CELENT

AI MADE TO REDUCE FALSE POSITIVES

PART 2: VENDOR SPECTRUM

McGowan, Joan
03 July 2018

OLIVER WYMAN

CONTENTS

EXECUTIVE SUMMARY

KEY RESEARCH QUESTIONS

1 *What can AI promise?*

2 *Why is AI so well-suited to spotting suspicious activities and reducing false positives?*

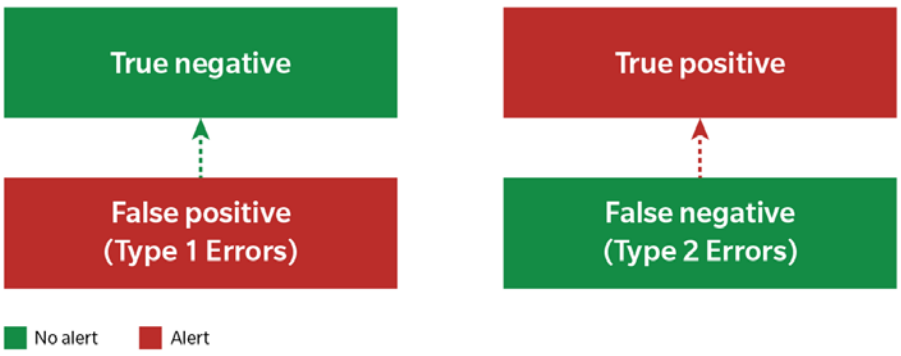
3 *How do you win over the regulators?*

In Part 1 of this two-part report, *AI Made to Reduce False Positives, Part 1: Detection Capabilities and Use Cases*, Celent looks at the limitations of transaction monitoring systems and the crippling impact of high false positive rates on the industry. The report explains the causes of false positives and shows why artificial intelligence (AI) has the potential to be a powerful accelerator of surveillance systems and more accurate risk identification. It also explores the combinations of AI technologies that can be leveraged to help reduce false positive rates, while being explainable to the regulators.

Celent believes that AI is the key to delivering optimal intelligence-driven monitoring and more precise risk identification. Today, a typical financial institution has two options: it can either lower risk thresholds to capture more suspicious activities or it can tighten risk thresholds to lower the number of false positives. If the institution chooses to lower thresholds, the number of false positives increases. If it tightens thresholds, the probability of missing fraud cases increases.

Figure 1 shows a classification of alert types. Financial institutions must be able to identify false positives as true negatives and, more critically, identify false negatives as true positives, without compromising the risk profile of the organization.

Figure 1: Financial Institutions Must Identify False Positives (type 1 errors) as True Negatives and Unearth False Negatives (type 2 errors) as True Positives



Source: Celent

Key Research Question

1

What can AI promise?

AI promises to break the traditional trade-off between false positives (type 1 errors) and false negatives (type 2 errors), allowing financial institutions to lower thresholds without increasing false positive numbers. In fact, false positive rates will drop.

Part 2 of the report series profiles 13 vendors that are actively developing AI solutions for the reduction of false positive numbers. All of the vendors offer a form of advanced data analysis and machine learning techniques. Some vendors focus on access to news content, watchlists, and unstructured data, where others focus on intelligent automation, robotic process automation or more advanced segmentation analysis. Notably fewer vendors are developing natural language processing and natural language generation techniques. Celent believes the implementation of narrative generation tools are low risk and low cost, and that these tools are suitable for the parsing, analysis, and construction of negative news content and regulatory filing narratives, as well as the generation of suspicious activity reports.

INTRODUCTION

The financial services industry continues to struggle with out of control false positive numbers. Standard Chartered Bank recently stated that 99% of alerts from its transaction monitoring systems are false positives. Europol estimates that only 10% of suspicious transaction reports are further investigated after collection, a figure that is unchanged since 2006, and that less than 1% of the $1 trillion of illicit funds (2014 estimate) that flow through the financial system each year is frozen or confiscated[1].

Fortytwo Data estimates that large financial institutions spend in excess of £3 billion (US $4.6 billion) per year on AML screening alone[2], but despite the high spend on detection technology the industry continues to struggle to monitor and accurately analyze vast amounts of data. Transaction monitoring systems are one of the biggest consumers of data across the institution, but they are not designed to handle data quality, data complexity, and extensive data flows, and they don't have the capabilities to search the internet to uncover hidden links. Transaction monitoring models typically use pre-configured risk scenarios to screen for anomalous behavior. These scenarios don't account for what we know we don't know — "unknown knowns" or for what we don't know we don't know — "unknown unknowns" or what risk scenarios should look like for emerging products and services.

AI is particularly well-suited to reducing the hundreds of thousands of false positive alerts generated in a typical institution. By combining AI technologies, institutions can improve detection rates, reduce false positives, and free up analysts to focus their efforts on investigating high-risk activities.

AI is a complex topic that brings with it a new class of acronyms. For ease of reading, this report uses the following acronyms:

Acronyms Used in the Report

AI	Artificial Intelligence	AML	Anti-Money Laundering
ML	Machine Learning	SAR	Suspicious Activity Report
RPA	Robotic Process Automation	STR	Suspicious Transaction Report
NLG	Natural Language Generation	KYC	Know Your Customer
NLP	Natural Language Processing	EDD	Enhanced Due Diligence
IA	Intelligent Automation	UBO	Ultimate Beneficial Ownership
API	Application Programming Interface	POC	Proof of Concept

[1] Europol Financial Intelligence Group: From Suspicion to Action: Converting financial intelligence into greater operational impact, 2017.
[2] Banks' AML divisions wasting almost £3 billion every year

AI FALSE POSITIVE USE CASES

Key Research Question

2

Why is AI so well-suited to spotting suspicious activities and reducing false positives?

In the world of risk, AI has a very distinct use case. Machines can sift through millions of data sets and spot ambiguous behaviour probabilistically — an impossible task for a human. Additionally, AI can quickly recalibrate and improve its models based on feedback, another task beyond the ability of a human.

AI uses a combination of advanced technologies to imbue computer systems with some of the "cognitive intuition" of an investigator.

- **Computing Power** enables financial institutions to rapidly drill down through thousands of data rows to make informed assessments that an investigator simply cannot reach quickly enough. Once the data is normalized and categorized, it can be matched against behavioral patterns, asset information, vulnerability information, watchlists, and data lists to determine relationships in real time. The use of in-memory processing can help the institution segment and prioritize more complex and riskier activities.

  Machine Learning takes place when computers change their parameters / algorithms on exposure to new data without the need for an analyst to reprogram. One of the major benefits of ML is its capacity to process more data than an analyst ever could, and then to use the compiled data to spot patterns that would be hard for a human to identify. The use of ML allows analysts to reach insights into suspicious activities that previously would have remained undiscovered.

  The ability to retrain and recalibrate models and automatically adjust thresholds and parameters is a powerful tool for risk model management.

- **Data Analysis** of texts, images, and audio will greatly expand the universe of data that can be analyzed in a meaningful way.
  - Semantic analysis applied to large data sets containing multiple instances of the same entities can help leapfrog issues such as name variants. Semantic analysis assesses the latent risk of an entity in the context of a larger corpus of negative news content, without the complexity and cost of data normalization.
  - Link analysis of entities and social networks uncovers who's who and who knows who. It connects hidden activities and relationships at a network dimension.

Most institutions don't have the data science resources required to update models in a timely manner. Assembling and testing the data needed to retrain an analytics model can take months, and it has become common practice for organizations to recalibrate rules-based models once a year.

- **Intelligent Automation** combines analytics, workflow, and RPA with capabilities such as ML to streamline and optimize processes. IA improves efficiencies, consistency, and decision-making.
- **Robotic Process Automation** handles routine and smart processes that join robotics with IA to enable the automation of workflow tasks that require decisions.

RPA is a growing feature in KYC checks and regulatory obligations, where automation is used to bring in data, run compliance checks, and capture and record information. Unsupervised RPA can be deployed to automate rote work and achieve quick resolution of false positive alerts. Supervised RPA can support the analyst in tasks such as copying and pasting or navigating between systems and screens to expedite the evidence-gathering processes.

- **Natural Language Processing** uses human communication, naturally spoken or written, as an input to prompt computer activity. The human's unstructured words are parsed and converted into machine-readable instructions. Once the program has understood and processed the instructions, it responds either in a computer-friendly format, a useful graph, or spoken or written plain language. NLP can be used to parse, analyze, and prepopulate part of the regulatory filing narratives. This saves analysts time in the manual compilation of efilings and reduces errors.
- **Natural Language Generation** produces human-quality prose based on a wide variety of inputs. Generating plain language responses is a critical to eliminating the need for human intervention. NLG can automate many types of routine tasks, including the generation of reports.

In the world of risk, AI has a very distinct use case. Machines can sift through millions of data sets and spot ambiguous human behaviour probabilistically — an impossible task for a human. Additionally, AI can quickly recalibrate and improve its models based on feedback, another task beyond the ability of a human.

AI development is advancing daily but the greater the coverage of the different AI approaches doesn't necessarily mean the better the product. The 13 vendors profiled in Part 2 of the report all offer a level of advanced analysis and ML but what is notable, is that each AI solution is heavily influenced by the core technology capabilities of its vendor. For example, Ayasdi, Brighterion, FICO, IBM, Intel Saffron, Oracle, Pelican SAS, and ThetaRay offer variations of advanced analysis techniques; **Arachnys,** LexisNexis Risk Solutions, and RDC focus on the collation of data and library of sources; and NICE Actimize offers a supervised and unsupervised RPA process.

This report looks at **Arachnys Customer Risk Decision** platform and its focus on curated risk intelligence. Financial institution should use this report to understand Arachnys' choice of AI strategy and technologies and decide if their requirements align to this approach.

REPORT METHODOLOGY

APPROACH

To analyze the ability of AI solutions to reduce false positives across the financial services industry, Celent invited a selection of financial crime risk-focused vendors to respond to detailed questions through RFIs, interviews, and demos. The information requested covered the capabilities provided by the solution, the choice of AI technologies and architecture, and roadmaps.

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

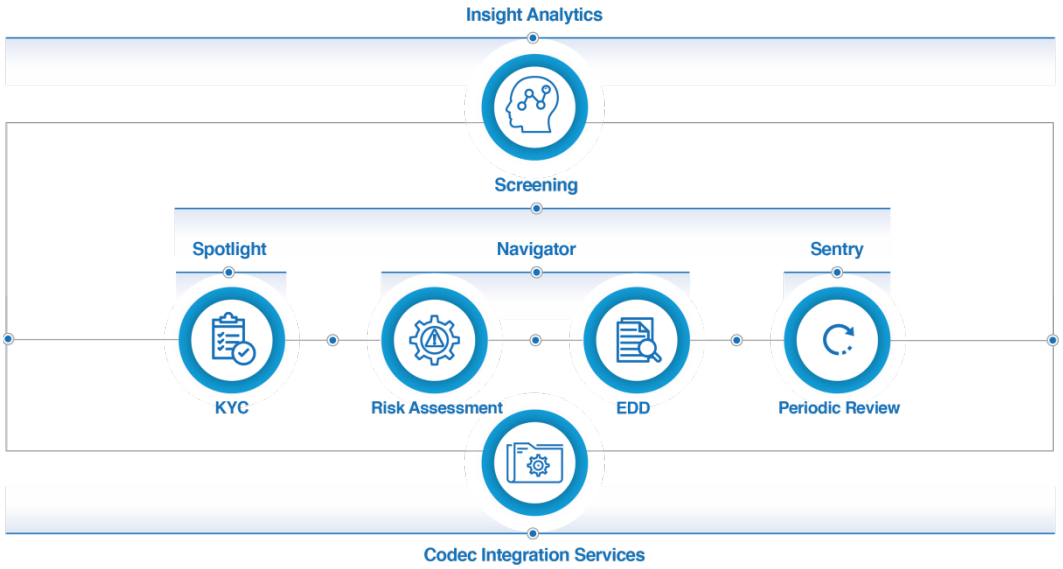
LIMITATIONS

Celent believes that this study provides valuable insights into exploratory solutions for fraud, AML, and security risk management, specifically focused on the prevention of false positives and the exposure of false negatives. However, readers are encouraged to consider these results in the following context. The vendors self-reported, and while this information was supplemented with publicly available information where possible, Celent did not independently confirm the details provided by the participants.

ARACHNYS

Arachnys was founded in 2010 and is run by a team with a strong pedigree in financial crime technologies. Its flagship cloud-native solution, the Arachnys Customer Risk Decision platform, is comprised of five connecting products that map to a financial institution's risk monitoring and evaluation journey. Arachnys has approximately 80 clients on the platform using some or all of its capabilities.

Figure 2: Arachnys Solution Comprised of Five Products that Map to an Institution's FCRM Risk Evaluation Process



Source: Arachnys

Figure 2 shows the connected capabilities and flow of Arachnys Customer Risk Decision platform:

- ***Spotlight*** builds, enriches, and maintains a comprehensive view of entities to produce KYC, Customer Identification Program profile assembly and client data verification, UBO, and relationship identification.
- ***Navigator*** centralizes investigations and policy adherence for high risk investigations, EDD, and transaction monitoring support.
- ***Sentry*** automates event-driven and real time delta monitoring and reporting. It focuses on the periodic CIP review and the monitoring of use cases.
- ***Insight*** provides analysis on operational performance, usage activity, various risk analytics, and metadata for business intelligence purposes.
- ***Codec*** is an integration platform that provides open APIs and web services that enable an institution to integrate in-house or third-party systems.

To minimize the number of false positives, Arachnys uses ML, RPA, and IA to process, index, monitor, and update vast quantities of structured and unstructured data, including content from Arachnys' proprietary database of over 23,000 global data sources. Clients can quickly search and assemble information relevant to an investigation. AI discovers the relevant content within a document and "robots" (RPA) record what a human does

and simulates the process (IA) for the purposes of automating data gathering. The system continues to monitor an event and automatically extracts updated information to improve the efficacy of an alert/case.

Platform capabilities that improve detection accuracy and reduce false positives include:

Identification of risk trends: ML and IA are used to identify risk trends and behavioral patterns within the data to enable more accurate risk decisions. Supervised ML deconstructs historical dispositions to improve insights into a likely future threat event.

Results clustering: Searching the internet for negative news coverage on a specific person or event is a burdensome exercise for analysts. A single search term on Google can return hundreds of thousands of results. The analyst has to make a decision as to what information to investigate and then begin the process of screen scraping, copy and pasting or downloading large volumes of information. The work is rote, time consuming, and prone to mistakes. Arachnys' use of automated analysis and result clustering on big data assists analysts in the collection and curation of information. The platform trawls the internet for negative news and then identifies, classifies, and prioritizes items that show similar risks or are related to the same event. Analysts leverage the platform to assemble a concise selection of news coverage.

Source relevancy: Over time, supervised ML algorithms identify which sources are best utilized and the relevancy score of each source is adjusted accordingly. The more useful the information, the higher the score. Scores are continually re-tuned based on the modeling of historical disposition results and through an analyst feedback loop.

Data assembly automation: Arachnys' Unified Data Adaptor accelerates the data acquisition process by capturing and classifying data and merging updated information into the entity profile. The automation of data collection reduces human errors and inconsistency and improves the quality of data being captured, allowing for more precise analysis and fewer false positives.

Keyword identification: Unsupervised ML algorithms analyze the data that has been marked as effective to identify patterns that can be used as search keywords. It then compares the effectiveness of search keywords with the adverse keyword terms defined by the institution as part of its investigation policy. This allows managers to fine-tune their research policy and improve search results.

Auto suggestion of risk conclusions: An assessment of source relevancy and risk classification enables the institution to preserve its knowledge, maintain consistency, and identify outliers within its own investigation processes.

Arachnys believes that AI makes the job of investigation more manageable, but that it will not replace the need for human judgement. By providing concise information in a ready format, analysts can make more informed judgments on the risk level of an alert and the actions required.

NEXT STEPS

Key Research Question

3

How do you win over the regulators?

Do not lose control or not know why the computer does something. Model governance, model validation, and transparency of machine-generated results will help get regulators on board with institutions' use of advanced analytics and AI.

Despite its portrayal in fiction, AI is not the monster inside the machine. It is a series of enabling technologies that range from intelligent automation to deep cognitive learning. Celent believes AI can reduce the volume of false positive alerts generated in a typical institution, without the institution having to adjust its risk exposure.

Celent offers the following high-level steps to make AI less daunting and more manageable:

- **Become educated about the potential of AI.** Educate staff on the potential of AI technologies. Evangelize the institution's AI strategy and emphasize that its purpose is to complement the work of analysts. Remember, when the cost of prediction falls, there will be an increase in demand for human judgment.
- **Develop a governance program.** AI governance should reflect an institution's risk appetite statement. It is important to bring internal stakeholders and regulators to the table to determine the mechanisms that will minimize the risks and possible downsides of AI and autonomous systems.
- **Take caution.** Do not lose control or not know why the computer does something. Regulators are making it clear that compliance processes, including analyses, actions, and decisions generated by compliance technology, must be demonstrable and auditable. Model governance, model validation, and transparency of machine-generated results will help get regulators on board with institutions' use of advanced analytics and AI.
- **Do not focus AI business cases on reducing costs.** Although AI can boost efficiencies through the automation of highly manual compliance tasks, the real ROI is freeing up analysts to focus on high-value risks and data scientists to study new threats.
- **Agree on an AI Charter.** A charter keeps teams focused on the objectives by clearly defining what is in and out of scope. It identifies who should be involved, names project roles and responsibilities, and serves as a reference point when making decisions.
- **Order data.** Data is the foundation of any successful AI initiative. An institution can benefit from data management structures already in place. There should be no reason to reinvent the wheel.
- **Prioritize initiatives and identify an early win.** Institutions should work toward initiatives that have a high and immediate impact. For example, the reduction of false positives will have a mushrooming effect on risk mitigation and compliance.

- **Provide metrics.** Design tracking and feedback mechanisms from the beginning so that management can gauge progress from the outset and make the inevitable adjustments based on a complete set of information.
- **Don't go it alone.** AI is a new and emerging technology with relatively few experts; institutions should look to trusted partners to help them in their AI journey. Although the selection of vendors covered in the report is limited to 13, their profiles will provide financial institutions with a better understanding of what AI technologies are being developed for risk and compliance and, specifically, for the reduction of false positives.

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

LEVERAGING CELENT'S EXPERTISE

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

SUPPORT FOR FINANCIAL INSTITUTIONS

Typical projects we support related to risk management include:

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

Business practice evaluations. We spend time evaluating your business processes, particularly in domains including operational risk (cybersecurity, fraud, AML, and compliance) and finance risk. 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

RegTech on the Rise: Transforming Compliance into Competitive Advantage
June 2018

AI Made to Reduce False Positives, Part 1: Detection Capabilities and Use Cases
May 2018

Innovations in AML and KYC Platforms: New Models Powered by Advanced Computing
January 2018

Artificial Intelligence in Insurance: Starting at the Beginning
December 2017

Bank Insider for Sale: Analytic Approaches to Deter Bank Insider Threats
November 2017

Cloud-Enabled Governance, Risk, and Compliance Solutions
October 2017

Artificial Intelligence in Banking: Where to Start?
August 2017

Under the Spotlight: Innovative Vendors in Financial Crime Case Management Technology
August 2017

Understanding the Investment into AI in Banking: Celent Digital Panel Series 6
July 2017

Artificial Intelligence in Insurance: Use Cases from Early Adopters
December 2016

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

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

Artificial Intelligence in the Banking Industry: From Data Analysis to Semantic Analysis
July 2016

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

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

Joan McGowan jmcgowan@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucri Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

Canada

1981 McGill College Avenue
Montréal, Québec H3A 3T5

Tel.: +1.514.499.0461

EUROPE

France

28, avenue Victor Hugo
Paris Cedex 16
75783

Tel.: +33.1.73.04.46.20
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Spain

Paseo de la Castellana 216
Pl. 13
Madrid 28046

Tel.: +34.91.531.79.00
Fax: +34.91.531.79.09

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059

China

Beijing Kerry Centre
South Tower, 15th Floor
1 Guanghua Road
Chaoyang, Beijing 100022

Tel: +86.10.8520.0350
Fax: +86.10.8520.0349

Singapore

8 Marina View #09-07
Asia Square Tower 1
Singapore 018960

Tel.: +65.9168.3998
Fax: +65.6327.5406

South Korea

Youngpoong Building, 22nd Floor
33 Seorin-dong, Jongno-gu
Seoul 110-752

Tel.: +82.10.3019.1417
Fax: +82.2.399.5534