CELENT

FIGHTING FINANCIAL CRIME AMIDST GROWING COMPLEXITY

THE NEED TO RETHINK AML TECHNOLOGY AND APPROACH

Arin Ray
18 April 2018

OLIVER WYMAN

CONTENTS

GROWING COMPLEXITIES IN FINANCIAL CRIME COMPLIANCE OPERATIONS

Financial institutions are facing intense pressure in financial crime compliance operations. Exploding costs and risks of running compliance programs are forcing banks to rethink their strategy, resulting in some cases in termination of relationship and service offerings. In addition to impacting revenue streams for individual banks, such trends can impact the broader economy by stifling commercial activities and economic output.

NO SIGNS OF REGULATORY RESPITE

There are no signs of regulatory respite after many cases of heavy fines, penalties, and settlements, running to the order of tens of billion dollars at the industry level. Instead **the remits and expectations of regulators continue to grow**.

- Beginning with a focus on tackling organized crime, scope of financial crime compliance has expanded to include a range of activities such as terrorist financing, economic sanctions, political corruption, tax evasion, trade based money laundering, and other illicit activities; these risks are often managed by an institution's Anti-Money Laundering (AML) program.
- **A complex web of multiple and disparate regulatory regimes at global, regional, national, and local levels creates additional challenges**. A New York State law can have a major impact on a faraway bank in Asia with a single branch in New York.
- **Critical regulatory changes**, such as shift away from rule based procedural approach to risk based analytic approach, or tighter Ultimate Beneficial Ownership (UBO) identification requirements will **require new strategies in compliance**.

Regulatory scrutiny and technology evolution are exposing critical limitations of AML operations.

Efficient management of the growing scale and complexities in AML will require intelligent automation.

TECHNOLOGY: A BANE AND A BOON IN COMPLIANCE

Rapid evolution of technology is transforming traditional business models in financial services, giving rise to new products, delivery channels, and customer segments. Fintech companies and players from adjacent industries are creating competition as well as partnership opportunities for banks. On the other end of the technology spectrum, new risks are emerging in areas that are still reliant on paper documents, such as in trade finance.

Growing speed, volume, and technological complexities raise the challenges in AML, because banks lack complete information, prior knowledge, and advanced technology to detect evolving criminal behavior. The good news is that recent developments in **artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA) are producing solutions which have the potential to overcome the challenges, and make AML programs more efficient and effective**.

ABOUT THIS RESEARCH

This research is part of Celent's ongoing coverage of emerging technology in compliance. It was commissioned by SAS Institute[1], while Celent kept full editorial control. In addition to Celent's extensive knowledge base, this research benefitted from detailed discussions with compliance professionals from eight banks. This report analyzes the challenges in AML, and highlights how RPA, AI, and ML can help in solving them. A separate report will discuss how banks are approaching AI and RPA adoption in existing operations.

[1] www.sas.com

INCREASING OVERLAP AMONG AML COMPONENTS

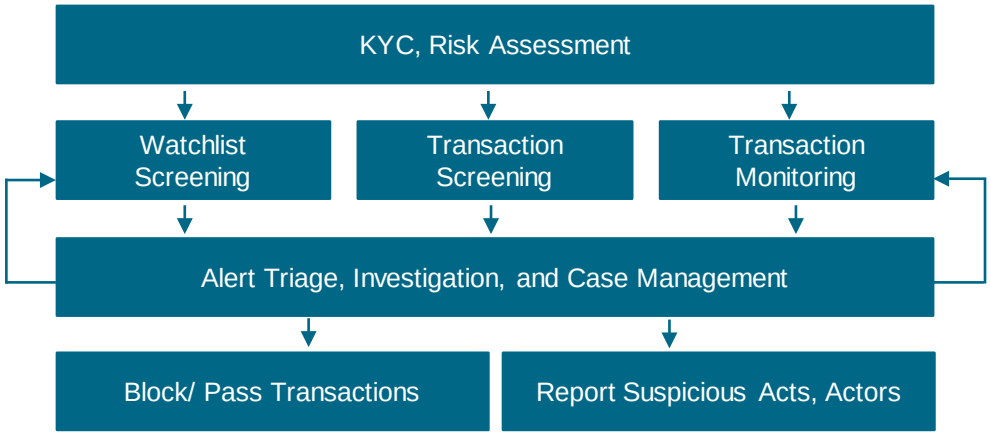
AML operations at financial institutions span across client and transaction lifecycles, and consist of several components as shown in Figure 1.

- In **watchlist screening**, customers are screened against public and private lists during on-boarding, and periodically, to identify suspect entities and their associates.
- In **transaction screening**, payment details are examined to prevent sanctioned or potentially illicit transfers from taking place.
- In **transaction monitoring**, completed transactions are analyzed in detail because money launderers can evade detection during transaction screening.
  - For example, in "transaction structuring" criminals make several smaller transactions below usual detection thresholds, which can only be detected by analyzing aggregated flows, ideally across accounts, channels, and products.
  - Similarly, not all transactions exceeding given thresholds are illicit.
- In **alert triage and case management**, all potentially suspicious activities are investigated, and resolved by sourcing and analyzing additional information.

The **investigation process is highly resource intensive**; it is therefore essential to focus compliance resources on the highest risks areas. Appropriate **risk assessment** during Know Your Customer (KYC) process and on an ongoing basis is therefore a critical component, and **lays the foundation of AML operations**.

Holistic AML analysis requires information and knowledge sharing based upon a *single view of customer* across multiple lines of business.

Figure 1: AML Programs Consist of Different Components



Source: Celent

Traditionally banks have managed the different AML components separately with limited ability for interaction among them. **A truly risk based approach and integrated strategy will necessitate the ability to leverage information and knowledge across AML components and other systems**. For example, transaction monitoring results can be used to update customer risk assessments; similarly, watchlist screening results can be used to risk-prioritize transaction monitoring alerts. Similarly, operational silos along business or geographical lines need to be dismantled for smoother information flow and intelligent analysis.

"We want to add new information in case investigation, such as information from KYC documents, other internal sources, as well as external sources; but getting the data is a challenge." — Tier 1 global bank

INEFFECTIVE USE OF DATA AND TECHNOLOGY IN AML

Efficient management of AML components and their interplay is difficult to achieve due to suboptimal use of data and technology plaguing banks' compliance operations.

FRAGMENTED AND SILOED OPERATIONS CREATE INEFFICIENCIES

Banks have highly fragmented and siloed technology and operational framework, which results from having a wide range of business lines, regional presence, and accretion of systems through organic and inorganic growth. Disparate regulatory regimes in different regions hinder achieving enterprise wide common standards and frameworks, and exacerbate technological inconsistencies and operational fragmentation.

POOR DATA MANAGEMENT LIMITS ANALYTICAL CAPABILITIES

Traditional bank operations and data management processes create challenges for accessing quality data and complete records.

- Data collected using manual processes at KYC on-boarding can **contain incomplete or erroneous records**. **Banks also lack adequate information in critical areas**, such as beneficial ownership, or counterparty information in correspondent banking.
- Banks use customer information file identifiers to create a single view of customer; but the **views may be inconsistent across business lines or subsidiaries**.
- Aggregating customer and transaction records with alert information, building profiles and networks of entities, and analyzing their changes over time are challenging.
- Regulatory expectations on data lineage are rising, and **banks will have to do more to ensure accuracy, consistency, and integrity of data across its lifecycle**.

Data collection and preparation therefore involve additional research, outreach to different divisions, and other manual efforts, **making it a critical source of inefficiency**. Banks often have to undertake major projects to improve data governance.

Current AML operations are mired with poor data management practices, and difficulty in sourcing data creates gaps in coverage.

"Many of our banking clients also have brokerage accounts with us, but because of different systems of records we do not have a holistic view of their activities." — Tier 2 American bank

CURRENT TECHNOLOGY FALLS SHORT OF COMPLIANCE REQUIREMENTS

Technology and models used in AML detection work with simple rules, scenarios, and thresholds. These are based on prior and subjective assessments of risk, and **seldom informed by data on a bank's specific client or business mix**.

- Current AML software predominantly work with structured data, and have **limited capability to analyze multiple and different types of variables**, such as geo-locations, images, or text information.
- Current AML technology is mainly based on relational databases, and are **ill-equipped to support big data analytics**, such as, finding complex patterns and networks in large datasets, or **unstructured data analysis** for analyzing text in payment messages, watchlists, news media, and suspicious activity reports (SARs).
- The **mechanisms for learning** from investigation decisions are inconsistent due to the subjective nature of case resolution.

IMPLICATIONS FOR EFFECTIVENESS AND EFFICIENCY

The technology and data challenges greatly limit effectiveness and efficiency levels of AML programs, as highlighted in Figure 2.

Figure 2: Efficiency and Effectiveness of AML Hampered by Data and Technology Challenges

AML Components	Risk Assessment	Screening	Monitoring	Case Management
Data Challenges	▪ Limited data used for risk classification ▪ Incomplete data to create customer, peer group profiles	▪ Name variations, languages, scripts ▪ Missing information in secondary fields ▪ Poor ownership information	▪ Incomplete counterparty information ▪ Limited variables and time period used in monitoring	▪ Entity resolution, alert correlation difficult due to disparate and fragmented data
Technology Challenges	▪ Difficult to find, quantify risk attributes ▪ Cannot find hidden, unknown segments ▪ Behavior analysis, anomaly detection requires profiles, peer group	▪ Managing numerous and changing lists ▪ Analyzing secondary fields ▪ Analyzing paper documents ▪ Lack of real time support	▪ Generic scenarios and rules ▪ Subjective parameters and thresholds ▪ Cannot find new patterns	▪ Manual sourcing, aggregation of data ▪ Visualization ▪ Manual case filing and reporting ▪ No dynamic feedback and learning
Drag on Efficiency and Effectiveness	▪ Disproportionate alert generation for different segments ▪ Little risk prioritization of alerts	▪ Manual efforts needed to source data from documents, on beneficial owners ▪ Duplicate alerts for multiple list hits	▪ Model tuning difficult, resource intensive, infrequent ▪ Duplicate alerts for same transaction ▪ Cannot find hidden patterns, networks	▪ Recurring alerts ▪ High false positives ▪ Long time to resolve cases ▪ Inability to improve through adaptive learning

Source: Celent

High volume of false positives is the biggest challenge in AML, but they are symptomatic of strategies driven by generalized typologies.

Risk assessment

- **Generic risk segmentation** with subjective and ill-defined thresholds results in skewed alert distribution, and **is a drag on productivity**.
- **Alert prioritization is also based on generic classifications** (e.g., particular list hits or high value transactions bear highest risk), and is not effective.

"Our client segmentation is so broadly defined that 95% of our alerts come from just 5% of our client base. We are rethinking our approach in segmentation."— Tier 1 Asian bank

Screening

- **Managing multiple lists, name variations, secondary fields** (e.g., date of birth), with incomplete and erroneous records are challenges in screening.
- **Foreign language analysis in native scripts, secondary sources for ownership information, news and media scanning** are not well supported in current solutions.

"Our digital channels are witnessing high growth in Asia, and customers there want end of day onboarding if not in real time, but onboarding currently takes days. We need better and faster screening tools with good local language support." — Tier 1 Global bank

Monitoring

- **Rules based systems may not always detect hidden and unknown patterns**, identify behavior nested across undeclared relationships, or group alerts through correlations in underlying alert attributes. The lack of consolidation makes it difficult to see the holistic picture of activity, and firms may miss illicit reportable activity.

- Subjective tuning of rules and parameters generate **high false positives** in transaction monitoring, typically over 90 percent, which includes high share of duplicate alerts on same customer or transactions, and recurring alerts of similar activity that were previously resolved**.**

"Even after statistical modeling our false positive rates are over 80%, we are now thinking of using advanced analytics to manage so many false positives."— Tier 1 European bank

Case Management

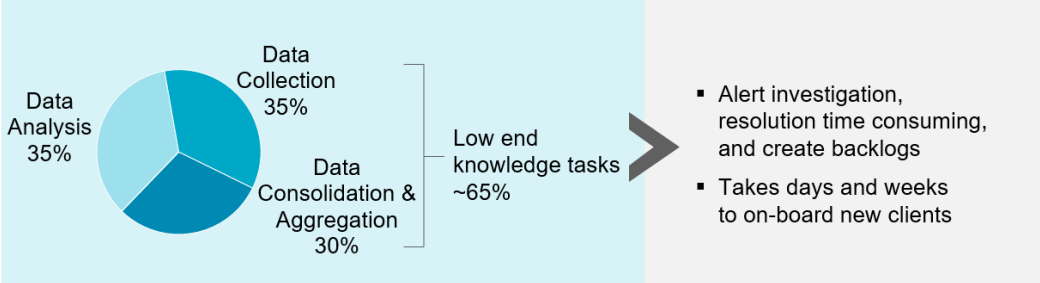
- **Data challenges, and lack of automated workflows and search tools limit ability to conduct entity resolution** leveraging holistic customer and transaction records. It also makes peer analysis, network analysis, and behavior profiling challenging.
- System fragmentation is a barrier to automatically combining, correlating, and enriching alerts. Reporting workflows similarly rely on manual efforts.

Banks have tried to throw more bodies to manage the volume of false positives; the result is exploding costs and high inefficiency

AML Programs are Costly and Inefficient

Banks take a conservative approach to be safe from regulators, and set low thresholds. The result is **high operational cost**, because alert management is resource intensive.

Figure 3: Compliance Analysts' Time is Spent Mostly Doing Low Productivity Work



Source: Celent

- Celent estimates bottom half of banks in developed markets can spend up to US$100 million in their KYC-AML programs annually. **Costs rapidly escalate for larger banks with the largest banks spending close to a billion dollars or more**.
- Similarly, the bottom half of banks have up to 100 people in their compliance teams. **Team size also grows rapidly and can be close to 1,000 people for large banks.** Some banks have even reported to have close to 10,000 compliance staff.
- Most importantly, **both costs and team sizes have grown at a rapid pace**, becoming double or triple in the last five years at many banks, and growing even more rapidly at banks that have received consent orders, or been fined.
- Despite the efforts, **efficiency and productivity levels in compliance is abysmal**, as shown in Figure 3. Close to two-thirds of compliance analysts' time is spent on low level knowledge tasks, and only a third is left for productive investigation.

"Our analysts spend almost 80% of their time on routine and highly tedious work. We are looking to automate many of the tasks to not only improve efficiency, but also make analysts' life easier and raise productivity." — Regional bank in the US

False positives are demonstrably costly. However, false negatives – where AML systems fail to spot actual suspicious cases – may carry higher risk and be hard to quantify. As criminals become smarter, ability to quickly identify new and previously unknown patterns will be paramount in AML. **Advanced analytics such as AI, ML, and RPA offer opportunities for real improvements and efficiency gains in AML operations.**

TRANSFORMING THE RULES IN AML WITH AI

Artificial intelligence is an umbrella term used to describe several analytical techniques which automate manipulation of large and disparate data sets resembling human thinking, and can be improved through feedback. **Robotic process automation** on the other hand **automates collection of data** with less emphasis on analytics. Figure 4 highlights some examples where the new tools can be applied in AML.

Figure 4: AI and RPA Tools Have Numerous Applications in AML

AI Techniques	Feature	Application
 **Link Analysis**	Reveal association among entities, its nature, direction, and strength	Find money laundering networks involving accounts, entities, regions for entity resolution, case investigation
 **Graph Analytics**	Easy visualization of complex patterns, evolution over time, interrogative drill down	Forensic analysis in enhanced due diligence for in-depth investigation; case specific query and drill down
 **Correlation, Regression Analysis**	Analyze relationship among variables; identify critical (and spurious factors) influencing target variable; forecasting	Identify critical and unknown risk attributes and their statistical importance; develop and update risk scoring models
 **Cluster Analysis**	Identify groups, extract group features, spot outliers	Risk assessment and segmentation; create profiles of customers and groups; model expected behavior; spot unusual activity
 **Neural Network, Predictive Analytics**	Identify complex and unknown patterns, including numerous and different types of variables	Find hidden patterns, behavior; behavior analysis; alert prioritization, auto escalation and closing
 **Natural Language Processing and Generation**	Advanced text mining including foreign languages; context based document and media analysis; narrative generation	Name matching; transaction screening; UBO and adverse media analysis; trade finance, regulatory document analysis and classification; SAR generation and analysis
 **Robotic Process Automation**	Automated data fetch; data reconciliation; report filing; local and global search; chatbots	List consolidation; information collection; alert enrichment; reporting; compliance assistants

Source: Celent

Link analysis facilitates **easy discovery of complex networks** involving individuals, entities, jurisdictions by highlighting the nature of relationships (e.g., transaction, ownership), its strength (e.g., transaction volumes, frequency), and other features.

Graph analytics display networks, patterns, and their evolution over time. **Interrogative drill down allows detailed investigation** based on specific nuances of each case.

- Link and graph analyses help in **understanding a specific customer or transaction more holistically** within a larger context of its connections and over time; these are particularly **helpful in entity resolution and case investigation**.

Correlation and regression analyses analyze **extent of dependence among variables**, and are used when there is a general understanding of the dynamics among several variables, but its strength and statistical significance are not well understood.

- These can reveal which attributes are **most important predictors of risk based on a bank's specific business and client portfolio**. Based on this, **new risk scoring or alert prioritization models** can be developed**,** calibrated, and updated regularly.

Cluster analysis **classifies entities in different groups**, and identifies commonalities within a group and differentiating features separating groups.

- Clustering helps find **new groups, or subgroups within subjectively defined groups**, and **new classification approaches**. Identification of common characteristics among group members helps in creating **profiles of peer groups,** which can be used to track **behavioral anomalies** for spotting suspicious activities.

Neural networks and predictive analytics tools can analyze data sets with numerous variables and different types of data (such as name, location, transaction details, counterparties), and **find hidden patterns and trends**.

- These are helpful for **finding hidden patterns and networks, modeling expected behavior, and detecting unusual activity**.
- Predictive capabilities enable machines to generate probabilities or likelihood, and thereby **suggest if alerts are potentially true or false positives, rank them, or recommend next steps** such as auto alert escalation or closing for disposition.

Natural language processing (NLP) is used to **scan and extract context** from documents, free text, internet, deep and dark web, and **classify them based on context and relevance**. **Natural language generation** (NLG) enables **narrative based report generation from given data sets**, and is already in use by media companies.

- The NLP techniques can **enhance name matching algorithms**. It can also be used to **extract information from message fields** to aid payment screening analysis. Context based media and web analyses help in UBO assessment and due diligence.
- Document scanning with NLP can be used for regulatory analysis where machines **identify and recommend changes**, or for analyzing Suspicious Activity Reports (SAR), Currency Transaction Reports (CTR) to identify unknown risks.
- Another use case is NLP application **in trade finance to scan documents**, **classify** them in different categories, and **extract information** for analysis.
- For internal and external reporting, **reports can be generated quickly using NLG**.

Natural language analyses are part of a larger group of unstructured data analysis that can also aid in analysis of images, geo-location, digitized communication, and more.

Robotic Process Automation enables huge improvements in efficiency by automating routine manual tasks. Cognitive capabilities can be added to perform data repair, reconciliation, and context based searches through automated intelligent tools.

- In screening, **lists can be consolidated** using web crawlers. Similarly, **information can be scraped** from internal or external sources to **enrich alerts and cases**.
- Reconciliation of account level data across systems or business lines can help in de-duplication of customer data and **create a single 360-degree view of customers**.
- **Intelligent bots can act as digital assistants** and respond to commonly asked questions (written, oral) with relevant information, documents, and suggestions.

These applications of AI and RPA to AML will **enhance efficiency** by automating manual processes, and **improve effectiveness** by generating superior insights and intelligent visualization. Banks have started dipping their toes into the pool of AI through pilots and proof of concepts, and there is growing interest for wider adoption. A separate report will discuss how banks are approaching AI and RPA adoption in existing operations.

Applying AI, RPA in AML can enhance efficiency through workflow automation, and improve monitoring effectiveness through superior insights and visualization

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 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 management 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

Achieving Holistic AML: Focus on Watchlist Screening
March 2018

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

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

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