

CELENT

INSURANCE FRAUD- DETECTION SOLUTIONS: PROPERTY AND CASUALTY INSURANCE, 2022 EDITION

A Celent SolutionScape, powered by VendorMatch

Andrew Schwartz and Fabio Sarrico

September 30, 2022

CONTENTS

Contents	2
Executive Summary	3
Introduction.....	5
Key Resources and Capabilities of A Fraud-Detection Platform	10
Report Methodology	12
P&C Fraud-Detection Solution Providers	13
Celent Technical Capability Matrix	16
Vendor Profiles	18
Appian: Appian Fraud Detection.....	19
Charlee.ai.....	31
CRIF: Sherlock	39
FraudKeeper: FraudKeeper	48
FRISS: Fraud Detection at Claims	56
Hugin: Bayes Fraud	67
LexisNexis Risk Solutions, Inc.: Accurint® for Insurance	74
SAS: SAS® Detection and Investigation for Insurance.....	81
Shift Technology: Shift Claims Fraud Detection	92
Verisk: Verisk’s Fraud Solutions.....	101
Path Forward	109
Leveraging Celent’s Expertise	111
Related Celent Research	112
Copyright Notice	113

EXECUTIVE SUMMARY

A claims fraud-detection system helps insurance carriers identify fraudulent claims, at both the individual and organizational levels. It is typically used by claims teams and in special investigative units (SIU). 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 carriers the confidence to quickly indemnify claims that are deemed valid.

This report provides an overview of fraud-detection solutions for property-casualty insurance carriers. The report profiles 11 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 property-casualty 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.

The following vendors and solutions are included in this report:

- Appian: Appian Fraud Detection
- Charlee.ai: Charlee.ai
- Cogitate Technology: CFNA
- CRIF: Sherlock
- FraudKeeper: FraudKeeper
- Friss: Fraud Detection at Claims
- HUGIN: Bayes Fraud
- LexisNexis Risk Solutions, Inc.: Accurint® for Insurance
- SAS: SAS® Detection and Investigation for Insurance
- Shift Technology: Shift Claims Fraud Detection
- Verisk: Verisk's Fraud Solutions

While this list is not exhaustive, Celent believes it provides a valuable sampling of vendors.

The goal of this report is to help property-casualty insurers to 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.

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.

While insurance fraud has existed for thousands of years, today’s actors are more sophisticated than ever before. Organized crime rings have, in many instances, been able to scam insurance carriers for large sums of money. According to the Coalition Against Insurance Fraud, 10% of property-casualty insurance losses are estimated to be fraudulent.¹ Industry estimates indicate \$500 billion in property-casualty claims were paid out in 2021, which would mean approximately \$50 billion in claims were fraudulent.²

While organized fraud accounts for a significant portion of false claims payouts, the incidence of “soft fraud,” the padding of a legitimate claim, is rampant and arguably more damaging. In a poll by the Insurance Research Council, 24% of respondents in the United States believe it is acceptable to inflate an insurance claim to make up for their deductible.³ And that is just those who were not too embarrassed to admit it. Overall, soft fraud is estimated to cost insurers a staggering \$32 billion a year.⁴

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

² <https://www.iii.org/fact-statistic/facts-statistics-industry-overview>

³ <http://www.insurancejournal.com/news/national/2013/03/20/285243.htm>

⁴ <https://www.iii.org/article/background-on-insurance-fraud>

Figure 1: Fraud by the Numbers

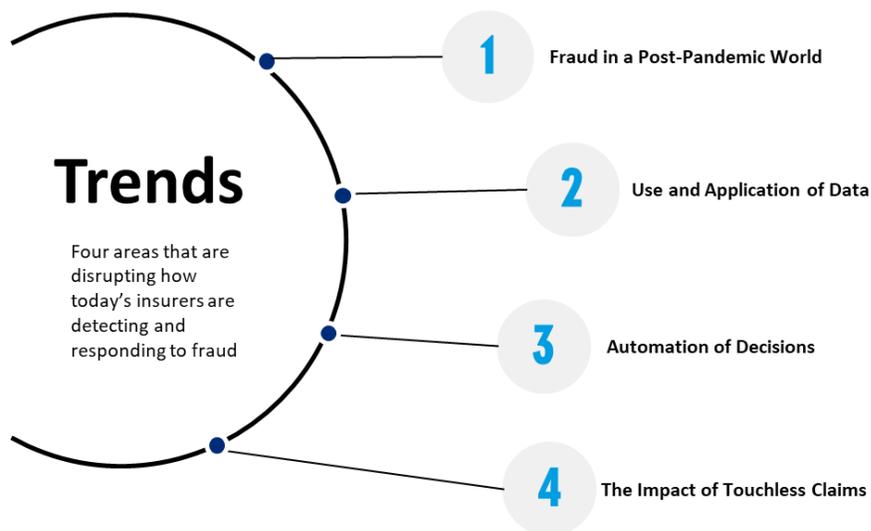


Source: Celent

Trends Impacting P&C Insurance Fraud

Celent believes there are four major trends that are impacting how insurers are detecting and responding to fraud. Accordingly, today’s leading vendors in the fraud-detection space have made valiant strides over the last several years to provide solutions that support carriers. Figure 2 outlines four trends that are disrupting how insurers are detecting and responding to fraud.

Figure 2: Trends Impacting Fraud



Source: Celent

Fraud in a Post-Pandemic World

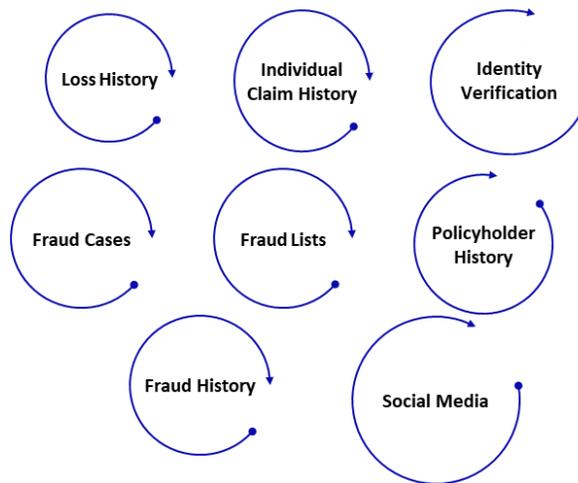
The pandemic has had a profound impact on the ways in which individuals interact with others and conduct business. Insurance carriers are no exception. With the shift to digital, claims have increasingly been submitted and handled through different, typically more remote, channels. By allowing the policyholder to submit a claim without a human adjuster, there may be increased vulnerabilities to claims fraud. As such, there may be an increased need for fraud-detection tools that can act as guardrails.

Additionally, the “great resignation” has altered the make-up of some organizations. Without a sufficient number of seasoned adjusters who are trained to detect signs of fraud, and combined with the limited number of young employees coming into the workforce, there may be increased reliance on fraud-detection tools as well.

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, carriers 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 carriers 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 3: Data Points that May Inform Fraud Detection

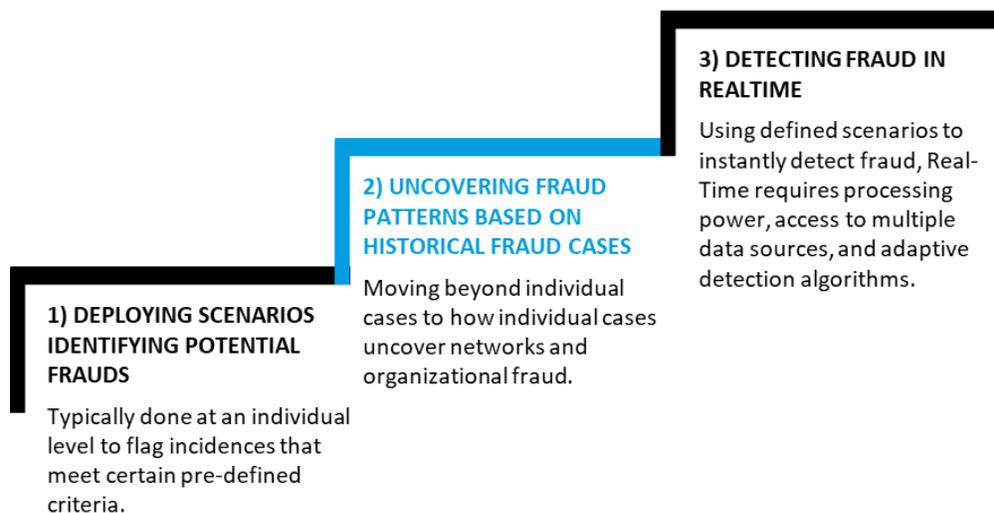


Source: Celent

Automation of Decisions

Today’s advanced fraud tools are going beyond simply providing information for an adjuster or SIU employee to decipher. Directionally, they are moving from showing what happened to making intelligent automated decisions based on the fraud model. Figure 4 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 4: Evolution of AI in Fraud-Detection Tools



Source: Celent

The Impact of Touchless Claims

Many carriers have been moving toward removing human touchpoints in the claims process to create an either touchless or partially touchless claims process. With fewer interactions, there is a perceived increased susceptibility to fraud. In Celent's joint survey⁵ with PropertyCasualty360.com on industry attitudes toward touchless claims, respondents were asked to rank eight possible barriers to the adoption of touchless claims. The results indicated that among SIU and adjuster staff, fraudulent behavior was ranked as the No. 1 barrier. To assuage these concerns and create a claims process that is seamless but also protects the carrier, many are looking toward employing real time fraud detection. Having an effective and fully auditable fraud-detection tools can lead to increased organizational buy-in and more confidence in claims that are automated.

⁵ <https://www.celent.com/insights/356012498>

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Claims fraud pattern identification. • Anomaly detection.

FUNCTION	FEATURES
	<ul style="list-style-type: none"> • Social network analysis. • Claims severity modeling. • Claims frequency modeling. • Claims settlement optimization.
Special investigation unit (SIU) features	<ul style="list-style-type: none"> • 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 P&C 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 11 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 P&C 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.

P&C FRAUD-DETECTION SOLUTION PROVIDERS

The Solution Market

Each vendor in this report offers a fraud-detection solution for P&C carriers.

Table 1: Snapshot of P&C Insurance Fraud-Detection Solutions

VENDOR	PRODUCT
Appian	Appian Fraud Detection
Charlee.ai	Charlee.ai
Cogitate Technology	CFNA
CRIF	Sherlock
FraudKeeper	FraudKeeper
Friss	Fraud Detection at Claims
HUGIN	Bayes Fraud
LexisNexis Risk Solutions, Inc.	Accurint® for Insurance
SAS	SAS® Detection and Investigation for Insurance
Shift Technology	Shift Claims Fraud Detection
Verisk	Verisk's Fraud Solutions

Source: Vendor RFIs

Table 2: Claims Fraud-Detection Technique Availability

Vendor	Product	Pattern Identification	Anomaly Detection	Social Network Analysis	Severity Modeling	Frequency Modeling
Appian	Appian Fraud Detection	☒	☒	✓	✓	✓
Charlee.AI	Charlee.ai	✓	✓	✓	✓	✓
Cogitate Technology	CFNA	✓	✓	✗	✓	✓
CRIF	Sherlock	✓	✓	✗	✓	✓
FraudKeeper	FraudKeeper	✓	✓	✓	✓	✓
Friss	Fraud Detection at Claims	✓	✓	✓	✓	✓
HUGIN	Bayes Fraud	✓	✓	✓	✓	✓
LexisNexis Risk Solutions, Inc.	Accurint for Insurance	✗	✗	✓	✗	✗
SAS	SAS Detection and Investigation for Insurance	✓	✓	✓	✓	✓
Shift Technology	Shift Claims Fraud Detection	✓	✓	✓	✓	✓
Verisk	Verisk's Fraud Solutions	✓	✓	✓	✓	✓

✓ = Available within the solution; ☒ = Available with integration to a third party solution; ☐ = Available with integration to another solution provided by this vendor; ✗ = Not supported

Source: Vendor RFIs

Table 3: Public Cloud Options

Vendor	Azure	AWS	Google Cloud	Alibaba Cloud	IBM Cloud	Oracle Cloud	Salesforce Cloud	Other
Appian	Not disclosed							
Charlee.AI	✓	✓	✓	✗	✗	✗	✗	✗
Cogitate Technology	✓	✗	✗	✗	✗	✗	✗	✗
CRIF	✓	✓	✓	✗	✗	✗	✗	✗
FraudKeeper	✓	✗	✗	✗	✗	✗	✗	✗
Friss	✓	✓	✗	✗	✗	✗	✗	✗
HUGIN	✗	✗	✗	✗	✗	✗	✗	✗
LexisNexis Risk Solutions, Inc.	✓	✗	✗	✗	✗	✗	✗	✗
SAS	✓	✓	✓	✓	✓	✓	✓	✗
Shift Technology	✓	✓	✗	✗	✗	✗	✗	✓
Verisk	✗	✓	✗	✗	✗	✗	✗	✗

✓ = Supported;; ✗ = Not supported

Source: Vendor RFIs

CELENT TECHNICAL CAPABILITY MATRIX

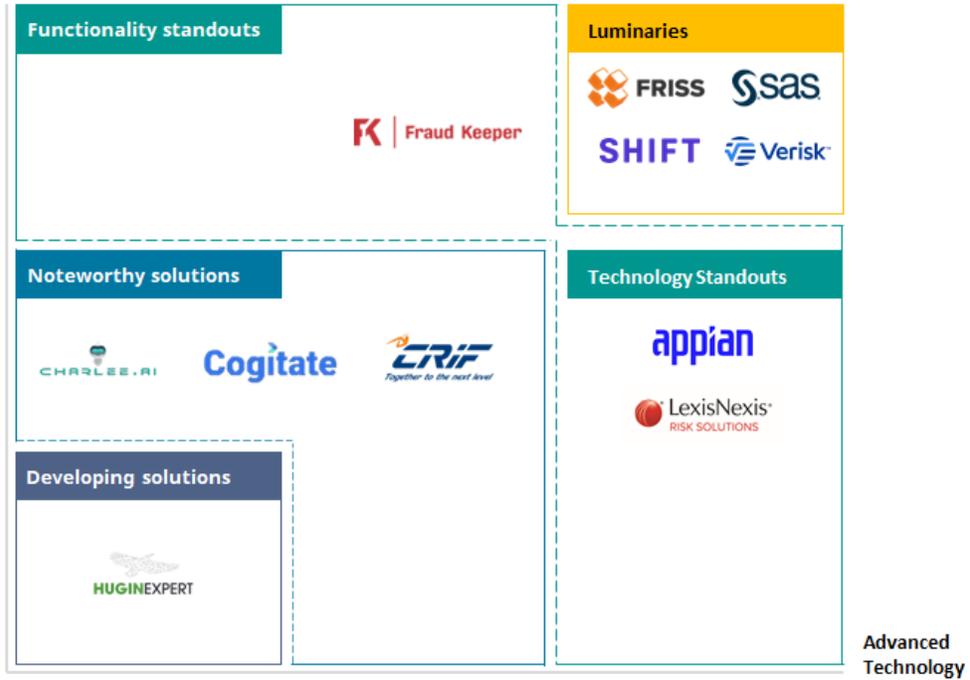
New to Celent's solution reports this year is the Technical Capability Matrix. We have placed each solution into one of five categories based on the sophistication and breadth of its technology and functionality (i.e., plotting the A and B dimensions). Solutions are not ranked within the assigned category;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

Figure 1: Celent Technical Capability Matrix

Breadth of
Functionality



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.

APPIAN: APPIAN FRAUD DETECTION

Company and Product Snapshot

Appian is a public company headquartered in Virginia, US, with sales and professional services personnel located throughout North America, Latin America, Africa, Middle East, Europe, and Asia Pacific. The company has 2,000 employees, of whom 484 are available to provide professional services/client support for the Appian Fraud Detection solution.

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

Table 1: Company Snapshot

Year Founded	1999
Number of Employees	2,000
Revenues (USD)	\$369.3 million (2021)
Financial Structure	Public company Nasdaq: APPN
VendorMatch Link	https://www.celent.com/vendormatch/discovery/vendors/appian/solutions
User Conferences	The vendor offers an annual user conference or customer event.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Appian Fraud Detection
Year Originally Released	2004
Current Release and Date of Release	22.2/2022
Revenue Derived from the Product	Appian's subscription revenue for 2021 was \$179.4 million. Appian's total revenue for 2021 was \$369.3 million.
R&D Expense	Not disclosed
FTEs Providing Professional Services for Product	484
Regional FTEs (NA/EMEA/APAC/LATAM)	253/135/31/01
Target Market	Appian targets global enterprises that need an enterprise standard platform for rapid application development and process automation. Insurance organizations like Aon, Cigna, CNA, Pacific Life, and Aviva use Appian to create mission-critical

business applications with enterprise-wide deployments that cut across various lines of business, geographies, and the front/back offices.

Appian is used in every industry vertical, but insurance, banking, and capital markets make up its largest business segments. These areas are covered by dedicated industry sales and marketing teams, led by industry-sourced subject matter experts.

Relevant insurance industry solutions and use cases can be found here:
www.appian.com/insurance.

Appian sells equally to business and IT leaders at the director level or above, with developers as the key influencer persona. It sells to them by showing how custom low-code automation applies to 150+ industry-specific use cases that they care about. For example, Appian highlights claims management and connected underwriting for insurers, customer onboarding for banks, and new product development for capital markets.

Appian also has a global presence with 20 offices in North America, EMEA, and APAC. Thirty-four percent of Appian's total revenue came from outside the US in 2020.

Installed Base	Confidential
Notable Clients	AON, Aviva, CAN, Pacific Life, SSQ, Cigna
Source: Vendor RFI	

Overview

The vendor states that the Appian Low-Code Automation Platform integrates end-to-end process automation, data, and rapid visual application development natively in the cloud. The platform is specifically designed to meet the needs of sophisticated

enterprises, regardless of where they are on the digital maturity journey, and is used by some of the largest banking, capital markets, and insurance companies in the world. When clients create apps with the Low-Code Automation Platform, they should expect to build apps 10x faster, reduce maintenance costs by 50%, and gain superior functionality compared to traditional development. Only the Appian Guarantee provides a focused eight-week delivery period for a client's first application project with a flat services fee. Appian also guarantees that anyone technical can be trained as an Appian developer in two weeks. The Appian Guarantee includes clearly documented guidelines, full use of Appian standard features, collaborative application design, implementation best practices, and more to ensure successful delivery.

Key features include:

- *Low-Code Application Development: Go from idea to implementation fast with visual design tools that increase business and IT collaboration.*
- *Build Once, Deploy Anywhere: Create powerful experiences that automatically work across mobile devices and digital touchpoints.*
- *Workflow: Orchestrate all of a client's resources into a single workflow, driving productivity and exceptional customer and employee experiences with comprehensive business process management capabilities.*
- *Process Mining: Discover how clients can reduce costs, increase efficiency, and optimize processes.*
- *Low-Code Data: Integrate data from anywhere without expensive migrations for unified and actionable data.*
- *Low-Code Robotic Process Automation (RPA): Build bots quickly to handle high-volume, repetitive tasks so people can focus on the work that matters most.*
- *Artificial Intelligence: Add intelligence with best-of-breed AI services from Appian or the vendor of client's choice to classify documents, extract data, embed next best action, and more.*
- *Case Management: Handle exceptions and ad hoc activities with task management and actionable data views for improved performance.*
- *Business Rules: Define and automate complex business logic with zero coding.*
- *World-Class Cloud Security: Appian Cloud is built from the ground up for security, scalability, and reliability, meeting multiple industry security standards for compliance and data privacy.*

Key benefits include:

- *Faster Claim Settlement: A holistic view of data from all systems, plus omnichannel intake capability and prebuilt claims journey.*
- *High Flexibility and Agility: Add new lines of business through self-service configurations, and customize the claims journey for any line of business (LOB).*
- *Superior Customer Service: Appian Connected Claims brings a 360 degree view of the customer and their data, and pairs easily with Amazon Connect, an easy-to-use omnichannel cloud contact center for voice, chat, and task management.*
- *Prevent Fraud: Optimize fraud case management with a unified view and full control of all potential fraud alerts for special investigative unit (SIU) teams.*
- *Unified Data: Easily integrate with existing claims and policy systems to gain full visibility into the claims lifecycle in one dashboard.*
- *Stay Agile: Dramatically reduce time and cost to implement with the speed and power of the Appian Low-Code Platform.*

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, Size, Type of Insurer, and Deployment Type (Global)

Not disclosed

Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Java: 35%; JavaScript: 35%
Database	DB2, Kdb+, MongoDB, NoSQL, 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, XML (not through web services), HTML, HTTP, RESTful HTTP style services, JSON format, MQSeries, JMS or similar queue technology, custom APIs, flat files, native messaging, other integration methods

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	No
Type of effort required to update the solution	Evergreen—client chooses when to upgrade
Cadence of upgrades for multitenant deployments	Every three months
Deployment approach supports elasticity	Yes, within less than a day
Current API-related strategy	Pre-connected cloud environment (fully connected and ready to use)
Deployment model can leverage a serverless approach	Yes
Solution enables independent services (microservices)	Yes
Proportion of the system architected as microservices	Over 80%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	Yes
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	Not Disclosed
Amazon Web Services (AWS)	Not Disclosed
Google Cloud Platform (GCP)	Not Disclosed
Alibaba Cloud	Not Disclosed
IBM Cloud/Bluemix	Not Disclosed
Oracle Cloud	Not Disclosed
Salesforce Cloud, Force.com, AppExchange	Not Disclosed
Other	Not Disclosed

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.	✓
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

Appian's data model is not proprietary.

Regarding industry standard data model schemas, the vendor states Appian can be used in conjunction with any industry data model. The low-code data flexibility allows the company to use any data model or even use multiples data models.

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

Appian uses a low-code data approach including:

- Visual modeling tools for defining data models.

- Autodiscovery of data models from databases like SQL Server, Oracle, IBM, MySQL, and MariaDB as well as Salesforce or Web Services. The data model can be released to the client, can be easily published to a client's data model, and can map to an intermediate format to share with a client (such as an industry standard).

Appian provides a graphic interface to add or update fields as well as tables. It is also possible to make relationships that are coming from other systems.

Appian will also auto detect data model changes from underlying databases and auto update the offering with the latest changes.

Customers can implement their data models on the Appian Platform. They can reuse existing data models and/or use industry standard data models.

Security

Appian complies with the following security standards: Appian invests millions of dollars each year in quarterly third party security audits and in maintaining the deepest set of security certifications in the low-code market.

Appian maintains the following certifications: ISO27001, ISO27017, ISO27018, HiTRUST, DISA Level 2, DISA Level 4, FedRAMP Level 2, GDPR, HIPAA, SOC1/2/3, PCI-DSS, FISMA, UK G-Cloud, GxP, Cloud Security Alliance, EU-US and Swiss-US Privacy Shield Frameworks, FDA, 508/VPAT, ENS High-Level, and Qualys SSL Labs.

For more information, see <https://appian.com/why-appian/trust/compliance.html>.

In addition to these certifications, Appian's world-class security program includes the following:

Security Controls: Align to leading NIST, PCI, and other frameworks via access controls and authentication, audits, contingency planning, incident response, personnel and physical security, risk assessment, system acquisition and integrity, and systems communication protection.

Authentication: SAML, LDAP, Active Directory. PCI DSS compliant login and password management features. Virtual private network (VPN) for extending clients' data center. Bring Client's Own Key (BYOK) to secure the disk that stores clients' data. Role-based, delegated administration platform security.

Storage & Tenancy Protocol: Local geography hosting, data segmentation, application segmentation, data replication within the same region, tenant instance isolation, and regulatory compliance.

Continuous Monitoring: Continuous security monitoring for advanced threats, security notifications, performance and health, platform response times, uptime/availability, and compliance auditing.

Defense-in-Depth Protection: Multiple layers of security that apply defense-in-depth security strategy to the global infrastructure, including network intrusion detection system (IDS), host

IDS, web application firewall, network layer firewalls, file integrity monitoring, and strict access controls between infrastructure tiers.

Encryption & Data Isolation: Security of data in transit and at rest using strong encryption via transport layer security (TLS) for end-user connections and disk encryption to secure data at rest. Customer data backups are encrypted, secure connection channels with customer data sources, and each customer is allocated virtual server(s) and virtual drive(s) for application server, Appian application, and database use—these are never shared with other customers.

Vulnerability Testing: Appian contracts with an independent expert security firm to perform tests on Appian Cloud including vulnerability scanning, internal penetration testing, external penetration testing, and isolation architecture exploitation. Customers are encouraged to perform their own vulnerability testing.

Personnel: Appian Cloud personnel are located alongside their services and engineering staff in the US, Australia, and the UK. A formal screening process includes a required background check. There is extensive cloud security training and continuous training on operational practices.

Security Incident Reporting: Appian takes security seriously. It encourages reporting security vulnerabilities and security incidents to Appian. All submissions are investigated by the Security Incident Response Team. Appian takes appropriate action in the form of hotfixes, upgrades, or published mitigation information. Appian notifies affected customers.

For more information, see <https://appian.com/why-appian/trust/security.html>.

The vendor is PCI compliant, and this is achieved by The Payment Card Industry (PCI) Security Standards Council offers standards to enhance payment card data security. The PCI Data Security Standard (PCI DSS) provides a framework for developing a robust payment card data security process, including prevention, detection, and appropriate handling of security incidents.

Customers can leverage Appian Cloud's PCI-DSS certification to reduce their own PCI compliance complexity after agreeing to the Appian Cloud PCI-DSS terms.

Appian Cloud has been assessed by an external independent auditor and is compliant with PCI-DSS.

For more information, see <https://appian.com/why-appian/trust/compliance.html>.

One-time passwords, flexible user permissioning, out of band identification, security tokens/pins, biometric security support, multifactor authentication, and federated identity support are available as authentication factors for internal and external users..

For cybersecurity arrangements, Appian contracts an independent expert security firm to perform tests on Appian Cloud including, vulnerability scanning, internal penetration testing, external penetration testing, isolation architecture exploitation. Customers are encouraged to perform their own vulnerability testing.

The system has penetration security by Appian contracts an independent expert security firm to perform tests on Appian Cloud, including vulnerability scanning, internal penetration

testing, external penetration testing, and isolation architecture exploitation. Customers are encouraged to perform their own vulnerability testing.

Documentation of quarterly security audits can be available upon request.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	<p>Appian has a global network of 573 delivery partners, including global alliances with KPMG, Accenture, Deloitte, Atos, Wipro, Cognizant, PwC, HCL Technologies, Capgemini, Tata Consultancy Services (TCS), Perficient, Infosys, EPAM, and Persistent.</p> <p>All of these SIs have dedicated Appian COEs. There are 15,000+ certified individuals in these organizations for Appian implementation and support services.</p> <p>In addition to providing implementation and support services, all of these partners offer prebuilt solutions created on the Appian platform, engage in joint go-to-market activities, and/or sponsor Appian events. Many of these partner-built solutions are listed on their public AppMarket. Examples include:</p> <p>KPMG: Insurance Claims Modernization: https://community.appian.com/b/appmarket/posts/kpmg-insurance-claims-modernization</p> <p>TCS: Retail Loan Origination System: https://community.appian.com/b/appmarket/posts/retail-loan-origination-system</p> <p>Wipro: EUC Remediation Framework: https://community.appian.com/b/appmarket/posts/euc-remediation-framework</p> <p>Persistent: Revenue Cycle Optimization: https://community.appian.com/b/appmarket/posts/revenue-cycle-optimization</p> <p>Vuram: VATT Test Automation: https://community.appian.com/b/appmarket/posts/vatt---appian-rpa</p> <p>Princeton Blue: Automated Vendor Onboarding with RPA:</p>

Appcino: Sanctions & Adverse Media Screening:
<https://community.appian.com/b/appmarket/posts/sanctions-and-adverse-media-screening>
 Cognizant: Smart Grid Maintenance:
<https://community.appian.com/b/appmarket/posts/smart-grid-maintenance>
 ...and more

Fintech Partners	InsurTech/FinTech: Shift, Swiss Re, Jumio, Galaxy AI, SWIFT, Dow Jones, Bloomberg, Quantexa, Dun & Bradstreet, NorthRow, Companies House, OFAC
-------------------------	--

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	6 to 10
Resource Breakdown	Not disclosed
Location of Employees	Appian has employees in North America, EMEA, APAC, and LATAM, with 253 in North America, 135 in EMEA, and 31 in APAC.
Average Time to Implementation	<u>Initial implementation</u> : 1 to 3 months <u>Second and subsequent line of business</u> : 1 to 3 months <u>Second and subsequent states/jurisdictions</u> : 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Term license, enterprise license, subscription based license
Factors Used to Determine Pricing	<u>Usage-based factors</u> : Number of concurrent users, number of total or named users, per active user/seat, per user/seat <u>Tier-based factors</u> : None <u>Other factors</u> : Flat pricing, freemium entry level followed by a standard pricing plan

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	US\$100,001 to US\$250,000	Not disclosed	Not disclosed
Average Remaining Costs (Year Two and Beyond)	Not disclosed	Not disclosed	Not disclosed

Source: Vendor RFI

CHARLEE.AI: CHARLEE.AI

Company and Product Snapshot

Charlee.ai is a private company headquartered in California, US, with sales and professional services personnel located throughout North America and India. The company has 20 to 40 employees, of whom 15 are available to provide professional services/client support for their Charlee.ai solution.

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

Table 1: Company Snapshot

Year Founded	2016
Number of Employees	20 to 40
Revenues (USD)	Charlee.ai is a privately held company and does not disclose that information.
Financial Structure	Private
VendorMatch Link	https://www.celent.com/solutions/343171754
User Conferences	No annual conference or customer event is offered.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Charlee.ai
Year Originally Released	2016
Current Release and Date of Release	Charlee.ai 3.0/2022
Revenue Derived from the Product	Charlee.ai is the core product, and all revenue is derived from it.
R&D Expense	The vendor targets between 12% and 15% each year.
FTEs Providing Professional Services for Product	15
Regional FTEs (NA/EMEA/APAC/LATAM)	8/0/7/0
Target Market	The target market includes property and casualty insurance companies, MGAs, TPAs, and self-insureds.
Installed Base	3
Notable Clients	Confidential

Source: Vendor RFI

Overview

The vendor states that Charlee.ai is a technology company providing artificial intelligence and predictive analytics solutions for the insurance industry. The company’s solutions help insurance companies reduce claims litigation and severity while managing reserves efficiently.

Key features include:

Charlee.ai helps insurance companies reduce claims litigation and severity while managing reserves efficiently. Its unique and patented approach leverages natural language processing and machine learning techniques to extract tags/topics from policy and claim files and documents that helps improve their prediction accuracy. The AI solution has been trained and developed by industry experts. Currently, Charlee.ai has over 50,000 pre-trained tags and topics on more than six lines of business having been trained on over 50 million claims. The pre-trained tags and topics enhance prediction accuracy to over 80% and accelerate implementations by 60%.

Key benefits include:

In the US, insurance companies spend over \$200 billion on fraud and litigation, causing increased premiums or no coverages. Charlee.ai™, the predictive analytics solution, helps insurance companies reduce litigation, reduce claims severity, and manage reserves.

Functionality

Table 3: Functionality

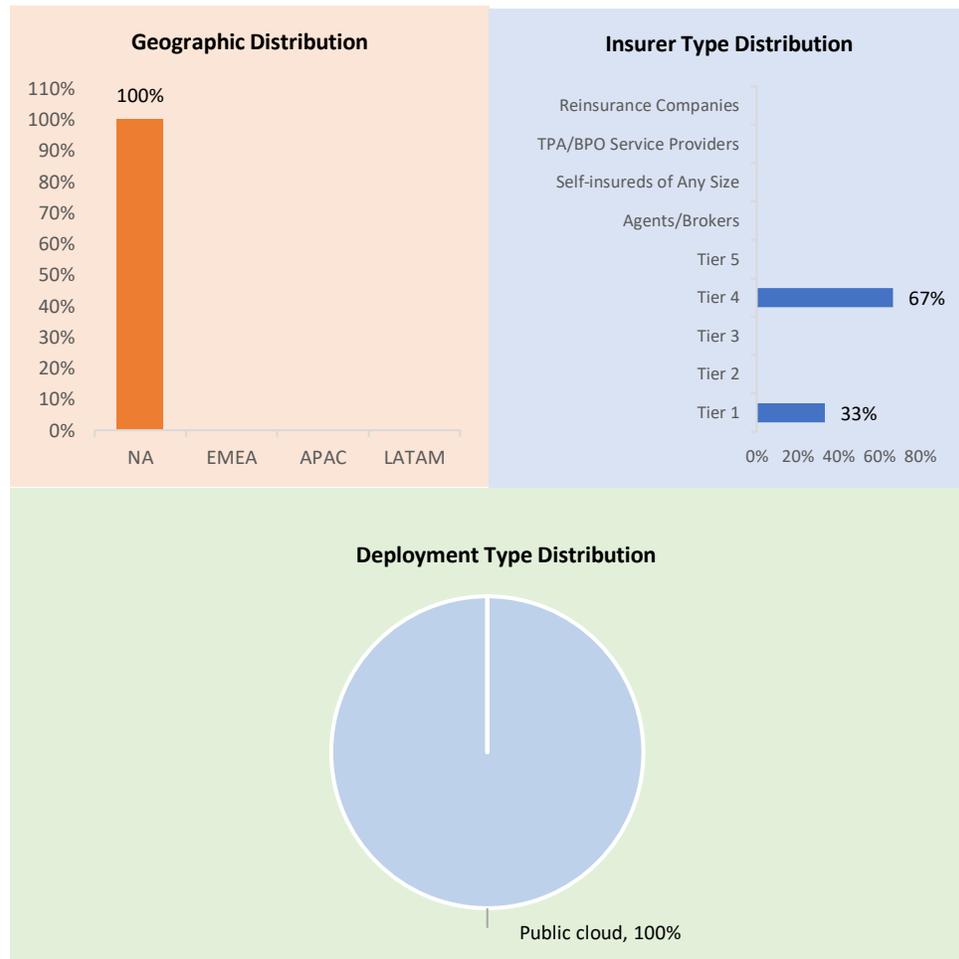
Function	In Production with Clients	Supported, But Not in Production with Clients	Not Supported
Data			
Aggregate historical data from different internal databases	●		
Integrate with external data capture tools (IoT, wearables, sensors, etc.)	●		
Consolidate data coming from external databases	●		
Data 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, Size, Type of Insurer, and Deployment Type (Global)



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Java: 5%; JavaScript: 25%; Python: 70%
Database	NoSQL, Postgresql, SQL

Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Tier 1 with three subsidiaries Claims volume of 7 million, historical and open
Integration Methods	Web services, HTML, HTTP, RESTful HTTP style services, JSON format, custom APIs

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes
Type of effort required to update the solution	Project based—manual upgrade
Cadence of upgrades for multitenant deployments	Every six months
Deployment approach supports elasticity	Yes
Current API-related strategy	Pre-connected cloud environment (fully connected and ready to use)
Deployment model can leverage a serverless approach	Yes
Solution enables independent services (microservices)	Yes
Proportion of the system architected as microservices	25% to 50%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	No
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✓
Amazon Web Services (AWS)	✓
Google Cloud Platform (GCP)	✓
Alibaba Cloud	✗
IBM Cloud/Bluemix	✗
Oracle Cloud	✗

Public Cloud Providers	Availability
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.	■
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

Charlee.ai's data model is proprietary.

Regarding industry standard data model schemas, the vendor states it uses no-SQL databases that do not confine to any one specific industry model. It has a custom-developed Charlee.ai proprietary data model to support unstructured data, with claims and policy data for six lines of insurance business.

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

Clients are not able to change their proprietary data model. They are given their standard data model templates, and they will configure Charlee.ai for any deviations to that model based on project objectives and goals. The data model can be released to the client, can be easily published to a client's data model, and can map to an intermediate format to share with a client (such as an industry standard).

Client cannot directly make any changes to Charlee.ai proprietary data models. The company works with clients to modify their data models based on their project goals and additional data that would be needed to accomplish this.

The company versions its APIs and data models and works with customers' IT teams for any changes.

Security

Charlee.ai complies with the following security standards: SOC2 Type 2, OWASP.

Flexible user permissions, multifactor authentication, and other options are available as authentication factors for internal and external users.

For cybersecurity arrangements, the company has Trend Micro agent running on all of its servers, which provides IDS, IPS, anti-virus, and anti-malware functions. The system is set up such that only a web gateway and sftp server are internet facing. All other machines, including databases and application servers, only have a private IP address. They can be accessed only via VPN (for internal users) or via reverse proxy from the web gateway (for external users). All object storage is kept as non-internet facing. All data is encrypted in-transit and at rest.

Charlee.ai performs quarterly vulnerability scans and penetration testing by internal staff, as well as yearly vulnerability scans and penetration testing by an external third party company. Security patching on all servers is performed at least quarterly. Any alerts from Trend Micro or the cloud provider's security alerts are monitored and addressed in a timely manner.

The system has penetration security by the company's application servers and isolated from the web/sftp servers. Only the web/sftp servers are internet facing. Application servers can be accessed only via VPN (for internal users) or via reverse proxy from the web gateway (for external users). All object storage is kept as non-internet facing. All data is encrypted in transit and at rest.

Vulnerability scans and penetration tests are performed quarterly, and any issues identified are addressed in a timely manner.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Eclaro, Neosoft
Fintech Partners	0
Core System Vendors	Majesco, OneShield, two others (names not disclosed by vendor)

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	10 to 12
----------------------------------	----------

Resource Breakdown	Vendor: 70%; Insurer: 10%; Third party: 20%
Location of Employees	Charlee.ai has employees in North America, APAC, with 8 in North America and 7 in APAC.
Average Time to Implementation	<u>Initial implementation</u> : 1 to 3 months <u>Second and subsequent line of business</u> : 1 to 2 months <u>Second and subsequent states/jurisdictions</u> : 1 to 2 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Term license, enterprise license, subscription based license
Factors Used to Determine Pricing	<u>Usage-based factors</u> : Per functional components/modules used, or policy or account volume <u>Tier-based factors</u> : Lines of business, entities and direct written premium <u>Other factors</u> : Flat pricing, freemium entry-level followed by a standard pricing plan

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	Under US\$100,000– US\$250,000	Under US\$100,000– US\$250,000	Not disclosed
Average Remaining Costs (Year Two and Beyond)	Under US\$100,000– US\$250,000	Under US\$100,000– US\$250,000	Not disclosed

Source: Vendor RFI

CRIF: SHERLOCK

Company and Product Snapshot

CRIF is a private company headquartered in Bologna, Italy, with sales and professional services personnel located throughout Europe. The company has 6,200 employees, of whom 20 are available to provide professional services/client support for the company's Sherlock solution.

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

Table 1: Company Snapshot

Year Founded	1988
Number of Employees	6,200
Revenues (USD)	\$633,298,880
Financial Structure	Private
VendorMatch Link	https://www.celent.com/solutions/872819349
User Conferences	No annual conference or customer event is offered.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Sherlock
Year Originally Released	2013
Current Release and Date of Release	Internal versioning/changes continuously released
Revenue Derived from the Product	\$6,000,000 USD
R&D Expense	The vendor's spend on research and development expense over the past two years has been 20% of total revenue attributed to this solution.
FTEs Providing Professional Services for Product	20
Regional FTEs (NA/EMEA/APAC/LATAM)	0/10/10/0
Target Market	Insurance companies worldwide
Installed Base	100
Notable Clients	Not disclosed

Source: Vendor RFI

Overview

The vendor states that Sherlock is designed to deliver, in one click, counter-fraud intelligence to the investigator. By consolidating best-of-breed data sets on a single

screen, Sherlock supports around 100 UK insurers in speeding up the investigation process, delivering operational efficiencies, and reducing the time to collect and integrate key information.

Key features include:

- *Just 3 seconds to investigate 100% of all claims, identify hidden fraudulent connections, assess risk, and personalize the insurer’s offer.*
- *Evaluation of the level of anomaly for each claim, identifying hidden connections between parties involved in past and present claims, and preventing and managing both opportunistic and organized claims fraud across multiple lines of business.*
- *A reduction in operational overheads and an improved overall customer experience.*
- *Automate and fasten internal processes to effectively deliver services via remote working models and adapt to a rapidly changing operating environment. Claims and fraud teams have the ability to share information and utilize normal checks virtually and cohesively to offset vulnerabilities.*
- *Application of the CRIF insurance fraud analytics engine and multiple techniques: business rules, AI and proprietary machine learning techniques, anomaly detection, and network link analysis to automatically and selectively manage claims based on relevancy.*
- *Noninvasive and agile, Sherlock is a Software as a Service (SaaS).*
- *Flexible and complementary, it is suitable for insurance companies with or without an existing anti-fraud platform in place.*

Key benefits include:

Discover Actionable Insights: Hidden claims connections between parties of past and present claims whether motor, home, personal injury, or pet. Sherlock provides the insurer with a fraud risk score for every claim supported by an intuitive report, written in simple business language, which evaluates the level of anomaly for each claim.

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	●		

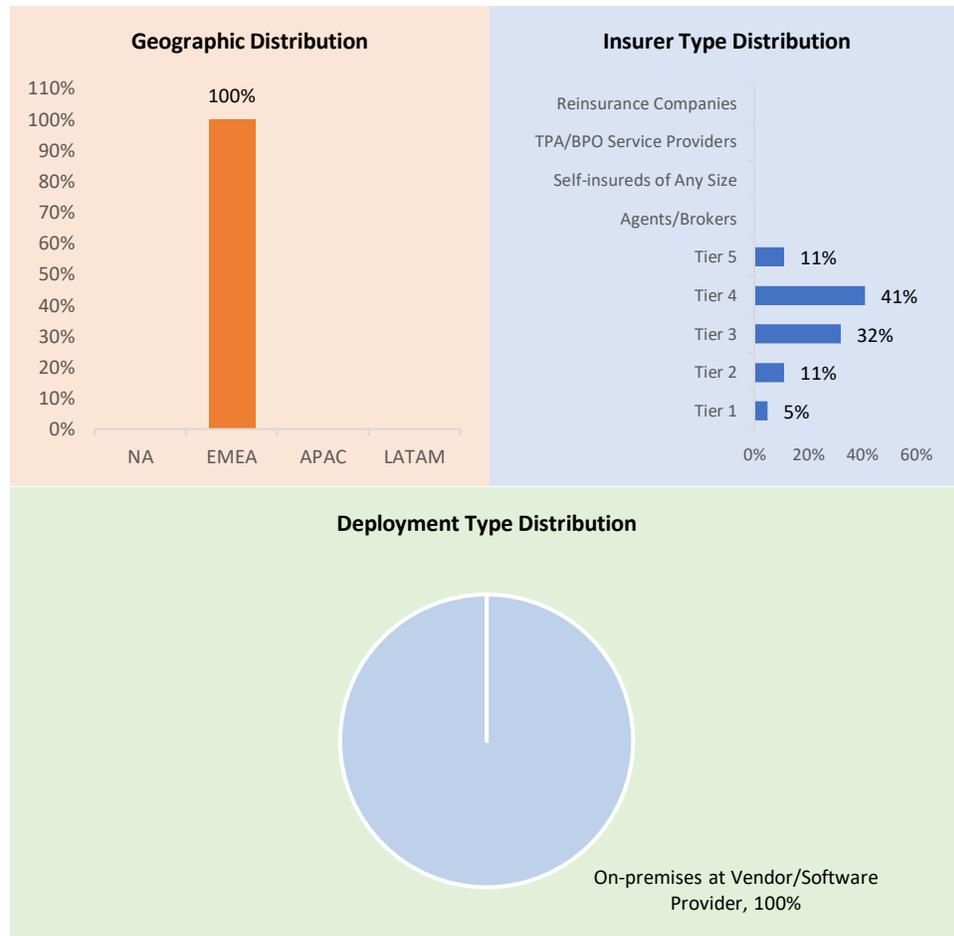
Integrate with external data capture tools (IoT, wearables, sensors, etc.)		●	
Consolidate data coming from external databases	●		
Data quality checking tools	●		
Automatic data adjustment prompts (unstructured, inconsistent, or redundant data)	●		
Uses additional hardware infrastructure in the cloud 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 using simple tools for business user
 - = Configurable using simple tools for IT user
- = Configurable through a scripting language/coding
 - = Available with integration to a third party solution
 - = Available with integration to a separate module provided by this vendor
- = Under development/On road map
 - = Could develop—would be considered customization
 - = Not available/Not applicable

Source: Vendor RFI

Customer Base

Figure 1: Client Base by Geography, Size, Type of Insurer, and Deployment Type (Global)



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	C#: 60%; JavaScript: 5%
Database	Not disclosed
Scalability	The vendor's largest deployment (total number of transactions processed daily system): 10,000 Scalability metrics:
Integration Methods	RESTful HTTP style services, JSON format, other integration methods

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes
Type of effort required to update the solution	Evergreen—all clients are on the same latest version
Cadence of upgrades for multitenant deployments	Quarterly
Deployment approach supports elasticity	Yes
Current API-related strategy	In-house expertise and experience to build with confidence
Deployment model can leverage a serverless approach	No
Solution enables independent services (microservices)	No
Proportion of the system architected as microservices	25% to 50%
Supports automation of development and deployment processes (DevOps)	No
Solution runs and deploys under containers to improve the application deployment	Yes
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✓

Public Cloud Providers	Availability
Amazon Web Services (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.	●
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

CRIF's data model is proprietary.

Regarding industry standard data model schemas, the vendor states Sherlock implemented a JSON-based data model tailored specifically for the supported insurance business lines.

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

The data model implemented for Sherlock is typically sufficiently generic to support the needs of typical clients.

Should any client need to integrate a specific data set, an ad hoc extension of the data model can be developed by CRIF IT staff and plugged into the existing source code of the service. The data model can be easily published to a client's data model and can map to an intermediate format to share with a client (such as an industry standard).

The data model is governed by CRIF project team, prioritizing maximum flexibility for future changes and maximum compatibility with existing features.

In-depth analysis of requirements needs to confirm whether an actual change to the data model is required and if such a change can be accomplished by extending rather than modifying the existing model.

If an actual change to the existing model is required, backward compatibility is ensured by adapting data mapping layers and thorough non-regression tests.

Data is stored in JSON format. Mapping to data model published for user interfaces, including any changes, is managed by CRIF project team and undergoes strict non-regression tests.

Security

CRIF complies with the following security standards: All transactions by CRIF and customers' users are logged, and all inner calls to different system components are also logged and linked to the main transaction.

All IT systems access (e.g., database, operating systems) are also logged, kept, and monitored in the corporate SIEM.

The system is not PCI compliant because it does not process payments. However, CRIF provides other PCI-compliant services, and it would be possible to make Sherlock compliant if required.

Flexible user permissioning is available for internal and external users.

The system infrastructure, architecture, and software code is analyzed and validated by an automated code analysis tool and an internal CRIF IT team and information security experts.

Static code analysis is performed before each release.

Intrusion detection, prevention, and active monitoring of security events are performed by the CRIF corporate IT security team.

Standard communication and security protocols have been employed throughout the solution.

An independent ISECOM certified third party regularly performs penetration testing against the application and technological infrastructure, following OSSTMM methodology and the OWASP testing guide. This ensures that testing and reporting are standard; use a widely accepted approach; are comprehensive, consistent, repeatable, and measurable; and comply with applicable regulations.

A certified STAR report is produced at the end of each test.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Percayso Inform
Fintech Partners	Tinexta, Certego, YOLO, KIND, STEP 4 BUSINESS, Fido

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	30 to 40
Resource Breakdown	Vendor: 80%; Insurer: 10%; Third party: 10%
Location of Employees	CRIF employees dedicated to Sherlock are located in EMEA and APAC with 10 in EMEA and 10 in APAC.
Average Time to Implementation	<u>Initial implementation</u> : 4 to 6 months <u>Second and subsequent line of business</u> : 1 to 3 months <u>Second and subsequent states/jurisdictions</u> : 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Subscription-based license, term license, perpetual license, enterprise license, other pricing model not listed
Factors Used to Determine Pricing	<u>Usage-based factors</u> : Per transaction <u>Tier-based factors</u> : None <u>Other factors</u> : Other basis not named

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

FRAUDKEEPER: FRAUDKEEPER

Company and Product Snapshot

FraudKeeper is a private company headquartered in Buenos Aires, Argentina, with sales and professional services personnel located throughout North America, Latin America, Middle East, and Europe. The company has 30 employees, of whom nine are available to provide professional services/client support for the company's FraudKeeper solution.

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

Table 1: Company Snapshot

Year Founded	2019
Number of Employees	30
Revenues (USD)	Not disclosed
Financial Structure	Private
VendorMatch Link	https://www.celent.com/solutions/841750597
User Conferences	No annual conference or customer event is offered.

Source: Vendor RFI

Table 4: Product Snapshot

Name	FraudKeeper
Year Originally Released	2020
Current Release and Date of Release	02/2022
Revenue Derived from the Product	\$1 million
R&D Expense	The vendor's spend on research and development expense over the past two years has been 20% of total revenue attributed to this solution.
FTEs Providing Professional Services for Product	9
Regional FTEs (NA/EMEA/APAC/LATAM)	5/5/5/15
Target Market	Insurers
Installed Base	9
Notable Clients	Allianz, Federacion Patronal, HDI, Southbridge Fairfax

Source: Vendor RFI

Overview

The vendor states that FraudKeeper is a digital platform based on automation rules and machine learning that allows detecting, preventing, and managing fraudulent transactions in the underwriting and claims processes.

Key features include:

- *Automatic Learning Techniques (Machine Learning): Ability to process thousands of transactions in real time and generate alerts automatically.*
- *Control Panel and Case Tracking: Rules based on experience, industry and custom.*
- *Advanced Analytics for Rule Feedback: Plug and use—simple and fast integration with company legacy systems.*

Key benefits include:

- *Improve customer experience by accelerating payments and underwriting.*
- *Minimize losses related to fraud.*
- *Lower operating costs, less resources, and fewer false positives.*

Functionality

Table 3: Functionality

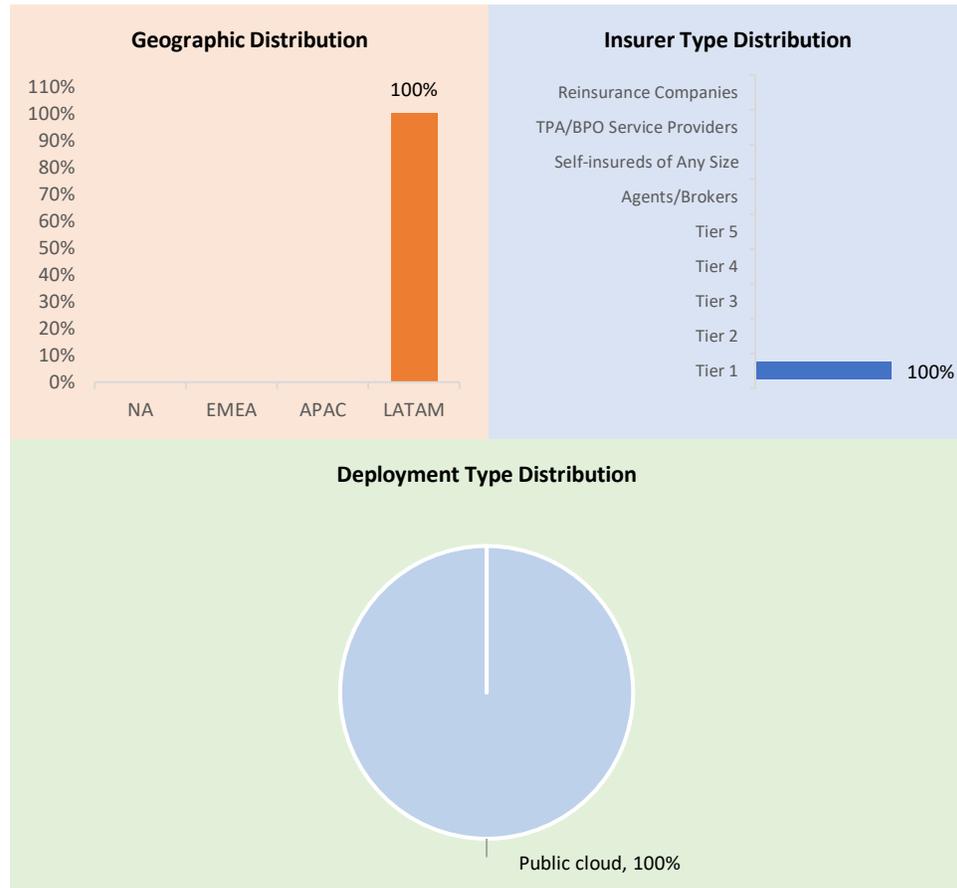
Function	In Production with Clients	Supported, But Not in Production with Clients	Not Supported
Data			
Aggregate historical data from different internal databases	●		
Integrate with external data capture tools (IoT, wearables, sensors, etc.)		●	
Consolidate data coming from external databases	●		
Data 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, Size, Type of Insurer, and Deployment Type (Global)



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Java: 50%; Python: 30%
Database	MongoDB, NoSQL, SQL
Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed

Integration Methods	Web services, RESTful HTTP style services, JSON format, MQSeries, JMS or similar queue technology, custom APIs, flat files
----------------------------	--

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes
Type of effort required to update the solution	Evergreen—all clients are on the same latest version
Cadence of upgrades for multitenant deployments	More frequent than every three months
Deployment approach supports elasticity	Yes
Current API-related strategy	In-house expertise and experience to build with confidence
Deployment model can leverage a serverless approach	Yes
Solution enables independent services (microservices)	Yes
Proportion of the system architected as microservices	50% to 80%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	Yes
Need for containerization to run in a cloud	Yes
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✓
Amazon Web Services (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.	✓
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

FraudKeeper's data model is proprietary.

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

The data model can be released to the client, can be easily published to a client's data model, and can map to an intermediate format to share with a client (such as an industry standard).

Security

FraudKeeper complies with the following security standards: GDPR.

One-time passwords, flexible user permissioning, security tokens/pins, multifactor authentication, and federated identity support are available as authentication factors for internal and external users.

The system has penetration security by external security providers.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	10

Fintech Partners

Charles Taylor InsureTech, Leverbox

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	FraudKeeper has employees in North America, EMEA, APAC, and LATAM, with 5 in North America, 5 in EMEA, 5 in APAC, and 15 in Latin America.
Average Time to Implementation	<u>Initial implementation</u> : 1 to 3 months <u>Second and subsequent line of business</u> : 1 to 3 weeks <u>Second and subsequent states/jurisdictions</u> : 1 to 3 weeks
Preferred Implementation Approach	Not disclosed
Pricing Models	Subscription-based license, other pricing model not listed
Factors Used to Determine Pricing	<u>Usage-based factors</u> : Number of total or named users, per functional components/modules used, per transaction <u>Tier-based factors</u> : None <u>Other factors</u> : Flat pricing

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

Source: Vendor RFI

FRISS: FRAUD DETECTION AT CLAIMS

Company and Product Snapshot

FRISS is private company with outside investors headquartered in Utrecht, Netherlands, and Ohio, US, with sales and professional services personnel located throughout North America, Latin America, Europe, and Asia Pacific. The company has 225 employees, of whom 61 are available to provide professional services/client support for the company's Trust Automation solutions.

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

Table 1: Company Snapshot

Year Founded	2006
Number of Employees	225
Revenues (USD)	Not disclosed
Financial Structure	Private with outside investors
VendorMatch Link	https://www.celent.com/solutions/929827122
User Conferences	The vendor offers an annual user conference or customer event.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Fraud Detection at Claims
Year Originally Released	2008
Current Release and Date of Release	FRISS is using an agile development methodology; therefore, releases happen regularly, with the most recent occurring in August 2022
Revenue Derived from the Product	Not disclosed
R&D Expense	The vendor's spend on research and development expense over the past two years has been 30% of total revenue attributed to this solution.
FTEs Providing Professional Services for Product	61
Regional FTEs (NA/EMEA/APAC/LATAM)	13/44/3/1
Target Market	FRISS focuses on the P&C insurance market
Installed Base	103
Notable Clients	Citizens, TD Insurance, UNIQA, SURA

Source: Vendor RFI

Overview

The vendor states that its Trust Automation Platform provides real time, data-driven scores and insights that give customers instant confidence and understanding of their inherent risks and interactions.

Based on next-generation technology, the Trust Automation Platform allows insurers to confidently manage trust throughout the insurance value chain—from the first quote all the way through claims and investigations when needed.

Trust is normalized throughout the organization, enabling consistent processes to flag high risks in real time.

Key features include:

- *AI-Powered Intelligent Detection*
- *Automated Fraud Scoring*
- *Confident Interactions*
- *Actionable Insights*
- *Integrated Case Management*

Key benefits include:

FRISS' Trust Automation Platform allows insurers to improve operational efficiency following the three pillars of trust:

1. *Standardize, safeguard, and automate competence; deliver products and services through process excellence and know-how.*
2. *Increase customer satisfaction by showing your motives, driven by the intention to do what's best for your customers you interact with, and think how to balance the needs for different groups when needed.*
3. *Enable fair processes and treatment of customers. Processes should be open and transparent, both for trustworthy customers as for those you need to verify.*

For claims, FRISS' Trust Automation Platform provides immediate informational fairness. Every result comes with the underlying rationale and is executed in a consistent, accurate, and unbiased manner, while maintaining the opportunity to add subject matter expertise when needed. This means that insurers can operate Claims Segmentation and Touchless Claims and make real time decisions based on real time data. Clients' claims are scored within seconds, allowing for direct interactions to pay out genuine claims faster, reduce clients' loss ratio, and improve customer satisfaction.

Functionality

Table 3: Functionality

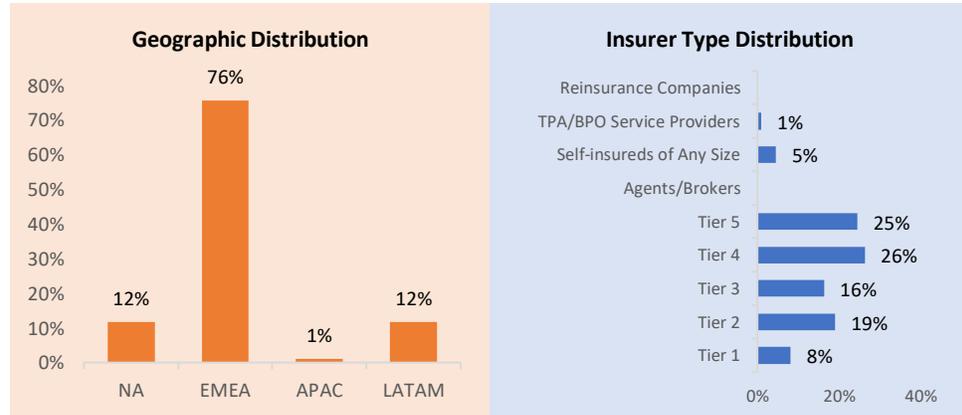
Function	In Production with Clients	Supported, But Not in Production with Clients	Not Supported
Data			
Aggregate historical data from different internal databases	●		
Integrate with external data capture tools (IoT, wearables, sensors, etc.)	●		
Consolidate data coming from external databases	●		
Data 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	●		

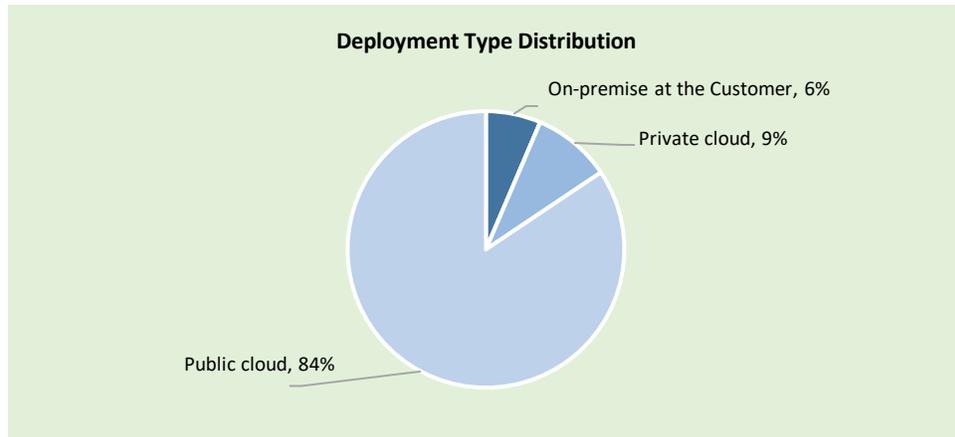
Special Investigation Unit (SIU) features		
Design and update monitoring dashboards	●	
Assign/share fraud cases with other investigators	●	
Check fraud case logs (status changes, audit trails, etc.)	●	
● = Available out of the box	● = Configurable through a scripting language/coding	● = Under development/On 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, Size, Line of Business, and Deployment Type (Global)





Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	.Net: 50%; JavaScript: 20%; Python: 20%
Database	Not disclosed
Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed
Integration Methods	Web services, XML (not through web services), RESTful HTTP style services, JSON format, custom APIs, flat files

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes
Type of effort required to update the solution	FRISS offers a SaaS service, and therefore, updates are performed by FRISS' DevOps Team. A small group of long-term clients are running on-premises solutions that are not all on the latest version. FRISS is in the process of moving these clients to the cloud.
Cadence of upgrades for multitenant deployments	More frequent than every three months

Deployment approach supports elasticity	Yes, automatically
Current API-related strategy	Enabled by consumable APIs
Deployment model can leverage a serverless approach	Yes
Solution enables independent services (microservices)	Yes
Proportion of the system architected as microservices	Over 80%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	Yes
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	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.	■
Interface Definition	■
Product Definition	■

Types of Changes	Availability
Role-Based Security, Access Control, and Authorizations	<input type="checkbox"/>
Screen Definition	●

Legend: ✓ = Configurable via tools for business users; □ = Configurable via tools for IT users; ■ = Configurable via the vendor; ⊖ = Configurable via scripting; ● = Coding required; x = Not available

Source: Vendor RFI

Data

FRISS' data model is proprietary.

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

Extra data can be added on top of the standard FRISS data specification to enrich the claim data (for example coming from the DWH). This extra information can improve the performance of the fraud-detection models. FRISS offers the possibility to add the data as API integrations to the platform. That data would then be mapped to the FRISS data model using the FRISS data mapper. Alternatively, this data can be delivered as an additional field when the claim gets sent to the FRISS solution. FRISS uses a proprietary entity resolution mechanism on its FRISS data model to ensure a single customer view, taking into account poor data quality. 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).

Clients cannot change the data model itself but are able to add any data they would like over the API and FRISS adds them to the data model.

FRISS manages its data model through API contracts. Making changes always leads always leads to a new API version.

Security

FRISS complies with the following security standards: FRISS has held an unqualified assurance ISAE3402 Type II report for many years in a row. This assurance report focuses on the domains of incident, change, release, operational, security, and supplier management, and is executed annually. FRISS shares the outcome with clients on an annual basis.

The company's framework and controls are audited by well-known audit bodies: EY for the last few years and currently by BDO.

Flexible user permissioning, out of band identification, security tokens/pins, and multifactor authentication are available as authentication factors for internal and external users.

Structural employee security and compliance trainings are provided by FRISS.

Considering the technology, FRISS has taken appropriate measures to ensure safe business continuity. These measures include, but are not limited to, protection against unintended or deliberate unauthorized processing of (personal) data. The following fields are mentioned specifically:

Security

1. Dedicated security and compliance team.
2. Physical security at HQ, including badge access to secure zones.
3. Physical security at the state-of-the-art secure data centers.
4. Certifications and attestations:
 - a. ISO27001 certification held by the company's office automatization partner.
 - b. ISO27001 and SOC22 certification held by the company's hosting provider.
 - c. FRISS' security program is covered by the ISAE3402 Type II. ISO27001 certification will be achieved by the end of 2022.
5. Yearly audit includes IT components.
6. Periodic mandatory education and awareness for all personnel and hired staff.

Privacy

1. Assigned data protection officer.
2. Established privacy program.
3. GDPR assessment executed by third party.
4. Vendor due diligence.
5. Periodic data privacy awareness and mandatory education for all employees and hired personnel.

Compliance

1. Vendor due diligence.
2. Pre-employment screening on personnel and similar requested from subcontractors.

Infrastructure

1. Servers are hosted in a secure data center, and a well-known cloud provider is used for local storage.
2. Security through strict IP whitelisting and logical controls for data segregation.
3. Tested and implemented business continuity and disaster recovery plan based on business impact analysis.

Back-ups

1. Five-minute replications to other data center.

2. Daily incremental back-up. Additional back-ups are weekly, monthly, and yearly.

Applications

1. FRISS as a processor:
 - a. Cooperation with controllers to execute data subject rights.
 - b. Configurable data retention policies.
2. Change management:
 - a. Governed by ISAE 3402 Type II.
 - b. Automated testing including SonarCube and OWASP.
 - c. Manual security and functional testing.
 - d. External penetration tests on new product release.
 - e. Changes and incidents are handled according to tiered access control lists.
3. Insights:
 - a. Audit trail in applications.
 - b. Extensive reports on data usage.

Personnel

1. Many policies, including a code of conduct and information security policy:
 - a. Nondisclosure agreements (including third parties).
 - b. Clear procedures on reporting incidents to security and privacy team.
 - c. Clean desk policy.
 - d. Structural employee security and compliance trainings are provided by FRISS.

The system has penetration security coordinated by the FRISS security officer and executed by an external company.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	EY, Deloitte, GFT, and Zensar

Fintech Partners

FRISS has a significant global partnership in place with Munich Re as the preferred provider of fraud detection and analytics solutions to customers. Munich Re ran a 12-month selection program to decide which software supplier provided the best solution and selected FRISS in 2016 as partner for Latin America and Iberia. This partnership was expanded globally in 2019. The benefits to Munich Re are that the FRISS solution has improved its customer portfolios, improved its profitability, and reduced the risk of reinsurance contracts.

FRISS has several global data suppliers and maintains a relationship with Dun & Bradstreet for Business Information and Info4C for PEP/Sanctions data. FRISS has also connected WebIQ, which can provide insight to social media networks to supplement network detection. The partnership with Legentic integrates real time and historic data into FRISS.

FRISS also has relationships with consultancy firms that act as system integrators, such as Zensar, EY, KPMG, and Deloitte.

FRISS also has an association with IASIU, and several of their team are individual members. Other service providers connected to FRISS include:

- Omnius: Provide OCR services.
- Eviid: Provide secure image software to help the evidentiary trail.
- Mohawk: Provision of screening of online classified listings.
- Brightmaven: Provision of services to locate stolen items listed on the internet.

FRISS has partner and relationships with all major core solution vendors such as Guidewire, Duck Creek, Keylane, MSG, Salesforce, IBA, Regnum, RGI, etc.

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	6 to 10
Resource Breakdown	Not disclosed
Location of Employees	FRISS has employees located in North America, EMEA, APAC, and LATAM.
Average Time to Implementation	<u>Initial implementation</u> : 4 to 6 months <u>Second and subsequent line of business</u> : 1 to 3 months <u>Second and subsequent states/jurisdictions</u> : 1 to 3 months
Pricing Models	Subscription-based license
Factors Used to Determine Pricing	<u>Usage-based factors</u> : None <u>Tier-based factors</u> : None <u>Other factors</u> : None

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

HUGIN: BAYES FRAUD

Company and Product Snapshot

HUGIN is a private company with outside investors and headquartered in Aalborg, Denmark. The company has seven employees, of whom two are available to provide professional services/client support for the Bayes Fraud solution.

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

Table 1: Company Snapshot

Year Founded	1989
Number of Employees	7
Revenues (USD)	Confidential
Financial Structure	Private with outside investors
VendorMatch Link	https://www.celent.com/vendormatch/discovery/solutions/831166913
User Conferences	No annual conference or customer event is offered.

Source: Vendor RFI

Table 5: Product Snapshot

Name	Bayes Fraud
Year Originally Released	2006
Current Release and Date of Release	9.1/2021
Revenue Derived from the Product	~\$100,000 USD
R&D Expense	The vendor's spend on research and development expense over the past two years has been 25% of total revenue attributed to this solution.
FTEs Providing Professional Services for Product	2
Regional FTEs (NA/EMEA/APAC/LATAM)	0/5/0/0
Target Market	Small and midsize insurance companies, focused on northern Europe
Installed Base	6
Notable Clients	Not disclosed

Source: Vendor RFI

Overview

The vendor states that Bayes Fraud is a market-leading predictive analytics solution that provides insurers with advanced, automated fraud detection capabilities during claims handling. The solution consistently evaluates all submitted claims for fraud and alerts claims handlers to high-risk claims. In this way, routine claims can be fast-tracked for immediate settlement, and claims with the highest likelihood of fraud can be investigated further—before costly claims are paid out. The resulting positive end-to-end claims experience strengthens customer loyalty and retention. And when only high-risk claims are sent to investigators, hit-rate accuracy increases and valuable time and resources can be dedicated to claims with the greatest potential of fraud—and cost savings for insurers.

Key features include:

The following table lists the features and functionality supported by the solution and how it is supported around:

- *Data preparation*
- *Model configuration*
- *Claims fraud techniques*
- *Special unit investigation (SIU)*

Key benefits include:

Bayes Fraud combines claims data with valuable input from claims and fraud experts in one model. It quantifies missing and uncertain data and observations, to “fill in the data holes” in claims data. The solution calculates fraud based on all evidence available and uncovers insight about fraud patterns and relationships that would otherwise be missed using manual or rules-based processes. Bayes Fraud learns from data as more claims data and information become available.

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.)		●	

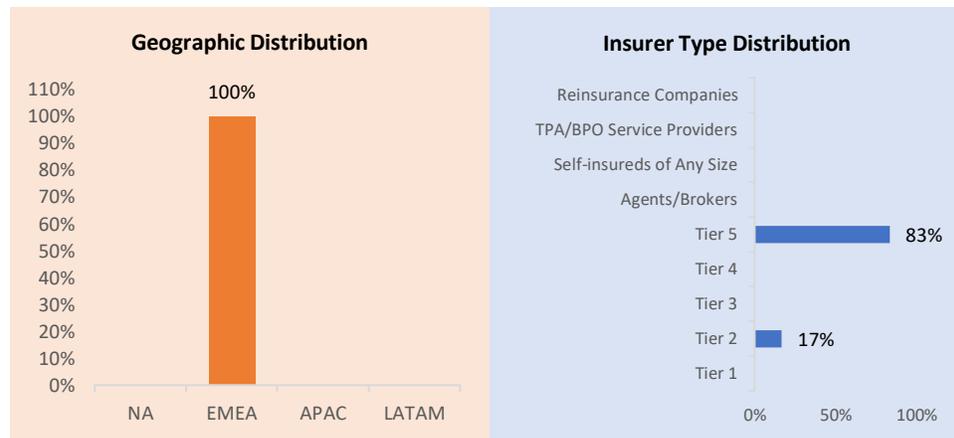
Consolidate data coming from external databases	●		
Data quality checking tools		●	
Automatic data adjustment prompts (unstructured, inconsistent, or redundant data)		●	
Uses additional hardware infrastructure in the cloud to run models on large amount of data		●	
Model Configuration			
Reusable, sharable 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, Size, Type of Insurer, and Deployment Type (Global)



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	.Net: 10%; C: 30%; C++: 10%; Java: 30%; JavaScript: 10%; Python: 10%
Database	
Scalability	The vendor’s largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed
Integration Methods	Web services, RESTful HTTP style services, custom APIs, flat files

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	No
Type of effort required to update the solution	Evergreen—all clients are on the same latest version
Cadence of upgrades for multitenant deployments	Every 12 months
Deployment approach supports elasticity	Yes, within months
Current API-related strategy	Not disclosed
Deployment model can leverage a serverless approach	Not disclosed
Solution enables independent services (microservices)	Not disclosed
Proportion of the system architected as microservices	Not disclosed
Supports automation of development and deployment processes (DevOps)	Not disclosed
Solution runs and deploys under containers to improve the application deployment	Not disclosed
Need for containerization to run in a cloud	Not disclosed
System's functions and capabilities can be distributed among a private cloud and a public cloud	Not disclosed

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	No
Amazon Web Services (AWS)	No
Google Cloud Platform (GCP)	No
Alibaba Cloud	No
IBM Cloud/Bluemix	No
Oracle Cloud	No
Salesforce Cloud, Force.com, AppExchange	No
Other	No

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.	●
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

Hugin's data model is not proprietary.

Regarding industry standard data model schemas, the vendor states HUGIN software has an application programming interface (API) to a range of different programming languages.

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

The fraud-detection model can be extended or changed using HUGIN Graphical User Interface or one of the HUGIN Decision Engine Application Programming Interfaces. The data model can be released to the client and can be easily published to a client's data model.

The fraud-detection model can be extended or changed using HUGIN Graphical User Interface or one of the HUGIN Decision Engine Application Programming Interfaces.

HUGIN Decision Engine is integrated into the customer IT system by the customer.

Security

Hugin complies with the following security standards: ISAE 3000 with annual audit.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	None
Fintech Partners	None

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
Resource Breakdown	Vendor: 10%; Insurer: 80%; Third party: 10%
Location of Employees	Hugin has five employees in EMEA.
Average Time to Implementation	<u>Initial implementation</u> : 7 to 12 months <u>Second and subsequent line of business</u> : 7 to 12 months <u>Second and subsequent states/jurisdictions</u> : 7 to 12 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Term license, enterprise license, subscription-based license, other pricing model not listed
Factors Used to Determine Pricing	<u>Usage-based factors</u> : Number of total or named users, annual premium volumes/revenues <u>Tier-based factors</u> : None <u>Other factors</u> : Flat pricing

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	Under US\$100,000	Under US\$100,000	Under US\$100,000
Average Remaining Costs (Year Two and Beyond)	Under US\$100,000	Under US\$100,000	Under US\$100,000

Source: Vendor RFI

LEXISNEXIS RISK SOLUTIONS, INC.: ACCURINT® FOR INSURANCE

Company and Product Snapshot

LexisNexis Risk Solutions, Inc. is a public company headquartered in Alpharetta, Georgia, US, with sales and professional services personnel located throughout North America. The company has around 6,000 employees, of whom 50 are available to provide professional services/client support for the Accurint® for Insurance solution.

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

Table 1: Company Snapshot

Year Founded	2000
Number of Employees	Approximately 6,000
Revenues (USD)	\$2,500,000,000
Financial Structure	Public Company NYSE: RELX
VendorMatch Link	https://www.celent.com/vendormatch/discover/y/vendors/499808609
User Conferences	The vendor offers an annual user conference or customer event.

Source: Vendor RFI

Table 6: Product Snapshot

Name	Accurint® for Insurance
Year Originally Released	2000
Current Release and Date of Release	Releases are biweekly from January to November; current release June 2022
Revenue Derived from the Product	N/A
R&D Expense	Not disclosed
FTEs Providing Professional Services for Product	50
Regional FTEs (NA/EMEA/APAC/LATAM)	Not disclosed
Target Market	Auto claims, life claims, SIU, subrogation, life policy owner services, life unclaimed property
Installed Base	Not disclosed
Notable Clients	93% of Fortune 500 companies

Source: Vendor RFI

Overview

The vendor states that it uses specialized analytics and data-linking technology designed to help validate relevant information about parties to a claim quickly by harnessing the power of 65 billion records. Market-leading technologies and premium information sources help leading insurers nationwide increase efficiency, productivity, and profitability.

Key features include:

- *Access Expansive Data Sets: Enhance insurance fraud detection and resolve claims faster. Search more than 65 billion records from 10,000+ sources, with 800,000 records added daily.*
- *Easy Account Management: Easily manage employee access, change passwords, set search functions, retrieve invoicing and activity reports, and more with premium administrative tools.*
- *Gain Valuable Insights: Uncover connections among people, businesses, assets, and locations. LexID linking technology reveals insights that cannot be discovered through public records alone.*
- *Unmatched Support and Training: Perform confidently with 24/7 customer service, dedicated account management, technical support, and search assistance.*

Key benefits include:

- *Access More Data in Less Time: Leverage one of the nation's largest databases of public and nonpublic records, publicly available information, proprietary content, and contributory information.*
- *Boost Profitability: Save money with just one search. Get one-stop access to police reports, medical records, court filings, and more.*
- *Improve Performance: Help validate and verify customer-provided information, increase insurance fraud protection, and better comply with unclaimed property standards.*
- *Position Clients' Business for Growth Through Efficiency: Leverage 35+ years of deep industry knowledge and expertise to help improve clients' processes, business outcomes, and return on investment.*

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, Size, Type of Insurer, and Deployment Type (Global)

Not disclosed

Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Not disclosed
Database	SQL, Sybase
Scalability	The vendor’s largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed
Integration Methods	Not disclosed

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	No

Type of effort required to update the solution	None. It is a SaaS solution delivered via secure web.
Cadence of upgrades for multitenant deployments	
Deployment approach supports elasticity	
Current API-related strategy	Enabled by consumable APIs
Deployment model can leverage a serverless approach	No
Solution enables independent services (microservices)	No
Proportion of the system architected as microservices	Under 25%
Supports automation of development and deployment processes (DevOps)	No
Solution runs and deploys under containers to improve the application deployment	No
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✓
Amazon Web Services (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

LexisNexis Risk Solutions, Inc.'s data model is proprietary.

Regarding industry standard data model schemas, the vendor states it uses a SaaS model via a secure web application.

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

The data model can map to an intermediate format to share with a client (such as an industry standard).

Security

LexisNexis Risk Solutions, Inc. (LNRS) complies with the following security standards:

The vendor is PCI compliant. For products and services that are in scope of PCI (e.g., process, store, or transmit credit card information), LNRS undergoes annual assessments and associated testing to ensure that the services are PCI compliant.

Multifactor authentication is available as an authentication factor for internal and external users.

LNRS has partnered with several reputable vendors to provide cybersecurity-related testing, assessments, consulting, and other security-related services. More information can be provided if there are more specific questions.

Penetration testing is performed on an annual basis by independent and qualified parties.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Please see recent news releases regarding partnerships in claims for the US insurance market, including a 2022 announcement on a strategic partnership with Shift Technology

Fintech Partners See above

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
Resource Breakdown	Not disclosed
Location of Employees	Not disclosed
Average Time to Implementation	<u>Initial implementation</u> : 1 to 3 months <u>Second and subsequent line of business</u> : 1 to 3 months <u>Second and subsequent states/jurisdictions</u> : 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	None
Factors Used to Determine Pricing	<u>Usage-based factors</u> : None <u>Tier-based factors</u> : None <u>Other factors</u> : None

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.

Lexis Nexis Risk Solutions offers a transactional pricing model.

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)	N/A	N/A	N/A

Source: Vendor RFI

SAS: SAS® DETECTION AND INVESTIGATION FOR INSURANCE

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 Insurance 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 Insurance
Year Originally Released	2009
Current Release and Date of Release	SAS Viya 4.0/2022
Revenue Derived from the Product	\$15.5 million
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)	100/200/50/50
Target Market	Property & casualty and life insurers
Installed Base	57

Notable Clients

NC Dept of Insurance, AKSigorta, Ethniki, CNseg, The Insurance Fraud Bureau, Shin Kong Life

Source: Vendor RFI

Overview

The vendor states that SAS® Detection and Investigation for Insurance provides an end-to-end solution for detecting, preventing, and managing both opportunistic and organized fraud detection across multiple lines of business. The solution includes components for fraud detection using advanced analytics and machine learning, advanced searching, alert management and case handling, along with the unique ability to uncover hidden relationships among fraudsters, enabling clients to focus on stopping the highest-value fraud networks. It is designed specifically for special investigation units, fraud analysts, and managers in insurance companies.

Key features include:

Single, end-to-end framework uses multiple techniques—automated business rules, predictive modeling, text mining, exception reporting, network link analysis, etc.—to better identify fraudulent activity and stop payments before they are made.

- *Data management*
 - *Provides an insurance-specific fraud 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 third party systems.*
- *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 clients 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 clients can harness the power of advanced analytics right out of the box.*
 - *Lets clients create and logically manage business rules, analytic models, alerts, and watch lists.*
 - *Enables clients to customize analytical models to identify fraud not found by existing business rules.*
 - *Enables easy management of the deployment, aggregation, scheduling, suppression, and routing of simple or complex rules across multiple factors, such as parties, data sources, and business lines.*
 - *Lets clients run groups of rules and models alone, in parallel or at different times (intraday, daily, weekly, monthly, etc.).*
 - *Facilitates collaboration with other business units 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 clients can stop suspicious activity at the prepayment stage. Enables clients 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 clients can customize to accommodate clients' investigative units' processes.*
- **Social network analysis**

- *Provides a unique network visualization interface that lets clients analyze related activities and relationships at a network dimension and identify linkages among seemingly unrelated claims.*
- *Enables clients 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 clients 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 clients 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 clients refine searches using interactive filters and facets that are customized for the specific user groups.*
 - *Provides full entity descriptions that include other linked entities, which clients can open and explore to evaluate the likelihood of fraud.*
 - *Provides an intuitive interface that lets clients construct complex queries without the need to understand specific syntax. For example, clients can use fuzzy searching, proximity searching, and field boosting while restricting searches to specific entity types, fields, comments, or insights.*
- *Case handling*
 - *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 staff to oversee the system.*
- *Can be hosted at a client's site, with SAS providing implementation assistance and training.*
- *Can be fully integrated with the client's existing operations environment, workflow solution, and business process management objectives, including thorough business process discovery and review to ensure the client's objectives are met or exceeded.*

Key benefits include:

Detect more fraudulent activity

- *Insert analytical models into the process, in addition to rules engines.*
- *Leverage advanced data mining and machine learning algorithms, as well as open source models.*
- *Analyze millions of claims records and scale both in real time and in batch to gain scores where you need them in the claims process.*
- *Use customized anomaly detection methods to detect previously unknown schemes.*
- *Automatically spot linked entities and crime rings, which can help stem larger losses.*
- *Overcome poor data quality issues associated with imperfect matching and highly linked entities.*

Lower loss adjustment expenses

- *Greatly reduce false positives.*
- *Improve investigator efficiency with advanced case handling tools.*
- *Increase ROI per investigator by prioritizing higher-value claims, entities, and networks and conducting more efficient and accurate investigations.*
- *Capture all claim settlement amounts within the system for reuse with similar claims in the future.*

Gain a greater competitive advantage

- *By quickly deciding which claims require further scrutiny and allowing the rest to pass, receive fewer false positives to reach greater customer satisfaction for legitimate customers.*
- *Satisfy regulatory compliance mandates through enhanced fraud management.*

Prevent fraud losses before settlement

- *Prevent payment on fraudulent claims using online, real time scoring or daily or intraday batch scoring.*
- *Detect loss padding in similar insurance claims with anomaly and loss comparisons.*

- Detect repeat offenders and more accurately score incoming claims by searching databases and watchlists of known fraudsters and other key entities (physical addresses, phone number, IP address, etc.) and capturing all fraud outcomes, referrals, and suspects within the system for reuse.
- Apply risk- and value-based scoring models to output before presenting to investigators.
- Detect insider or collusive fraud by integrating staff data and audit records that show who handled which claims.

Gain a consolidated view of fraud risk

- Identify cross-product fraud by seeing customer claims for all lines of business.
- Move analytics into new business processes to prevent and detect fraud.
- Continually improve models and adapt the system to address changes in insurance fraud trends.
- Better understand new claim threats and prevent big losses early using social networks 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

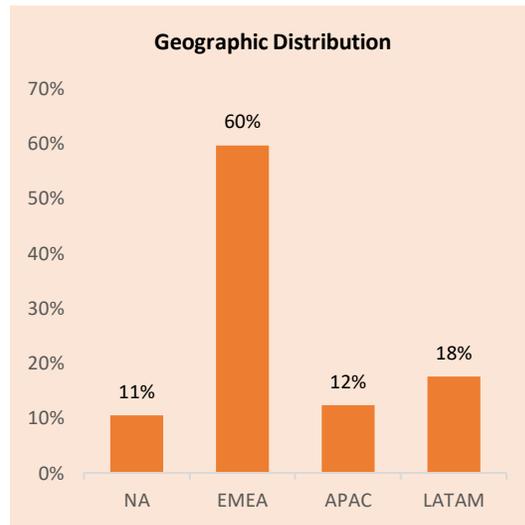
Design and update monitoring dashboards	●
Assign/share fraud cases with other investigators	●
Check fraud case logs (status changes, audit trails, etc.)	●

- = 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, Size, Type of Insurer, and Deployment Type (Global)



SAS did not provide insurer type distribution but noted 57 P&C carriers in addition to 11 insurance fraud consortiums.

Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	Java: 50%
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	# Clients Globally
Microsoft Azure	✓	Not disclosed
Amazon AWS	✓	Not disclosed
Google Cloud Platform (GCP)	✓	Not disclosed
Alibaba Cloud	✓	Not disclosed
IBM Cloud / Bluemix	✓	Not disclosed
Oracle Cloud	✓	Not disclosed
Salesforce Cloud, Force.com, AppExchange	✓	Not disclosed
Other	✗	Not disclosed

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.	✓
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 follows ACORD.

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, Core Compete (now part of Accenture), Tata Consulting (India), Zencos (US), Paspara (Lithuania), Zreya (Malaysia), Timestamp (Portugal), Accord Business Group (United Arab Emirates), MIAC Computing (Israel), DataScience (Middle East), Facts Consulting (Southern Africa), and GMWIT (Brazil)
Fintech Partners	Guidewire, Duck Creek, ISO, NICB, ThreatMetrix, GIACT, Plaid, Boku, Prove, Intellicheck, BioCatch, DataVisor, Iovation, Socure, and TransUnion

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
---	--------

Resource Breakdown	Vendor: 60%; Insurer: 30%; Third party: 10%
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	<u>Initial implementation:</u> 4 to 6 months <u>Second and subsequent line of business:</u> 1 to 3 months <u>Second and subsequent states/jurisdictions:</u> 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	Subscription-based license, term license, enterprise license, other pricing model not listed
Factors Used to Determine Pricing	Annual premium volumes/revenues; however, the vendor notes it will be moving more toward usage based pricing in 2023. <u>Usage-based factors:</u> Number of concurrent users <u>Tier-based factors:</u> None <u>Other factors:</u>
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			

SHIFT TECHNOLOGY: SHIFT CLAIMS FRAUD DETECTION

Company and Product Snapshot

Shift Technology is a private company headquartered in Paris and Boston with sales and professional services personnel located throughout North America, Latin America, Africa, Europe, and Asia Pacific. The company has 450 employees, of whom three are available to provide professional services/client support for the company's Shift Claims Fraud Detection solution.

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

Table 1: Company Snapshot

Year Founded	2014
Number of Employees	500
Revenues (USD)	Not disclosed
Financial Structure	Private
VendorMatch Link	https://www.celent.com/vendormatch/discover/solutions/153338105
User Conferences	The vendor offers an annual user conference or customer event.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Shift Claims Fraud Detection
Year Originally Released	2014
Current Release and Date of Release	08/2022
Revenue Derived from the Product	N/A; Shift does not disclose revenue figures due to corporate policy.
R&D Expense	The vendor's spend on research and development expense over the past two years has been 30% of total revenue attributed to this solution.
FTEs Providing Professional Services for Product	Average of three FTEs per client
Regional FTEs (NA/EMEA/APAC/LATAM)	29/102/14/4
Target Market	Tier 1 and Tier 2 Insurance Carriers in Europe, Asia, and North and South America. Lines of business include personal and commercial auto, commercial auto and

	commercial property, and workers' compensation.
Installed Base	80
Notable Clients	Assurant, P&V Group, MS&AD, CNA, Canadian Life and Health Insurance Association (CHLIA), Ethias, Équité, General Insurance Association (GIA), Generali, Admiral, Agence de Lutte contre la Fraude à l'Assurance (ALFA), l'olivier, Suravenir, Seguros Banorte, First Central, Central Insurance, iA, Insurance Fraud Bureau (IFB), Falcon, Tokio Marine, MAPFRE, Elephant, Areas Group, Hong Kong Federation of Insurers (HKFI) Generation, La Macif, Saison, Economical, Saluds, Amica, La Banque Postale
Source: Vendor RFI	

Overview

The vendor states that Shift Claims Fraud Detection is a best-in-class AI fraud-fighting solution for P&C insurers. It can detect claims fraud in real time or in scheduled workflows, and the solution can deliver 3x the detection hit rate compared to manual or rules-based implementations. Furthermore, Shift Claims Fraud Detection delivers transparent findings to users with detailed rationale for all of its conclusions. This allows investigators to make fraud decisions up to 4x faster with accuracy and confidence.

Key features include:

- *Finds previously undetectable fraud with AI analysis of all structured and unstructured claims data backed by the world's largest team of insurance-focused data scientists.*
- *Reduces false positives to drive more efficient workflows.*
- *Identifies simple cases of individual fraud and more sophisticated network fraud schemes.*
- *Clear contextual guidance and supporting documentation to speed investigations.*
- *Seamless API integration with insurer core systems.*
- *SaaS-based solution.*
- *Four months to full integration and accelerated ROI.*

Key benefits include:

Shift’s approach solves for the key barriers that prevent insurers from detecting fraud more accurately and rapidly, which is how Shift has now analyzed 2.6 billion claims and policies for more than 100 customers across the world. In addition to offering more precision and fewer false positives, customers enjoy the following:

- *Increased productivity among fraud handlers—letting them focus on the claims that matter.*
- *Low impact on the existing processes and activities—Shift Claims Fraud Detection adapts to fit into the insurer’s organizational structure.*
- *Quick adoption—ergonomic and customizable dashboard.*
- *Tangible short-term ROI—savings from increased detection rates can outweigh the implementation costs within weeks*

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

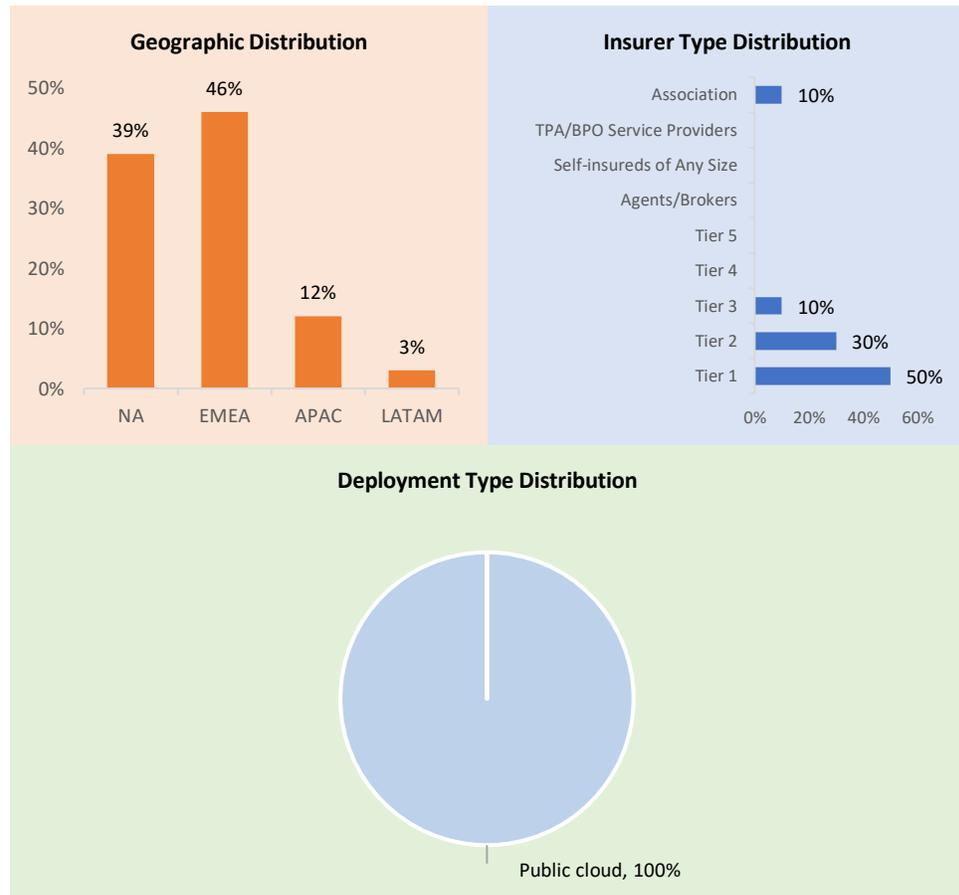
- Design and update monitoring dashboards ●
- Assign/share fraud cases with other investigators ●
- Check fraud case logs (status changes, audit trails, etc.) ●

- = 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, Size, Type of Insurer, and Deployment Type (Global)



Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
Code Base	C#: 70%; Java: 9%; Python: 21%
Database	SQL
Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: Not disclosed

Integration Methods	Web services, XML (not through web services), RESTful HTTP style services, JSON format, custom APIs, flat files
----------------------------	---

Source: Vendor RFI

Table 5 SaaS Capabilities

Elements	Response
Supports a multitenant architecture	No
Type of effort required to update the solution	Evergreen—client chooses when to upgrade
Cadence of upgrades for multitenant deployments	More frequent than every three months
Deployment approach supports elasticity	Yes, within less than a day
Current API-related strategy	Not disclosed
Deployment model can leverage a serverless approach	No
Solution enables independent services (microservices)	No
Proportion of the system architected as microservices	Under 25%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	No
Need for containerization to run in a cloud	No
System’s functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✓
Amazon Web Services (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.	■
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; x = Not available

Source: Vendor RFI

Data

Shift Technology's data model is proprietary.

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

Shift will extend its data model to support client needs. The data model can be easily published to a client's data model and can map to an intermediate format to share with a client (such as an industry standard).

The client can change the data format and which data is sent to Shift Technology. Shift Technology will do the necessary changes to integrate the new data. For example, if the client is sharing a new piece of information, Shift Technology will adapt the data integration process.

Shift Technology's data model is proprietary. The company integrates with any client data format. In cases where the client data model includes fields that do not exist in the Shift data model, Shift will extend its data model to support it.

Security

Shift Technology complies to the following security standards: SOC 2 Type 2; HITRUST; General Data Protection Regulation (GDPR); and ISO 27001.

The vendor is not PCI compliant.

One-time passwords, flexible user permissioning, multifactor authentication, and federated identity support are available as authentication factors for internal and external users.

For cybersecurity arrangements, Shift Technology designed Shift Claims Fraud Detection with data security and privacy in mind at all times. Shift is ISO 27001, SOC 2, HITRUST and GDPR

certified. The company undergoes annual security audits for these certifications, and reports can be shared upon request.

Shift Technology has extensive security policies in place defining strong technical and organizational controls as well as regular penetration tests, the results of which can also be shared.

Data flowing through Shift is always encrypted at rest and in transit. Each customer has its own virtual instance of the solution, segregated from the other customers through strict network isolation. Strong authentication policies are in place, which includes a fully configurable password policy, as well as the use of two-factor authentication and single sign-on (SSO).

The company answers any security questionnaires requested by customers and undergoes any additional audits upon request.

The system has penetration security.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Capgemini, Accenture, GFT, Deloitte, EY, BearingPoint, Avanade
Fintech Partners	N/A

Source: Vendor RFI

Implementation, Support, and Pricing

Table 9: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
Resource Breakdown	Vendor: 80%; Insurer: 20%; Third party: 0%
Location of Employees	Shift Technology has employees in North America, EMEA, APAC, and LATAM, with 29 in North America, 102 in EMEA, 14 in APAC, and 4 in Latin America.
Average Time to Implementation	<u>Initial implementation:</u> 1 to 3 months <u>Second and subsequent line of business:</u> 1 to 3 months <u>Second and subsequent states/jurisdictions:</u> 1 to 3 months
Preferred Implementation Approach	Not disclosed
Pricing Models	None

Factors Used to Determine PricingUsage-based factors: NoneTier-based factors: NoneOther factors:

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	Annualized Subscription	No Separate Fees	No Separate Fees
Average Remaining Costs (Year Two and Beyond)	Annualized Subscription	No Separate Fees	No Separate Fees

Source: Vendor RFI

VERISK: VERISK'S FRAUD SOLUTIONS

Company and Product Snapshot

Verisk is a public company headquartered in New Jersey, US, with sales and professional services personnel located throughout North America. The company has 9,367 employees, of which ~200 are available to support Verisk's Anti-Fraud Solutions.

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

Table 1: Company Snapshot

Year Founded	1971
Number of Employees	9,367
Revenues (USD)	\$2,999,000,000
Financial Structure	Public company Nasdaq: VRSK
VendorMatch Link	https://www.celent.com/solutions/417215462
User Conferences	The vendor offers an annual user conference or customer event. Verisk also co-sponsors the Insurance Fraud Management Conference (IFM) with the National Insurance Crime Bureau (NICB). This is the P&C insurance industry's premier anti-fraud conference for decision-makers.

Source: Vendor RFI

Table 2: Product Snapshot

Name	Verisk's Anti-Fraud Solutions Suite
Year Originally Released	1971
Current Release and Date of Release	Daily data updates. Tech 2022/2022
Revenue Derived from the Product	Proprietary
R&D Expense	The vendor's R&D investment is proprietary and proportional.
FTEs Providing Professional Services for Product	~200
Regional FTEs (NA/EMEA/APAC/LATAM)	200/0/0/0
Target Market	Insurers, TPAs, self-insureds, state governments, worker's comp funds, law enforcement, national insurance crime bureau
Installed Base	Not disclosed
Notable Clients	A selection of the 100 P&C providers in North America

Source: Vendor RFI

Overview

The vendor states that Verisk provides data-driven analytic insights and solutions for the insurance industry. Through advanced data analytics, software, scientific research, and deep industry knowledge, Verisk empowers customers to strengthen operating efficiency, improve underwriting and claims outcomes, combat fraud, and make informed decisions about global issues, including climate change and extreme events as well as political and environmental, social and governance (ESG) topics. Across the P&C and life/accident insurance industries, insurers, reinsurers, risk managers, and many supporting channels rely on Verisk to better understand the business of risk and advance their digital transformation initiatives. Clients infuse Verisk solutions into marketing and distribution, product and rating, compliance, underwriting, claims, and risk transfer workflows to improve customer experiences while fighting fraud to better manage their business of risk better. Verisk's anti-fraud options serve customers throughout the insurer value chain. Options include advanced technologies and cutting-edge fraud analytics, such as a proprietary source of more than 1.5 billion claims, AI and predictive models, composite analytics, network analytics, automated case management, trust then verify protocols, etc., to enable clients to better serve their customers and business.

Key features include:

- *19PB of data, including the largest claims database (ClaimSearch) and other proprietary databases (AMD, NICB).*
- *No ETL lift for most insurers to implement antifraud solutions.*
- *Extensive industry expertise.*
- *Over 50 years of safeguarding industry data.*
- *Configurable business user tuning and rule-creation capabilities.*
- *Machine learning predictive models, unsupervised modeling, expert business rules, digital photograph forensics, and network analytics exploration.*

Key benefits include:

Verisk's anti-fraud solution have many applications over the life of a claim. Real time scoring for the propensity of fraud utilizing extensive matching claim history data as well as robust third party data sets helps point the trajectory of claim investigations. This includes composite analytics, utilization of aggregated industry data, risk scoring, social and network analysis, and case management. Verisk's solution is customizable so that a client can tailor the solution to its needs and create alerts for its book of business. In addition, through acquisitions and internal development, Verisk has created a vast portfolio of anti-fraud solutions across the insurer value chain, serving many lines of business as well. In underwriting, for example, benefits

include: effectively and efficiently understanding a risk at point of sale (POS) to help avoid rate evasion and premium leakage, fight application fraud, enhance the customer experience, and boost conversion rates. Multiple proprietary and public sources cross-reference and employ advanced analytics and machine learning to score each transaction at POS and renewal to trigger for fraudulent activity such as rate evasion. Additional benefits can include alerting decisioning that might require recalculations to coverage or reinspection, such as renovations, deteriorating roof condition, a change in occupancy, undisclosed drivers, garaging issues, and other patterns of interest. In claims, for example, vast amounts of data improve claim matching and yields greater accuracy with additional benefits of no added time or expense from ETL setup.

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, Size, Type of Insurer, and Deployment Type (Global)

Not disclosed. However, the vendor is a global corporation with fraud solutions in every US state and Puerto Rico.

Source: Vendor RFI

Technology

Table 4: Technology Options for the Solution

Technology Options	Responses
--------------------	-----------

Code Base	Not disclosed
Database	Not disclosed
Scalability	The vendor's largest deployment (total number of transactions processed daily system): Not disclosed Scalability metrics: 33K
Integration Methods	Web services, HTML, HTTP, RESTful HTTP style services, JSON format, MQSeries, JMS or similar queue technology, flat files

Source: Vendor RFI

Table 5: SaaS Capabilities

Elements	Response
Supports a multitenant architecture	Yes
Type of effort required to update the solution	Cloud-based. It is automatic.
Cadence of upgrades for multitenant deployments	More frequent than every three months
Deployment approach supports elasticity	Yes, automatically
Current API-related strategy	Pre-connected cloud environment (fully connected and ready to use)
Deployment model can leverage a serverless approach	Yes
Solution enables independent services (microservices)	Yes
Proportion of the system architected as microservices	Over 80%
Supports automation of development and deployment processes (DevOps)	Yes
Solution runs and deploys under containers to improve the application deployment	Yes
Need for containerization to run in a cloud	No
System's functions and capabilities can be distributed among a private cloud and a public cloud	Yes

Source: Vendor RFI

Table 6: Deployment Options and Public Cloud Provider Support

Public Cloud Providers	Availability
Microsoft Azure	✗
Amazon Web Services (AWS)	✓
Google Cloud Platform (GCP)	✗

Public Cloud Providers	Availability
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.	✗
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

Verisk's data model is proprietary.

Regarding industry standard data model schemas, the vendor states ClaimSearch.

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

It is provided as-a-Service. The data model can be released to the client and can be easily published to a client's data model.

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

Security

Verisk complies with the following security standards: NIST Security Standards, SOC2 Type II + HITRUST, and ISO27001.

The vendor is not PCI compliant, and this is achieved by NA.

One-time passwords, flexible user permissioning, out-of-band identification, multifactor authentication, federated identity support, and other options are available as authentication factors for internal and external users.

The system's cybersecurity arrangements are proprietary.

The system's penetration security is proprietary.

Partnerships

Table 8: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Proprietary
Fintech Partners	Proprietary

Source: Vendor RFI

Implementation, Support, and Pricing

Table 7: Implementation, Support, and Pricing

Typical Implementation Team Size	1 to 5
Resource Breakdown	Not disclosed
Location of Employees	Verisk has employees in North America, EMEA, and APAC, with 200 in North America.
Average Time to Implementation	<p><u>Initial implementation</u>: 0 days to 1 to 3 months</p> <p><u>Second and subsequent line of business</u>: 1 to 3 months</p> <p><u>Second and subsequent states/jurisdictions</u>: 1 to 3 months</p>
Pricing Models	Subscription-based license, enterprise license
Factors Used to Determine Pricing	<p><u>Usage-based factors</u>: Number of total or named users, per functional components/modules used, per transaction, per user/seat, policy or account volume, annual premium volumes/revenues</p> <p><u>Tier-based factors</u>: None</p> <p><u>Other factors</u>: None</p>

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	Confidential	Confidential	Confidential
Average Remaining Costs (Year Two and Beyond)	Confidential	Confidential	Confidential

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. Owing to a variety of reasons, particularly heightened customer expectations, many carriers have focused on automating human touchpoints and creating a more frictionless claims process. With that comes increased susceptibility to fraud. As such, fraud-detection tools are vital resources with a proven ROI that Celent strongly suggests carriers employ.

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 both be aware of their business needs and the solution's capabilities so they can 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.

RELATED CELENT RESEARCH

[Insurance Fraud-Detection Solutions: Life Insurance, 2022 Edition](#)
September 2022

[Insurance Fraud-Detection Solutions: Health Insurance, 2022 Edition](#)
September 2022

[Taking a Pulse on Touchless Claims](#)
August 2022

[Claims Systems Vendors: North American P&C Insurance 2022 Edition](#)
March 2022

[Exploring The Wide World of P&C Claims Insurtechs](#)
February 2022

[Photo Finish: Seeing is Believing](#)
December 2021

[Unlocking the Value of Touchless Claims](#)
August 2021

[Data Science In Claims](#)
November 2020

[Claims Fraud Detection Systems: 2018 IT Vendor Spectrum](#)
May 2018

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
Fabio Sarrico

aschwartz@celent.com
fsarrico@celent.com

Americas

USA

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

[+1.617.424.3200](tel:+16174243200)

USA

1166 Avenue of the Americas
New York, NY 10036

[+1.212.345.8000](tel:+12123458000)

USA

Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

[+1.415.743.7800](tel:+14157437800)

Brazil

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

[+55 11 3878 2000](tel:+551138782000)

EMEA

Switzerland

Tessinerplatz 5
Zurich 8027

[+41.44.5533.333](tel:+41445533333)

France

1 Rue Euler
Paris 75008

[+33 1 45 02 30 00](tel:+33145023000)

Italy

Galleria San Babila 4B
Milan 20122

[+39.02.305.771](tel:+3902305771)

United Kingdom

55 Baker Street
London W1U 8EW

[+44.20.7333.8333](tel:+442073338333)

Asia-Pacific

Japan

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

[+81.3.6871.7008](tel:+81368717008)

Hong Kong

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

[+852 2301 7500](tel:+85223017500)

Singapore

138 Market Street
#07-01 CapitaGreen
Singapore 048946

[+65 6510 9700](tel:+6565109700)