost for vendors to be included.

Each participating vendor completed an online RFI in Celent's VendorMatch/RFX platform. The RFI asked for data about the features provided by the solution, its technology and architecture, the current client base, pricing models, and the vendor itself. RFIs were completed for 5 products.

Celent used that data to draft profiles but did not independently confirm the information provided by the vendors. 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 for inclusion in either the report or the subsequent profile.

About the Profiles

Each profile is structured the same way. Profiles present information about the vendor and its fraud-detection offering, client base, and staff dedicated to the platform. Charts provide more detailed information about specific features such as functionality, public cloud provider support, and pricing.

The profiles are presented in alphabetical order.

Limitations

Celent believes that this study provides valuable insights into current offerings in health insurance fraud-detection marketplace. However, readers are encouraged to consider these results in the following context. The vendors self-reported. Participants in the study were asked to indicate which capabilities they provide in addition to requesting general information about their client base. While this information was supplemented with publicly available information where possible, Celent did not confirm the details provided by the participants.

© CELENT

CELENT TECHNICAL CAPABILITY MATRIX

New to Celent's solution reports this year is the Technical Capability Matrix. We have placed each solution into one of five categories based on the sophistication and breadth of its technology and functionality (i.e., plotting the A and B dimensions). Solutions are not ranked within the assigned category; they are listed alphabetically.

The five categories are:

I. **Luminary:** Excels in both Advanced Technology and Breadth of Functionality.

II. **Technology Standout:** Excels in Advanced Technology but does not yet have as many features as leading competitors (low on Breadth of Functionality). Often newer, these solutions typically have chosen a focused set of functionalities to begin their journey.

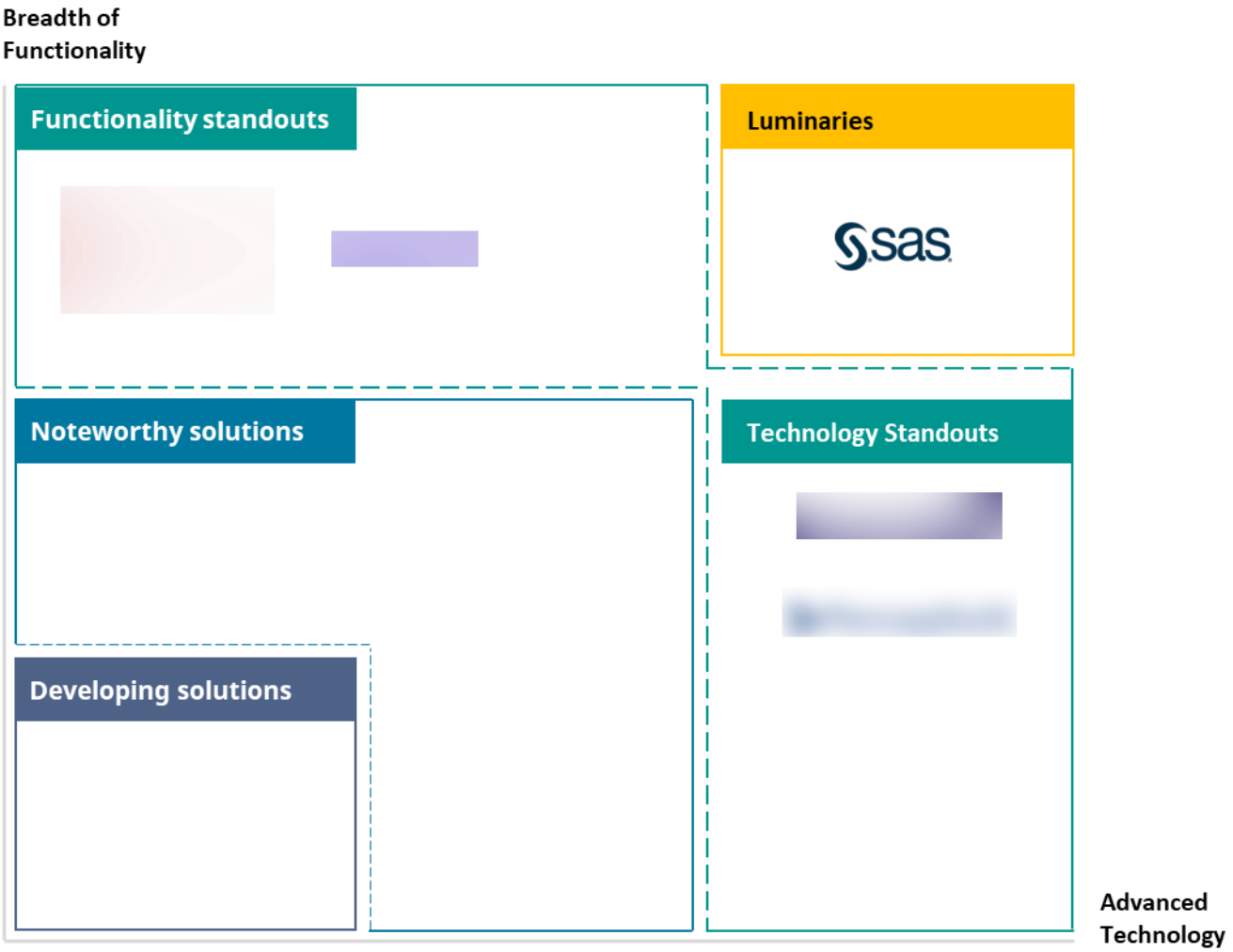
III. **Functionality Standout:** Lower on Advanced Technology, high on Breadth of Functionality (likely a large installed base). Often more established, these solutions have built out a robust set of features with technology that may not be cutting-edge.

IV. **Noteworthy Solution:** Relatively lower on both dimensions, yet still very worthy of consideration by financial institutions.

V. **Developing Solution:** Typically, new to the market and low on either Advanced Technology or Breadth of Functionality. Has the potential to mature into a more robust offering over time.

© CELENT

Figure 1: Celent Technical Capability Matrix



Source: Celent

VENDOR PROFILES

About the Profiles

Each of the vendor profiles presents information about the vendor and its solution, professional services and support capabilities, customer base, functionality, technology, partnerships, implementation time frames, and costs.

To gather data on implementation costs and fees, Celent asked vendors to provide their current client base's first-year total cost of ownership for costs associated with software licensing, initial installation, customization, annual maintenance, and training.

SAS: SAS® DETECTION AND INVESTIGATION FOR HEALTH CARE

Company and Product Snapshot

SAS is a private company headquartered in Cary, North Carolina, US, with sales and professional services personnel located throughout North America, Latin America, Africa, Middle East, Europe, and Asia Pacific. The company has 12,046 employees, of whom 400 are available to provide professional services/client support for the SAS® Detection and Investigation for its Health Care solution.

The vendor states it has had no legal issues or bankruptcies.

Table 1: Company Snapshot

Year Founded	1976
Number of Employees	12,046
Revenues (USD)	$3,200,000,000
Financial Structure	Private N/A
VendorMatch Link	https://www.celent.com/vendormatch/discovery/vendors/sas
User Conferences	The vendor offers an annual user conference or customer event.

Source: Vendor RFI

Table 2: Product Snapshot

Name	SAS® Detection and Investigation for Health Care
Year Originally Released	2009
Current Release and Date of Release	SAS Viya 4.0/2022
Revenue Derived from the Product	$100 million (approximate)
R&D Expense	SAS reinvests more than 25% of its revenue into research and development for all software products and solutions.
FTEs Providing Professional Services for Product	400
Regional FTEs (NA/EMEA/APAC/LATAM)	200/110/50/40
Target Market	Health care payers, including commercial plans, government health care systems, commercial supplemental benefit programs, and Program-Policy Departments;

	Property & Casualty insurers (for medical claims related to P&C policies); Worker's Compensation providers
Installed Base	67
Notable Clients	India National Health Authority (NHA); National Health Service (UK); Tawuniya (Saudi Arabia); CZ (Netherlands), Clalit (Israel); South Carolina Department of Health and Human Services; Oregon Health Authority

Source: Vendor RFI

Overview

The vendor states that: SAS® Detection and Investigation for Health Care takes a unique, end-to-end approach to detecting and preventing both opportunistic and professional fraud at each stage of the health care claims process.

The solution's fraud analytics engine uses multiple techniques (automated business rules, outlier analysis, predictive modeling, text mining, database searches, exception reporting, network link analysis, etc.) to uncover the likelihood of fraud, waste, abuse and other improper payments that cause loss and compromise payment integrity. Prioritized alerts are then routed to investigators, auditors, provider payment specialists and other business units, where analysts can use case management tools to efficiently triage and investigate.

Once a claim is scored and prioritized, an analyst can perform a more in-depth review of the claim's characteristics to determine if the claim or any associated historical data are fraudulent or suggest improper payment.

The solution provides an end-to-end framework and workflow for detecting, preventing and managing health care claims fraud. It includes components for fraud detection, alert management and case handling. In addition, clients get:

- A category-specific workflow.
- Rule and analytic model management.
- Content management.
- Advanced analytics, machine learning and artificial intelligence.
- Link and social network analysis.
- Integration with a case management system.
- Full integration with an enterprise-wide advanced analytics architecture and platform.

Key features include:

Fraud data management

- Provides a health care-specific fraud, waste and abuse data model.

- Consolidates historical data from internal and external sources – claims systems, watch lists, third parties, unstructured text, etc.
- Eliminates or reduces redundant or inconsistent data with the solution's built-in data quality tools.
- Seamlessly integrates with existing payment integrity solutions, including case management systems, overpayment recovery vendors, audit control systems, etc.

Advanced analytics with embedded AI and machine learning

- Provides a broad set of modern statistical, machine learning, deep learning and text analytics algorithms from within a single environment
- Enables you to improve fraud models by testing different approaches in a single run, and comparing results of multiple supervised learning algorithms with standardized tests.
- Provides an array of analytical capabilities, including clustering, different types of regression, random forests, gradient boosting models, support vector machines, natural language processing, topic detection and more.
- Continuously updates and improves models based on prior output results.

Rule and analytic model management

- Provides prepackaged heuristic rules, anomaly detection and predictive models, so you can harness the power of advanced analytics right out of the box.
- Lets you create and logically manage business rules, analytic models, alerts and watch lists.
- Enables you to customize analytical models to identify fraud, waste and abuse not found by existing business rules.
- Enables easy management of the deployment, aggregation, scheduling, suppression and routing of similar rules across multiple factors, such as parties, data sources and business lines.
- Lets users run groups of rules and models alone, in parallel or at different times (intraday, daily, weekly, monthly, etc.).
- Facilitates collaboration with other business units (e.g., member cost management, chronic condition management, operations analytics) on model development.

Detection and alert generation

- Calculates the propensity for fraud at first submission, then rescores claims at each processing stage as new claims data is captured.
- Reviews claims early in the adjudication process so you can stop suspicious activity at the prepayment stage.
- Enables you to incorporate fraud detection methods into the process at the most appropriate points – e.g., cases where anomaly detection scenarios may require data that is not available until later in the adjudication process.

Alert management

- Combines alerts from multiple monitoring systems, associates them with common individuals and provides a more complete perspective on the risk of particular individuals or groups.
- Prioritizes the investigative order of alerts by scoring them in real time, based on specific characteristics.
- Automatically routes alerts to appropriate team members based on user-set rules and requirements.
- Displays all evidence for each case on a dashboard that you can customize to accommodate your investigative unit's processes.

Social network analysis

- Provides a unique network visualization interface that lets you go beyond transaction and account views to analyze related activities and relationships at a network dimension, and identify linkages among seemingly unrelated claims.
- Enables you to produce complete dossiers of networks surrounding a case, and gain fast access to full details on all related parties and networks.
- Produces independent and combined fraud scores, so you can assess overall risk on a customer, claim or network basis.
- Increases investigator effectiveness by enabling investigators to merge and delete network entities, and add annotations (text and images) to specific entities in a network.
- Provides time slider functionality, which enables you to see how activity in a network develops over a time horizon.

Search and discovery

- Enables free-text, field-based or geospatial searches across all data (internal and external).
- Lets you refine searches using interactive filters and facets that are purposed for the SIU team.
- Provides an intuitive interface that lets you construct complex queries without the need to understand specific syntax. For example, you can use fuzzy searching, proximity searching and field boosting while restricting searches to specific entity types, fields, comments or insights.

Intelligent case management

- Systematically facilitates investigations using a configurable workflow.
- Stores all information pertinent to a case, including detailed investigation information – e.g., interview notes and evidence for criminal or civil prosecution, restitution and collections.
- Assesses overall fraud exposure, including losses due to fraud as well as fraud detected or prevented.

Flexible deployment options and analytical services

- Enables faster implementation (and faster ROI) when installed and administered at the SAS hosting site, eliminating the need for payer staff to oversee the system.
- Can be hosted at your site, in which case SAS Professional Services staff will assist with the implementation and provide training.
- Can be fully integrated with your existing operations environment, workflow solution and business process management objectives, including thorough business process discovery and review to ensure your objectives are met or exceeded.

Key benefits include:

Proactively detect more fraudulent activity

- Insert analytical models into the process, in addition to rules engines.
- Process all data (not just a sample) through rules and analytical models.
- Leverage advanced data mining and machine learning algorithms.
- Use customized models to detect previously unknown schemes.
- Spot linked entities and crime rings, which can help stem larger losses.

Reduce false positives and increase investigator efficiency

- Apply risk-based scoring to model output before it goes to investigators.
- Enable investigators to work more cases than ever before.

Lower fraud losses while increasing recoveries

- Prevent fraud before claims are paid using online, real-time probability risk scoring:
    - Detect loss padding in similar claims using anomaly and loss comparisons.
    - Identify repeat offenders and score incoming data more accurately by searching databases of known fraudsters and recording outcomes, claims settlement amounts, referrals and suspects for future reference.
- Uncover insider fraud by integrating staff data and audit records showing who handled claims.
- Focus investigations on higher-value networks and alerts by using risk- and value-based scoring models.
- Gain real-time access to information by inserting analytical models into your process workflow

Gain a consolidated view of fraud risk and improper payments

- Continually improve models and adapt the system to address changes in fraud trends.
- Manage waste, abuse and improper payments at the operations level by differentiating from fraud and routing for resolution.

- Better understand new threats and prevent big losses early using social network diagrams and sophisticated data mining capabilities.

Functionality

Table 3: Functionality

Function	In Production with Clients	Supported, But Not in Production with Clients	Not Supported
Data			
Aggregate historical data from different internal databases	●		
Integrate with external data capture tools (IoT, wearables, sensors, etc.)	●		
Consolidate data coming from external databases	●		
Data quality checking tools	●		
Automatic data adjustment prompts (unstructured, inconsistent, or redundant data)	●		
Uses additional hardware infrastructure in the cloud to run models on large amount of data	●		
Model Configuration			
Reusable, sharable rules, variables, and models	●		
Rules, variables, and models repository (searchable, version controlled)	●		
Compare multiple scenarios/models	●		
Real time fraud scoring service	●		
Create multivariable-based algorithms	●		
Schedule model run-time	●		
Prioritize model updates and model results (for instance, when multiple results are displayed on a shareable dashboard)	●		
Claims Fraud Detection Techniques and Claims-Related Models			
Fraud pattern identification	●		
Anomaly detection	●		

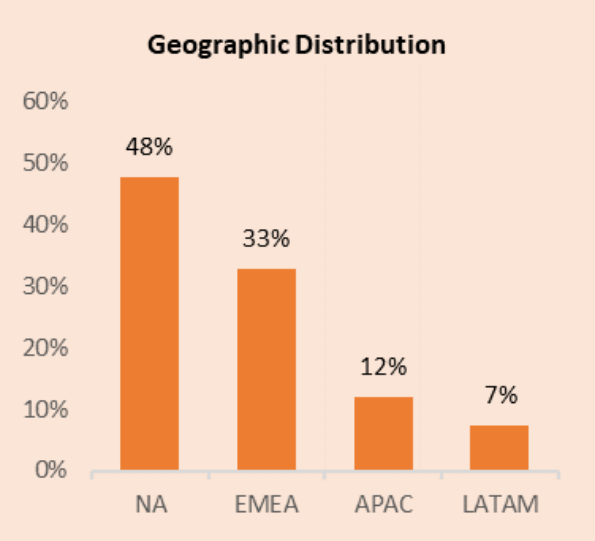
Social network analysis	●
Claims severity modeling	●
Claims frequency modeling	●
Claims settlement optimization	●
Special Investigation Unit (SIU) features	
Design and update monitoring dashboards	●
Assign/share fraud cases with other investigators	●
Check fraud case logs (status changes, audit trails, etc.)	●

● = Available out of the box
● = Configurable through a scripting language/coding
● = Under development/On road map
● = Configurable using simple tools for business user
● = Available with integration to a third party solution
● = Could develop—would be considered customization
● = Configurable using simple tools for IT user
● = Available with integration to a separate module provided by this vendor
● = Not available/Not applicable

Source: Vendor RFI

Customer Base

Figure 1: Client Base by Geography



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Not disclosed
Database	DB2, Oracle, Postgresql, SQL
Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed
Integration Methods	Web services, HTML, HTTP, RESTful HTTP style services, JSON format, Custom APIs, native messaging

Source: Vendor RFI

Table 5 SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✔
Amazon AWS	✔
Google Cloud Platform (GCP)	✔
Alibaba Cloud	✔
IBM Cloud / Bluemix	✔
Oracle Cloud	✔
Salesforce Cloud, Force.com, AppExchange	✔
Other	✕

Legend: ✔ = In production; ☐ = Supported but not in production; ✕ = Not supported

Source: Vendor RFI

Configuration

Table 7: Change Tooling and Upgrades

Types of Changes	Availability
Business Rule Definition	✔
Data Definition	✔
Table Maintenance, List of Values, etc.	✔

Types of Changes	Availability
Interface Definition	✔
Product Definition	☐
Role-Based Security, Access Control, and Authorizations	✔
Screen Definition	✔

Legend: ✔ = Configurable via tools for business users; ☐ = Configurable via tools for IT users; ■ = Configurable via the vendor; ⊖ = Configurable via scripting; ● = Coding required; ✕ = Not available

Source: Vendor RFI

Data

SAS' data model is proprietary.

Regarding industry standard data model schemas, the vendor states FHIR, HL7, USCDI, NCPDP.

The database was designed from the ground up for this product.

The solution uses a standard data model design that can be extended using standard RDBMS tools. The data model can be released to the client and can map to an intermediate format to share with a client (such as an industry standard).

The solution uses a standard data model design that can be extended using standard RDBMS tools. While SAS allows client-specific changes, it discourages them because of the potential impact in migrating to newer releases of the solution.

SAS provides data lineage capabilities to help document and manage metadata across systems—from both SAS and third party tools—transformation jobs, and data models. SAS helps clients build the set of policies, processes, and boundaries to holistically manage their data, helping their organizations achieve consistency and transparency for the long term.

Security

The vendor is not PCI compliant.

Security tokens/pins, biometric security support, multifactor authentication, and federated identity support are available as authentication factors for internal and external users.

The system does not have penetration security.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Accenture, Deloitte, DXC, KPMG, and Optum.

Fintech Partners	Guidewire, Duck Creek, ISO, NICB, ThreatMetrix, GIACT, Plaid, Boku, Prove, Intellicheck, BioCatch, Datavisor, Iovation, and Socure.

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
Resource Breakdown	Vendor: 70%; Insurer: 30%; Third party: 0%
Location of Employees	SAS has employees in North America, EMEA, APAC, and LATAM, with 200 in North America, 110 in EMEA, 50 in APAC, and 40 in Latin America
Average Time to Implementation	Initial implementation: 4 to 6 months Second and subsequent line of business: 1 to 3 months Second and subsequent states/jurisdictions: 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Subscription-based license: preferred option
Factors Used to Determine Pricing	Usage-based factors: Number of concurrent users, Annual premium volumes/revenues Tier-based factors: Tiered Price Functional components/modules, Jurisdictions (States/Provinces/Countries), Annual premium volume/revenues

Source: Vendor RFI

Pricing

The following table shows the average total costs of the vendor's current client base. This includes costs associated with the software license or subscription, initial installation, customization, annual maintenance, and training in the first year. It also estimates the remaining costs for full implementation, including license fees, maintenance, customization, and other fees.

Table 10: Five-Year Pricing Estimates for North America

Average Total Costs	Licensing/Subscription	Implementation	All Other
Average Year One Costs	Not disclosed	Not disclosed	Not disclosed
Average Remaining Costs (Year Two and Beyond)	Not disclosed	Not disclosed	Not disclosed

Source: Vendor RFI

PATH FORWARD

Insurance fraud is an age-old problem that will never cease to exist, but today's carriers have an opportunity to leverage solutions that will help them to at least mitigate the costly problem. Celent strongly suggests carriers employ fraud-detection tools as they are vital resources with a proven ROI.

For Insurers

There is no "one-size-fits-all" fraud detection solution, but there are myriad options to fit almost any set of requirements. An insurer seeking a fraud detection solution should begin the process by looking inward and outward. Every insurer has its own unique business objectives, mix of lines of business, staff capabilities and financial resources. This unique combination of these factors, along with the organization's risk appetite, will influence the list of vendors for consideration.

Some vendors are a better fit for an insurance company with a large IT group that is deeply proficient with the most modern platforms and tools. Other vendors are a better fit for a company that has a small IT group and wants a vendor to take a leading role in maintaining and supporting its applications.

We recommend that insurers looking for a fraud detection solution narrow their choices by focusing on four areas:

- *The technology:* Leading fraud detection tools have invested in AI/ML to create real-time fraud scoring models. Carriers should be aware of their business needs and the solution's capabilities to ensure the tool is best aligned with their objectives. It should be noted that not all carriers need the most cutting-edge fraud detection tools.
- *The functional capabilities:* It is important to understand the functionality needed and available out of box. Carriers should also check to see what is actually in production.
- *The vendor's stability, knowledge, and investment in the solution:* Consider the partnership dimension carefully. Key functional gaps are quickly closed by leading vendors.
- *Implementation and support capabilities and experience:* The relationship between an insurer and its fraud detection platform vendor will likely last a few years or more. Celent can help with selection projects; we know the vendors and the markets well.

For Vendors

Solution providers have invested significantly in bolstering their capabilities and differentiating themselves from their peers. The result is a maturing solution environment. The leading vendors have strong AI/ML capabilities, are delivering robust functionality, employ open application programming interfaces (APIs) for ease of integration, and are cloud ready.

Celent recommends vendors differentiate themselves by:

- Developing increasingly useful AI/ML models that can effectively make decisions.
- Continuing to move to open APIs and other integration frameworks to drive the easy orchestration of processes and data across external digital capabilities.
- Focusing on improving usability for both new and experienced users and managers.
- Making implementation faster and less expensive. It may be worth considering pre-integrating with a core claims system vendor.
- Continuing to expand functionality—especially in different lines of business and in the use of AI and analytics capabilities.
- Investing in embedding cloud-native capabilities into the product.

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 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 and requirements. 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.

© CELENT

RELATED CELENT RESEARCH

Insurance Fraud-Detection Solutions: P&C Insurance, 2022 Edition
September 2022

Insurance Fraud-Detection Solutions: Life Insurance, 2022 Edition
September 2022

Moving to Group Health Insurance: IT Architecture Alignment
September 2022

Healthtechs that are Changing Your World
August 2022

Claims Fraud Detection Systems: 2018 IT Vendor Spectrum
May 2018

Health Insurance Claims Fraud Detection Systems
March 2015

© CELENT

COPYRIGHT NOTICE

Copyright 2022 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

For more information, please contact info@celent.com or:

Andrew Schwartz aschwartz@celent.com
Fabio Sarrico fsarrico@celent.com

Americas

USA
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.424.3200

USA
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.8000

USA
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7800

Brazil
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

+55 11 3878 2000

EMEA

Switzerland
Tessinerplatz 5
Zurich 8027

+41.44.5533.333

France
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Italy
Galleria San Babila 4B
Milan 20122

+39.02.305.771

United Kingdom
55 Baker Street
London W1U 8EW

+44.20.7333.8333

Asia-Pacific

Japan
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokyo 107-6216

+81.3.6871.7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapore
138 Market Street
#07-01 CapitaGreen
Singapore 048946

+65 6510 9700