# CELENT

# DAWN OF A NEW ERA IN AML TECHNOLOGY

## ADVANCED ANALYTICS POWERING INTELLIGENT AUTOMATION

Arin Ray
June 2018

# CONTENTS

# EXECUTIVE SUMMARY

## KEY RESEARCH QUESTIONS

**1** *What are the main challenges in AML operations today?*

**2** *How can these challenges be solved?*

**3** *What is the outlook for adoption of advanced analytics in AML?*

**The stakes of financial crime compliance operations have risen manifold.** But **traditional technology used in compliance operations has reached an impasse**. Rules-based technology and siloed operations are proving to be inadequate in detecting hidden risks, and financial institutions are drowning in alerts that mainly deal with "spot checks" instead of profiles or events. **A flood of false positives and heavy reliance on manual processes are making AML programs costly, inefficient, and unsustainable.**

**Effective and efficient compliance will require more intelligent solutions and automated workflows**. Financial institutions are adopting several advanced analytical tools in AML, including graph analytics, artificial intelligence, machine learning, and process automation, on top of rules-based systems. They can help in several ways.

- *Risk based approach:* intelligent tools enable institutions to adopt a more informed and risk-based approach, and ensure that most critical attributes and scenarios are fed into a detection engine that has finely tuned parameters and thresholds.
- *Optimal, quality alerts:* the detection engine, augmented by machine learning techniques, will generate **optimal number of high quality alerts that are prioritized according to risk**.
- *Efficient investigation and feedback:* the alerts can be assigned to appropriate investigators based on alert risk and investigator seniority. **Case management can benefit from more automation, better visual analytics, and alert correlation** to investigate related alerts. **Automation also helps in case resolution and closure, and learnings can be fed back** into all stages for continuous improvements.

These will allow financial institutions **manage money laundering risks proactively and holistically, reducing costs, inefficiencies, and chances of fines**; "explainability", auditability and controls would be important to get regulatory approval.

It is clear that financial institutions will have to live with multiplicity of software and applications. It is **important to have easy integration of case management system with internal and external applications**, because analytics applications will need to be tied into a single case management for holistic review and efficient investigation.

AML departments at financial institutions have started dipping their toes in the pool of advanced analytics, and we expect wider adoption in 2018. They start with tactical adoption in one or a few areas; success in early stage should expedite further adoption. Choosing the right solution provider will depend on an institution's immediate needs, longer-term plans on data and infrastructure management, and the partner vendor's ability to offer effective models with easy deployment and maintenance support.

# INTRODUCTION

**Digitalization of financial services is transforming the payment and fund transfer landscape** by creating new products, channels, and modes for transferring funds. This is enabling authorities across the world to undertake major financial inclusion initiatives bringing in masses of new people under the umbrella of banking and payment services.

**The dark side of such developments is that the same tools and technology provide criminals, fraudsters, and money launderers easier access and newer means to engage in illicit activities**. Their complex web of operations is expanding beyond traditional boundaries, from banking channels and payment networks in a few countries, into new geographies, and adjacent services such as insurance, trading in securities and physical assets, casino and gambling, online commerce, and recently virtual currencies.

**The stakes of financial crime compliance operations have risen manifold**. Regulatory scrutiny is growing as evident from numerous instances of fines and consent orders. The scope of supervision is expanding into other industries (e.g., telecom) that are engaging in direct or indirect (e.g., prepaid cards) money services. There is growing pressure on regulators and political authorities to hold senior individuals accountable for lack of oversight and control, **prompting boards and senior management in financial institutions to call for upgrades in compliance practices**.

**Regulatory- and budget-constrained financial institutions are struggling with the difficult trilemma** of ensuring compliance and managing cost without adversely impacting client experience and revenue. **Traditional technology used in compliance operations has reached an impasse** because they have limited capabilities to deal with growing transaction volume, lightning speed of processing, and rapidly evolving web of criminal behavior.

**Effective and efficient compliance will require intelligent automation**, because currently used software systems cannot identify hidden and new risks, heavily rely on manual processes, and are costly to maintain. **Recent developments in advanced analytics and computing, such as graph and network analysis, artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA), are producing solutions with potential to alleviate the challenges**, and we are seeing interesting solutions and use cases emerge.

## ABOUT THIS RESEARCH

This research is part of Celent's ongoing coverage of evolution of new technology and advanced analytics in financial crime compliance operations. This report was commissioned by Oracle Financial Services[1], while Celent kept full editorial control. In addition to Celent's extensive knowledge base in risk and compliance operations, this research greatly benefitted from detailed discussions with compliance professionals from 10 financial institutions from across the globe.

---

[1]www.oracle.com/industries/financial-services/

# ESSENTIALS OF FINANCIAL CRIME COMPLIANCE OPERATIONS

Financial crime compliance operations involve supervision of different types of actors and activities, such as money laundering, terrorist financing, bribery and corruption, tax evasion, fraud, market abuse, insider trading, and other similar nefarious activities. Of these, Anti-money laundering (AML) operations receive the most scrutiny from a regulatory point of view. All nefarious activities end up being tied to AML (to launder the illicit funds), and so **AML is critical for financial crime compliance**.

- An essential aspect of AML operations is to identify and define enterprisewide risk policies based on regulatory guidelines, business portfolio, and client coverage.
- **Know Your Customer (KYC) and onboarding** is the first step in AML whereby institutions collect client information and documents for conducting client risk assessment and business suitability.
- **Watchlist screening** of clients is conducted against government, third party, and internal lists to prevent prohibited actors from accessing the banking system.
- **Payment screening** is conducted at a pre-execution stage to prevent illicit fund transfer.
- Financial institutions also conduct post-execution **transaction monitoring** to identify suspicious patterns and behavior; if found in violation of rules, they need to investigate and report them to appropriate authorities. This is a critical part of AML.
- Additional programs, such as **surveillance, anti-fraud**, for detecting different types of financial crimes can exist — within AML operations, or separately.

Overall effectiveness of AML operations rely on the following critical factors:

- *Identification* of risk (e.g., actors, activities, jurisdictions) in line with the institution's policies and risk appetite.
- *Detection* of bad or suspicious actors and activities involving the institution's customers and counterparties.
- *Investigation* of detected cases for escalation or rejection.
- *Resolution* through allowing acceptable cases, blocking bad cases, and reporting them to internal and external stakeholders.

Maximum utilization of data using appropriate tools and technology is essential for a successful AML program.

- Data can be of various types, such as raw data (e.g., customer name, product type, transaction value), derived data (e.g., risk score, account age, aggregate account activity), public data (government lists, media reports), private data (third party lists), structured, semistructured, and unstructured data, and so on.
- Accordingly, the role of technology and infrastructure to store, query, and process data over different systems and at high speed is paramount.

However, current practices are dominated by suboptimal use of data and technology that is resulting in numerous and growing challenges in AML operations.

# GROWING PAINS IN AML OPERATIONS

|  |  |
|---|---|
| *Key Research Question* **1** | *What are the main challenges in AML operations today?*<br><br>Rules based technology and siloed operations are proving to be inadequate in detecting evolving criminal behavior. A flood of false positives and heavy reliance on manual processes to resolve them are making AML programs costly, inefficient, and unsustainable. |

There are numerous challenges in every stage of AML operations as listed in Figure 1.

Figure 1: AML Operations Are Plagued With Numerous Challenges In Every Stage



| Identification | Detection | Investigation | Resolution |
|---|---|---|---|
| ▪ Regulatory complexity | ▪ Blunt detection engine | ▪ Fragmented systems | ▪ Repetitive and manual case filing |
| ▪ Suboptimal risk assessment | ▪ Limited tuning capabilities | ▪ Limited data availability | ▪ Limited feedback and learning |
| ▪ Data explosion, quality, completeness | ▪ High false positives | ▪ Limited visualization, analytical support | ▪ No knowledge sharing |

Source: Celent

## Identification

Identifying business-specific risks, and defining and implementing policies accordingly are critical to AML, but current practices fall short.

**Regulatory complexity:** Keeping pace with rapid changes in regulations, and understanding their applicability to different jurisdictions, businesses, and product lines is a major pain point. Layers of regulatory complexity — at global, regional, and local levels — create additional difficulties and uncertainties about future changes.

> *"New York Department of Financial Services recently came up with a new rule (Part 504); others in Taiwan, Hong Kong, and Singapore can follow suit. Managing these regular changes is very cumbersome and more important than overall AML cost."*
> *— Tier 1 bank in a leading Asian market*

**Suboptimal risk assessment**: Traditional risk assessment methodology (risk factors, typologies, scenarios) is highly generic, relies on simplistic matrix-based approach, and is driven by *a priori* and subjective understanding of risk, which is not regularly informed or validated by quantitative analysis.

Innovations in financial services are creating new products, clients, and players, but institutions lack the means to analyze and identify new risks and typologies.

**Data explosion, quality, completeness:** Risk assessment and due diligence can be improved by mining the new data available due to digitalization. Specifically, ultimate beneficiary owner (UBO) identification, which is proving to be a big challenge, can benefit from mining new and alternative data sources. Failure to use data that is available to the institution, or can be easily captured, can have serious regulatory consequences.

Even while dealing with traditional data, quality, integrity, and completeness issues are paramount. Cases of incomplete fields, disparate formats, or missing data are common challenges. This **greatly impacts identification and assessment of risks during on-boarding stage, and adds to the challenges during entity resolution in transaction monitoring and investigation**.

## Detection
Detecting suspicious actors and activities in large volume and low latency operations necessitate automated systems, but currently used software has critical shortcomings.

**Blunt detection engine:** Current detection engines are rules-based and perform basic analysis (e.g., payment exceeding threshold values, to prohibited jurisdictions) of a limited number of attributes, using simple descriptive statistics (e.g., mean, variance). They mostly work with structured (at best semistructured) data, using relational databases, and compute simple Boolean operations. They are only able to detect prespecified and basic patterns, and cannot find hidden patterns.

**Limited tuning capabilities**: Because of the limited sophistication of detection engines, users need to diligently choose input attributes and scenarios, and set parameters and thresholds judiciously. However, few financial institutions undertake a quantitative approach to tuning; usual practice is to set thresholds conservatively to minimize risks. In some cases, institutions set thresholds to keep number of alerts within manageable range of their compliance team resources.

**High false positives**: The output of a blunt and suboptimally tuned detection engine is a high number of alerts, an overwhelming share of which is false positives. Banks typically report 90–99% of all alerts are false positives, while those with advanced tuning capabilities report a lower, but still high figure of 80–85%. Worse, a significant part of them are either duplicate alerts (e.g., multiple alerts from same event), or recurrent alerts (repeat hits of previously resolved alerts). **False positives are the most visible symptom of several inefficiencies plaguing AML operations today**.

## Investigation
Investigating alerts is the most inefficient part in AML because of not only too many false positives, but also the complex, tedious, and manual steps involved in the process.

**Fragmented systems**: Gathering data from disparate and fragmented systems to conduct holistic analysis is a challenging proposition, which takes up the bulk of analysts'

time. There are few automated search tools for gathering data from across the enterprise including internal and third party systems, open sources, or public registry. Banks typically report 50–65% of analysts' time is spent doing low-level tasks of data collection, cleaning, and aggregation, while some mentioned a higher figure of 80%.

*"We acquired a bank of comparable size to ours couple of years ago. This has created multiple systems and significant operational complexities."*
*— Tier 2 North American bank*

**Limited data availability:** An additional challenge is the data obtained after such efforts can be poor in quality. Furthermore, relational databases greatly limit scope of using historical data over a long period and including many variables for investigation and analysis; most banks only use 12 to 15 months' data, and a few basic attributes like transaction volume and frequency.

*"Correspondence banking is a huge challenge for data quality, because I cannot control data of my customer's customer, which often lack crucial information such as location. In 40% of cases it can be resolved by additional research, but in 60% cases it is just not there, and regulator wants us to treat all those transactions as highest risk."*
*— Tier 1 global bank*

**Limited visualization and analytical support:** Case management systems have limited support for visualization and investigation tools. While simple charts, plots, and tables are available, moderately advanced operations such as finding links and hidden networks are just emerging. More advanced capabilities such as network drill down or interactive data mining that can aid investigation process are not supported in rules based systems and relational databases, and require separate analysis.

### Resolution
Resolving cases after investigation is another tedious and highly manual process.

**Repetitive and manual case filing:** Current solutions do not support alert prioritization or "low touch" auto closing. The result is low rate of suspicious activity reports (SAR) conversion, typically well below 5%, but filing such reports is manual and can take hours.

**Limited feedback and learning:** Learnings from resolved cases are seldom fed back into identification and detection processes except as rare and one time exercise. Some institutions use white lists, repeat hit suppression, and similar generic techniques, without necessarily incorporating the rationale behind exception handling.

**No knowledge sharing:** Criminal activity accounts for a miniscule share of a financial institution's overall activity, and often occurs using multiple institutions. In absence of industrywide knowledge sharing, financial institutions have limited means to learn and train models.

The cumulative impact of all the challenges is that financial institutions are drowning in alerts that mainly deal with **"spot checks" of specific individuals or transactions instead of profiles or events. They are not able to adopt a truly risk-based approach to focus their best resources on highest risk areas**. Compliance staff sizes at most institutions have grown by twice or thrice in recent years, while some have reported tenfold increase in staff and costs of AML programs. Current best practices in risk-based framework mostly involve a broad-based and tick the box approach, for example prioritizing sanctions list hits over PEP hits, or treating one jurisdiction as more risky than others. Granular and more precise assessment of behavior and risks, peer analysis, group analysis, or advanced segmentation is rarely seen.

# ADVANCED ANALYTICS OPENING NEW FRONTIERS

*How can these challenges be solved?*

Advanced analytical tools have the potential to reveal hidden patterns and risks, streamline alert investigation, automate manual processes, and continuously learn and improve. They will be essential for improving efficiency and effectiveness of AML operations.

It is evident that **there is a dire need for more intelligent solutions and automated workflows** to improve efficiencies and contain runaway costs of AML operations.

*"Our team size has grown 20 times and technology spending has gone up tenfold in the last few years. Regulators are comfortable with our controls now, but it is not sustainable. We now want to improve efficiency without compromising effectiveness."*
*— Tier 1 global bank*

Recent advancements in technology and advanced computing have accelerated the development and adoption of commercially viable advanced analytical tools in a range of industries including in financial services. Financial institutions are adopting several analytical tools in AML on top of rules-based systems, because in spite of the shortcomings current systems are deeply entrenched in financial institutions' operations, and are preferred by regulators due to easy auditability. Therefore the new tools will be additional kits in the AML team's toolbox which will augment the solitary hammer that is the traditional rules-based platform, as shown in Figure 2.

Figure 2: Next-Generation Compliance Toolbox
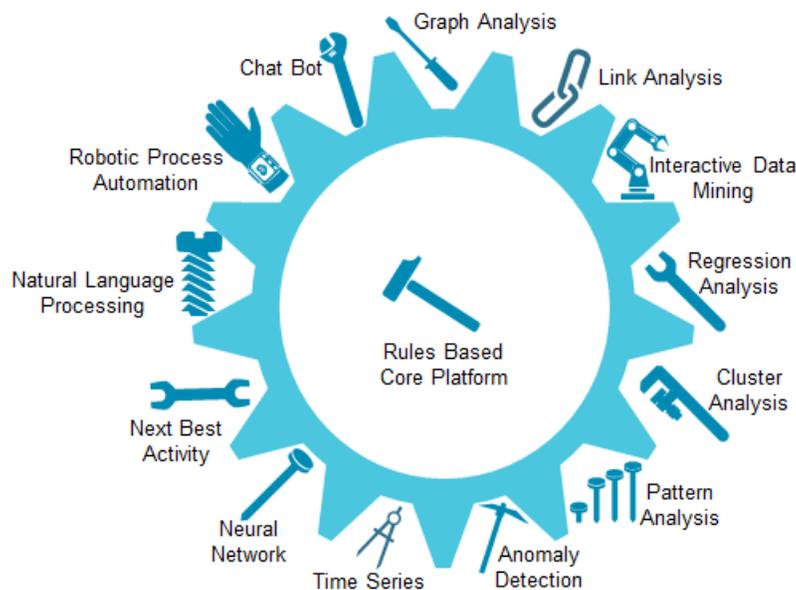


Source: Celent

These tools can be broadly classified into two groups: graph analytics that includes link analysis, and visualization tools; and artificial intelligence (AI) that includes advanced statistical and machine learning tools. We refer to all of them as advanced analytics. Figure 3 highlights examples of potential uses of advanced analytics in AML.

*Graph (or network) analysis* visually represents complex network of individuals, entities, connections (e.g., payments, ownership, media references), severity (payment volume, frequency), proximity (close connection), and centrality (key figure in a network).

– *Link analysis*, can **help in due diligence in on-boarding and UBO identification** by easily showing networks and connections of a customer.
– New dimensions, such as transaction flow and chronology, could be added to reveal flows over time that can **help in transaction or fraud monitoring**.
– *Interactive data mining* that allows users to drill down graphs based on their subject of interest (instead of predetermined, limited tables) can further **aid investigators in dynamically gathering additional and quality information**.
– *Graph analysis* can be used in **entity resolution, and event correlation** to present relevant events as a single case for improving investigation efficiency.

*Regression analysis* identifies relationship among many and different types of variables.

– It can help in **identifying attributes that are good predictors of risk,** remove redundant ones, **optimize tuning parameters**, and predict expected behavior.
– Similarly it can help in calculating risk scores of alerts (based on underlying attribute scores and past experience), which **helps in prioritizing alerts**.

*"We just finished a PoC where regression analysis revealed important attributes for predicting risk which we were not using previously."*
*— Tier 1 insurance company*

*Cluster analysis* identifies subsegments containing elements homogeneous to each other and distinct from others in a given population.

– This can help in **segmenting clients** into different subgroups based on their behavior and risk profiles, and identify peers with similar risk profile.

*Pattern analysis* is similar to cluster analysis, and can reveal hidden patterns.

– Patterns can be found in a person's behavior (cash inflow, outflow, or mouse movement in online banking session) to **create a normal behavioral profile. Same can be done for her peer group, or family**.
– Knowledge of "normal behavior" can then **help in identifying anomalous behavior**, when there are "outliers" or significant deviation from "expected behavior" used in **spotting fraud** such as card theft or account hacks.
– Pattern analysis can also reveal new scenarios and detection algorithms; including them in the core detection engine will require careful validation, controls, explainability, and regulatory approval.

*"We just finished a PoC where we used all our transaction history, and it threw up interesting outliers that are less in number and of better in quality than regular alerts. We plan to use it as a complementary tool to our transaction monitoring engine."*
*— Tier 1 bank in the Americas*

*Robotic process automation* which allows automated interaction between systems and processes **can boost productivity levels**. In AML it can **help in collecting and aggregating information needed in case investigation, and in filing automated**

**reports in prespecified formats**. Chatbots and virtual assistants can **easily offer commonly sought but tedious to find information**. Adding minimal cognitive capabilities to RPA tools can **help in data cleansing, repair, and reconciliation**.

*Next best activity*, a popular tool in digital marketing which helps users navigate a website based on her indicated interest, can **suggest investigators' likely next steps** based on learning and feedback from previously resolved cases.

*Natural language processing* (NLP) helps in **media and document analysis,** while *natural language generation* (NLG) creates **narrative reports quickly and at scale**.

Figure 3: Advance Analytics Can Improve Efficiency and Effectiveness of AML Program

| Identification | Detection | Investigation | Resolution |
|---|---|---|---|
| ▪ Cluster analysis for segmenting clients in different risk categories | ▪ Cognitive RPA tools to improve quality of data in message fields | ▪ Auto (low touch) closing of alerts | ▪ Automated case filing |
| ▪ Regression analysis to identify critical predictors of risk, tune models | ▪ Auto (low touch) threshold adjustments through regression, and what-if analysis for given risk level | ▪ Link and graph analysis for visual investigation | ▪ NLG for narrative based advanced reporting including SAR generation |
| ▪ Graph analysis for connecting different entities for entity resolution | ▪ Conditional thresholds for specific types of algorithms | ▪ Interactive data mining for detailed investigation | ▪ Automated learning and feedback to detection and investigation steps |
| ▪ What if analysis for ATL / BTL analysis and tuning | ▪ Graph analytics, queries, ML algorithms, e.g., neural network | ▪ NLP for Adverse Media Analysis | |
| ▪ Pattern analysis to reveal unknown patterns to create rules and scenarios | ▪ NLP for name matching | ▪ RPA for information collection and aggregation | |
| ▪ NLP to scan documents for regulatory change management | ▪ Intelligent list management for efficient screening | ▪ Chatbots and virtual assistants | |
| ▪ Dynamic risk assessment | ▪ Predictive analysis for risk based alert scoring, prioritization | ▪ Next best activity | |

Source: Celent

The new tools can help improve efficiency and effectiveness manifold.

- In identification stage they make it possible to **adopt a more informed and risk-based approach**, and help ensure that most critical attributes and scenarios are fed into a detection engine with finely tuned parameters and thresholds.
- The detection engine, augmented by graph analytics and machine learning, will generate an **optimal number of high quality alerts** prioritized according to risk.
- These alerts can then be assigned to appropriate investigators based on alert risk and investigator seniority. **RPA tools can increase productivity in case management, and visual analytics can provide new insights**. Predictive analysis helps in automated or low touch alert closure, and expedites investigation.
- Automation also helps in case resolution and closure, while knowledge and **learning can be fed back into all stages to for continuous improvements**.

These will allow financial institutions to **manage money laundering risks proactively and holistically, reducing chances of breaches and fines**. They should **bring down costs and improve productivity** levels, and minimize customer dissatisfaction and churn. We have seen 30–50% efficiency improvements in several use cases and PoCs.

*"In our PoC we found with intelligent alert prioritization, over 45% of alerts can be auto-closed with 95% confidence, and additional 20% can be closed with minimal oversight."*
*— Tier 1 global bank*

# CONSIDERATIONS FOR ADOPTION

Practitioners typically cite two types of questions while considering adoption of advanced analytics in AML.

## Auditability and Regulators' Reaction

Regulators demand AML programs to have strict controls, transparency, auditability, and documentation. Some of the **advanced analytics tools can have the perception of being black boxes that lack "explainability";** financial institutions therefore want to be cautious in their approach to adopting new tools and technology. Providers of these solutions are working on offering model explainability, audit trails, and documentation support as much as possible to assuage the concerns.

## Implications for Data and Infrastructure Management

Data management is a critical issue, because current practices suffer from system fragmentation and poor data quality. In addition to traditional data quality challenges seen across an enterprise, **AML operations suffer from data standardization issues** when dealing with names, aliases, addresses, different watchlists, etc.; preparing data for entity resolution therefore is a tedious process.

**Relational databases are not well-equipped to support high volume** (millions of customer and transactions in AML over a long time period) **and different types of data** (customer, transaction, reference data, lists, news media) from multiple internal and external sources, and at processing them at a low latency to support detection and investigation. Similarly, **relational databases have limited capabilities for representing graphs and networks,** and supporting interactive data queries in real time.

Financial institutions have been investing in data warehouses, data lakes, open source and big data in-memory distributed processing technlogy (e.g., Apache Spark) for some time for improving data management. Some interview participants mentioned **addressing data lineage, governance, privacy, and security issues can slow down adoption of new technology, especially because the big data technologies are evolving very rapidly**.

It is clear that **financial institutions will have to live with multiplicity of internal, third party, and increasingly open source software and applications** in any given part of operations, in spite of numerous efforts to rationalize them. Therefore, **modern thinking has shifted to adopting a modular approach** connecting different applications through APIs and microservices. In the AML context, **it is particularly important to have easy integration of case management system with internal and external applications**. This is because many applications, including those leveraging advanced analytics, will need to be tied into a single case management for holistic review and efficient investigation.

# DAWN OF A NEW ERA IN AML TECHNOLOGY

<table>
<tr><td>**Key Research Question**</td><td>*What is the outlook for adoption of advanced analytics in AML?*</td></tr>
<tr><td>**3**</td><td>2017 was the year for PoCs, and we expect wider adoption in 2018. Financial institutions will start with tactical adoption in one or a few areas; success in the early stage should expedite further adoption.</td></tr>
</table>

**AML departments at financial institutions have started dipping their toes** in the pool of advanced analytics. **2017 was the year for PoCs,** as several institutions mentioned having just completed major PoCs, and others have made public announcements along similar lines in the last 12–18 months. We observe the following adoption trends:

- Leading institutions, such as tier 1 and some regional, technologically sophisticated firms, have resources to manage technology and infrastructure in-house and are ahead in developing enterprisewide big data architecture and data lakes. They also have **strong compliance analytics divisions with many data scientists** who can **fine tune existing solutions with analytics tools embedded in them, work with AI and RPA platforms to develop custom applications, or partner with fintechs in developing PoCs**.

- Midsize players have not yet achieved mature data and infrastructure practices, and lack resources to experiment with analytics solutions in-house. They are more likely to **adopt proven and ready-to-deploy tools and applications on top of current systems**. They are looking to benefit from analytics tools while minimizing their impact on current data and infrastructure management practices.

- Some players are still grappling with more short-term issues, such as implementing a new platform or replacing in-house case management systems with a single third party solution. Ensuring system stability in the near term is more important for them than strategizing for medium-long term. They are seeking **RPA tools for productivity improvement, and enhanced analytics from existing platforms**.

**We expect to see wider adoption in 2018** as some of the finished PoCs are taken into production. **Early adoption will be tactical**, and focused on one or a very few areas to ensure the new solutions meet all requirements, especially in control and auditability.

*"We want to first walk before we run; but if we get the first one or two cases right I expect to see wider and faster adoption in the future, because the potentials are huge."*
*— Tier 1 global bank*

Traditional AML software providers are enhancing their offerings with advanced analytics, within the core platform or by building ancillary tools on top of it. An ecosystem of new players is emerging with custom solutions leveraging generic AI platforms. Accuracy and effectiveness of models, as well as ease of deployment and maintenance (especially for institutions without armies of data scientists), will be important parameters for choosing the right partner.

*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 and compliance 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 risk and compliance. 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

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

Innovation in AML Technology: New Tools for Optimizing Compliance Efficiency
November 2017

A New Era in Capital Markets Surveillance: As Far as the AI Can See
November 2017

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

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

Rearchitecting the Capital Markets: The Cloud Cometh
May 2017

The Cloud Comes of Age in Capital Markets: All Clear for More Cloud
December 2016

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

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

Risk Outlook for Banking: Calmer Times
June 2016

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

Emerging Solutions in Anti-Money Laundering Technology
May 2015

Emergence of a Utility Model: The Case of KYC On-Boarding Solutions
September 2014

# Copyright Notice

## Prepared by

Celent, a division of Oliver Wyman, Inc.

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

Arin Ray                          aray@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