PARTNER. ADVISOR. CATALYST.

Global AML Watch List: Technology Attacks False Positives

MAY 2019

Prepared for:

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
INTRODUCTION 4
METHODOLOGY 4
THE WATCH LIST ECOSYSTEM 5
WATCH LIST ALERTING 6
THE THREE-PRONGED APPROACH 10
DATA 10
TECHNOLOGY 11
SOCIALIZATION 13
WATCH LIST: THE NEXT GENERATION 14
ADVANCED TECHNIQUES 15
CONCLUSION 18
ABOUT AITE GROUP 19
AUTHOR INFORMATION 19
CONTACT 19
ABOUT COMPUTER SERVICES INC. 20

LIST OF FIGURES

FIGURE 1: SAMPLING OF RECENT WATCH LIST-RELATED FINES 6
FIGURE 2: WATCH LIST STAKEHOLDERS 7
FIGURE 3: THREE-PRONGED ASSESSMENT APPROACH 10

LIST OF TABLES

TABLE A: STAKEHOLDER IMPACTS 7
TABLE B: WATCH LIST BEST PRACTICES FUNCTIONALITY 11
TABLE C: MARKET TRENDS AND IMPLICATIONS 14

EXECUTIVE SUMMARY

Global AML Watch List: Technology Attacks False Positives, commissioned by Computer Services Inc. (CSI) and produced by Aite Group, presents the current environment for watch list software solutions, market trends, and how technology addresses both. This is an exploration of a path forward for stakeholders and vendors based on advanced capabilities currently available for improving compliance programs in financial services and other industries.

Key takeaways from the study include the following:

- Watch list programs face increasingly complex expectations and challenges as transaction volume grows and the characteristics of financial services change. New data types and sources as well as technology advancements are considerations for all stakeholders.
- For years, legacy technology has generated millions of anti-money laundering (AML) alerts annually across all sectors of financial services, creating ever-increasing pressures on costs and resources. Data management, operating environments, and the pace of change in technology are examples of forces that require monitoring for new options—not just in software but also in software delivery, given the advent of cloud, Software-as-a-Service (SaaS), and other innovations.
- AML leadership can take a three-pronged approach to evaluating watch list functionality needs both now and two to three years out. The approach uses (1) data, (2) technology, and (3) the socialization required to make improvements happen within an organization. This context for examination of watch list needs supports evaluation of vendor solutions.
- Proprietary algorithms are key differentiators, as are transliteration capabilities (an ability to translate between different language scripts) and the software's ability to interpret phonetic differences across languages. Names can be in various scripts (Arabic, Latin, or other) and spelled differently between languages (e.g., John versus Juan), and they can even be spelled entirely differently within a language; watch list software must overcome these variants as well as provide other benefits to increase effectiveness and efficiency.
- While suspicious activity report (SAR) volume is leveling off due to incremental improvements in AML software, regulatory expectations are growing. The number of lists, as well as entries on those lists, is growing, and sanctions continue to add complexity. The good news is that improvements in advanced analytics are occurring in leaps and bounds, helping firms to improve detection and reduce false positives.

INTRODUCTION

AML programs require major investment. Watch list filtering—the comparison of customer data against sanctions lists, sanctions programs, and other data such as politically exposed persons (PEPs) data—is a required and major part of an AML program. There are many considerations for the design, implementation, and maintenance of watch list compliance processes: the size and complexity of the organization and its clientele, the nature of products and services offered, risk characteristics (such as the organization's appetite for risk), internal and external stakeholder expectations, and geographic details. The digitalization and globalization of financial services further increase the challenge of balancing compliance with business goals. The future will require regulated providers to conduct significant examinations to remain compliant and meet the wide variety of stakeholder needs.

Due to the volume and complexity of money laundering, international organizations such as the Financial Action Task Force and The World Bank purposefully do not publish estimates for money laundering. It is a difficult task to research any money laundering-related statistics. However, the United Nations Office on Drugs and Crime (UNODC) has published an estimate that between 2% and 5% of global gross domestic product is laundered annually, which translates to US$800 billion to US$2 trillion per year. That office goes on to say that less than 1% of this is caught, even as businesses around the globe spend tens of billions of dollars annually on technology and staff to combat the problem.[1] Since the events of 9/11 in the U.S., millions of money laundering alerts have been generated, requiring financial institutions and other regulated entities to commit significant resources to AML compliance efforts. Systems and processes are in place to alert, investigate, and resolve potentially suspicious activities, and yet money laundering activities go on undaunted.

Constraints that elevate costs and contribute to the ineffectiveness of efforts to curb money laundering include data factors, technology limitations, internal and external stakeholder expectations, and budget/resource availability. Leaders responsible for AML programs must examine these constraints to find the sweet spot between vendors, software application users, and the interests of all other internal and external stakeholders.

METHODOLOGY

This watch list thought leadership analysis is based on interactions with 19 AML software vendors and interviews with more than 40 watch list software users in the fall of 2018 as well as Aite Group's ongoing conversations with watch list software users and vendors.

1. "UNODC Estimates That Criminals May Have Laundered US$1.6 Trillion in 2009," UNODC, October 15, 2011, accessed May 7, 2019, http://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html.

THE WATCH LIST ECOSYSTEM

Organizations across regulated industries are obligated to screen transactions and customers against sanctions lists, PEP lists, and negative news lists in order to identify high-risk customers and transactions, and to avoid transacting with sanctioned countries, individuals, and entities. Watch list screening software automates the comparison of customer and transactional data to sanctions and PEP lists. Due to the size and complexity of lists and sanctions, very small organizations often use online services for one-off look-ups. Because of the vast amount of customer data, large organizations rely on software automation. Legacy watch list technology has historically generated millions of false positive alerts, which is painful for the firms using it since regulators expect every alert generated to be examined. Organizations are experiencing increasing pressure to add manual and automated resources. The watch list screening process is at the breaking point—the ecosystem must change.

High alert rates in watch list screening are the product of a variety of regulatory expectations:

- Firms must screen new customers during onboarding as well as real-time payment activity, and also perform retroactive screens as new names are added to the various lists, resulting in a large volume of transactions to be compared against these lists.
- Fuzzy logic must be used to account for accidental or deliberate misspellings.
- Many of the sanctioned names appear on multiple lists, sometimes with different spellings.

The recent advent of sectoral sanctions increases the complexity. Specific financial prohibitions against countries such as North Korea and Iran are examples of U.S. and European sanctions. Sectoral sanctions block specified activities with specific companies or sectors of an economy, such as U.S. sanctions against Russian ship-building, defense manufacturers, and certain energy entities. Sanctions, export licensing, and other governmental restrictions can be present in any jurisdiction around the world; organizations must be aware of these legal requirements or face fines and reputational consequences.

Pressure for improvements in watch list software automation also originates from the digitalization and globalization of financial services. Digitalization results from an increasing variety of electronic products and services, and almost any organization can be a global business in today’s virtual economy. Both forces create a need for new techniques in watch list capabilities.

Lists, sanctions programs, and characteristics of the evolving financial services ecosystem are pushing the need for an abundance of caution in screening—caution that contributes to high alert volume. To balance and address both cost and regulatory expectations, the pursuit of effectiveness and efficiency is a must.

Nonbanks need to pay attention as well—now more than ever. At this time, the majority of global regulatory actions are against banks, but that ratio will change as regulators focus attention on nonbank/non-money services business (MSB) verticals: casinos/card clubs, futures and securities companies, insurance companies, housing government-sponsored enterprise

(HSEs), loan or finance companies, and others. Indications are that insurance companies as well as futures and securities companies will lead the way in increased regulatory scrutiny.

Reputations are affected as financial investigative units (FIUs) around the world continue to levy billions of dollars in fines. Just a sampling of watch list-related fines since September 2017 total about US$3 billion (Figure 1); adding all the other AML fines in the same time frame doubles that amount.

Figure 1: Sampling of Recent Watch list-Related Fines

Source: Aite Group

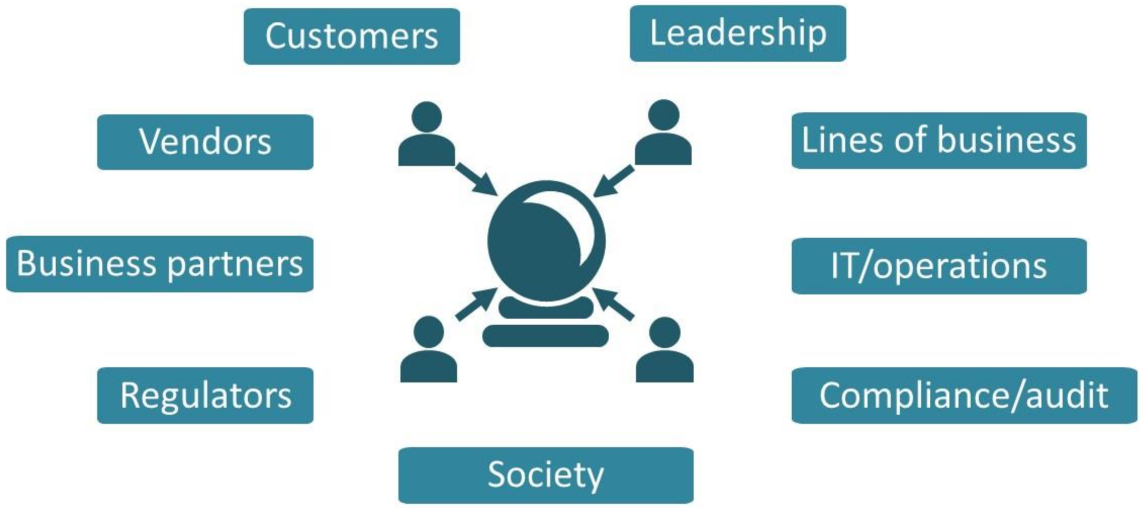
Increased enforcement is coming from multiple levels. FIUs around the world affect multinational organizations, while regional or state FIUs are another level of intranational regulation. The Financial Action Task Force's (FATF's) recommendations for PEPs, counterterrorism, proliferation of weapons of mass destruction, and beneficial ownership are added factors pressuring users to keep watch list capabilities as effective as possible.

As a result of the ongoing regulatory pressures, providers are throwing bodies and other resources at the problem, driving compliance costs upward.

WATCH LIST ALERTING

More data and data types contribute to the continuously increasing watch list alert volume. Addressing this ongoing growth and increased complexity requires new data management techniques and software capabilities. Stakeholders have differing needs: internal stakeholders expect compliance along with support for the organization's risk policies, while external stakeholders (i.e., the firm's customers) expect a good customer experience and identification of potential risks (Figure 2).

Figure 2: Watch List Stakeholders



Source: Aite Group

Each stakeholder experiences specific impacts and has particular concerns; Table A lists some of the characteristics of those impacts.

Table A: Stakeholder Impacts

Type	Definition
Board of directors/ owners	The ultimate responsibility for regulatory compliance is establishing watch list policies and then monitoring for adherence. Failure can result in fines, reputational impacts, and in some cases, personal legal action against members.
Executive leadership	The C-suite has responsibility for the execution of the organization's policies and processes. Despite any delegation of responsibility, this level of leadership must understand and act on watch list compliance.
Line-of-business management	Line-of-business managers must buy into and support the policies, processes, and procedures needed for meeting regulatory requirements. Updating the compliance team should occur any time there are changes, such as new products, markets, or processes. The business partner should be proactive and aid in assuring compliance.
IT and operations	This group is a critical part of the team needed to meet watch list compliance requirements. IT partners manage the environment needed for software automation. Operations often owns at least some of the compliance processes, which can occur in many ways: branch support, customer service (such as onboarding tasks), and interfacing with IT, business units, and compliance.
Compliance/ audit	Compliance owns the watch list program and audit monitors for adherence. Failure in either area can lead directly to fines and activity restrictions against the organization by regulators. A Bank Secrecy Act (BSA) officer (in the U.S.) or appointed officer of the organization must take ownership of the AML program; the individual is responsible for overseeing all aspects of compliance, which includes the filing of SARs.

Type	Definition
Society	There are many impacts to society when AML programs fail: undetected criminal activity, decreased confidence in the financial system, economic disenfranchisement, lack of access to global financial systems due to limitations on the provision of services, and costs associated with setting up and maintaining a regulatory framework.
Regulators	A regulatory framework is difficult and expensive to maintain. Capabilities constantly need updating, which requires balancing fairness with the solemn need to protect the financial services ecosystem. While regulators are often seen as the opposition, their role is as important as it is complex to perform.
Business partners and vendors	Financial services organizations have many business partners and are often in complex relationships. Anything that impacts the profitability or operational capabilities of the financial services provider affects the many vendors and business partners doing business with, or in any way interacting with, the financial organization.
Customers	The people and organizations served by financial services providers expect competent provision of products and services. Not detecting criminal activity, issues with processes, and other negative impacts will cause customers to reconsider or change the relationship with the financial services provider.

Source: Aite Group

Constraints affecting stakeholders include the following:

- Budgets and organizational resources
- Personnel burnout, high turnover, and increased hiring/training costs
- The need to minimize customer friction
- Regulators' expectation of effective watch list programs
- Thorough documentation, effectiveness, and users' ability to demonstrate an understanding of how watch list automation works and why

Sanctions and sectoral sanctions require specific focus to obtain and maintain lists and related data for use in a watch list solution. Sanctions programs can change without notice, and sectoral sanctions require an understanding of the program and its effects on customer data.

The six-to-18-month window for allocation of IT and operational resources adds to the complexity of watch list program planning, which itself has a time frame of one to three years. Also, forecasting new technology is difficult, and automation options can change significantly within a planning period. The ability to successfully forecast needs for watch list software requires thought leadership across many disciplines and several areas of the organization.

A team of watch list program collaborators is also needed to understand and meet compliance data needs. As software solutions are becoming more effective, data requirements are changing, and vice versa. New data expectations constrain as well as enable watch list functionality. Data availability, the increasing number of data sources, new data formats, and other factors require increasing expertise from the team that supports watch list efforts.

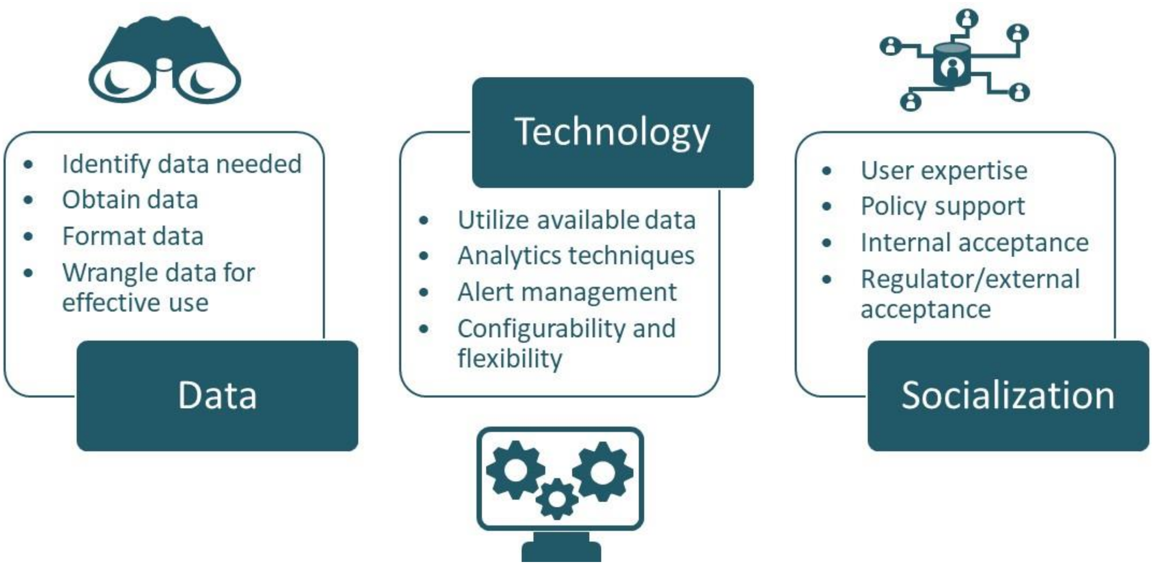
There are also many new or growing types of options affecting the watch list ecosystem: SaaS options, ID validation technologies to support Know Your Customer (KYC) in watch list investigations, outsourcing services, and cloud technology. New expertise is needed to anticipate, analyze, implement, and use these new processing/operating tools and environments.

The pace of change in watch list programs continues to increase. Technology is no longer the real constraint; the real limitation tends to be learning how to benefit from technology and not be constrained by it.

THE THREE-PRONGED APPROACH

Given just the volume of data in watch lists, manual information comparison is impossible, making software automation essential in any regulated organization. In smaller shops, one-off searches using a third-party service can suffice, but organizations of any larger size require automation. The three-pronged approach presented below—data, technology, and socialization—provides a useful conceptual framework for understanding, analyzing, and evaluating automation needs (Figure 3).

Figure 3: Three-Pronged Assessment Approach



Source: Aite Group

DATA

Advanced software capabilities require more and varying types of data. In addition to identifying the basic data needed for watch list automation purposes, organizations now have the opportunity to obtain data from many more sources, and those sources vary greatly both in terms of legacy data types and the wide variety of types becoming available today.

Formatting data takes on new meaning in advanced software systems. For instance, because of the new variety of data types and sources, data preparation and management technologies have evolved. To effectively use data in advanced analytics and new automation techniques, the search for and use of data has a whole new set of requirements and expectations.

TECHNOLOGY

Technologies available to maximize the new data discipline include both preprocessing and new analytics techniques. For better alert management, and to obtain other benefits, new capabilities in watch list software include alert scoring mechanisms and proprietary string approximation techniques that enhance text searches. Because of advanced computer hardware and processes, and more memory and storage than ever before, algorithms can now provide more and better user options. This technology also provides the user with an ability to configure the system so that output can be refined, adapted, and improved.

Technology often has a lot of hype around it. Compliance stakeholders must be able to discern what will work best, what is necessary, and what will be acceptable to regulators. New watch list automation techniques are available to increase effectiveness, improve efficiency, aid in documenting all activities, and make better use of existing and new data (Table B).

Table B: Watch List Best Practices Functionality

Function	Description	Capabilities	Benefits
User management	Establishment and configuration of all user roles/functions	Ability to add/modify roles for rights and privileges, and to manage users	With enough flexibility, the vendor is not needed for changes, user controls, or ongoing user maintenance
Notification management	Alerting controls, notification, and rule and parameter settings	Building and configuring how alerts are generated	Users, groups, and divisions will receive alerts based on client preferences; search parameters and scoring are user managed
System activity monitoring	Application performance	Dashboard, user activities, and system controls	Management reporting, key performance indicators (KPI), system utilization, and other management metrics
Alert settings/ configuration	Abilities to control functionality and processes	Configuration for results, workflows, reviews, and lists	Controls for primary user needs: functionality for searches, match scoring, item reviews, and review presentment/controls
Data management	Input/output controls	Batch and real-time settings, entity details, and lists	Provides for operational processes and screen content for alerts, system status, and reports
Analytics techniques	Filtering sensitivity and related settings	Configurations for screening: methods, scenarios, files, real-time actions, and data considerations	Basic capabilities affect how and when alerts are generated, more advanced capabilities address alert management and techniques for alert scoring; also establishes thresholds, notification conditions, and other outputs

Source: Aite Group

While there are many basic features of any watch list software, key differentiators should be sought to choose the better system and vendor. For example, providing the user with as much or as little control of the system as desired is a way to tailor software to the environment and meet compliance program needs.

Another key differentiator for a vendor solution is in the results—system output in terms of alert quality and quantity. Regulators must feel comfortable that the watch list screening software is working well, which creates a challenge when a user attempts to drive down alert volume. However, regulators and examiners are noticing vendor successes and are becoming more comfortable accepting fewer alerts or automated handling of alerts. In fact, U.S. regulators recently took the extraordinary step of issuing a joint statement on innovative efforts to combat money laundering and terrorist financing that expressly encouraged the adoption of new techniques to improve watch list screening and other AML processes.[2]

There are many ways to increase watch list system efficiency and effectiveness. Some of the more acceptable methods from an examiner's perspective are those that focus on highly explainable techniques. Proprietary algorithms, scoring outputs, and match suppression are examples of improvements that must be explainable to the regulator.

Proprietary algorithms can focus on improving matching using a variety of techniques. In one example, new underlying mathematics are used to obtain significant benefits when analyzing traditional data steps such as tokenization and distance scoring. Improvement can be found through other approximation techniques as well as contextual logic branches for specific pattern matching and transliteration.

Improved watch list screening software will include both proprietary and nonproprietary alert-handling techniques. Advanced computational approaches enable users to set sensitivity levels for matching as well as set thresholds for alert optimization, which even includes alert suppression.

Given the millions of transactions and other activities to be monitored, even a 1% hit rate is overwhelming, and that has been the case for years. Now targets are set for a 0.1% to 0.2% hit rate, but even then, the probability of a true hit is less than 0.001%, making watch list screening one of the most onerous compliance tasks an organization must manage. Expectations demand improvement, and better technology is the only way to obtain that improvement.

2. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, December 3, 2018, accessed April 4, 2019, https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

SOCIALIZATION

The third prong for obtaining watch list technology improvement has a great deal to do with transparency, or users' understanding of and knowledge about the technology to assure stakeholder acceptance. An organization's board of directors or executive management must be certain that the technology supports policies and risk appetite. Lines of business depend not only on system accuracy but also technology that does not create undo customer friction and delayed revenue. IT and operations partners must be able to support the software; to meet compliance goals, this group of partners must agree on the business and technical requirements as well as how to execute. And compliance, as the primary owner of the automation, must document decisions, provide audit trails, and demonstrate to all stakeholders that the system is performing as agreed and meeting expectations.

WATCH LIST: THE NEXT GENERATION

Market trends driving the need and demand for next-generation capabilities stem from four areas of the AML landscape (Table C). Increasing payment volume and new payment types necessitate developments in data related to payments. The need to stop real-time payments in flight is a daunting one that needs both data integration and availability, combined with integration among other systems. Rising regulator expectations increase watch list complexities and number. And the constant changes in typologies (i.e., criminal threats) drive the need for more sophisticated and highly adaptable systems. Watch list stakeholders must be aware of improvements in software automation to continuously meet these needs.

Table C: Market Trends and Implications

Market Trend	Implication
Increasing payment volume and new payment types	Alert volume is being driven by changes in financial services product offerings and the need for real-time payment interdiction.
Rising regulatory expectations	Ongoing changes in compliance expectations are multiplying the vectors of analysis and increasing the workload in financial services; this is especially affecting the six categories of organizations that are not financial institutions (FIs) or MSBs: casinos/card clubs, futures and securities companies, insurance companies, government HSEs, loan or finance companies, and others.
Escalating threat environment	Criminals are leveraging sophisticated technologies and automation to perpetrate money laundering, pushing vendors and users to develop and implement even better solutions to fight crime.
Advances in technology helping to improve efficiency and detection	Criminal sophistication, regulatory change, and challenges from startup firms—regtech firms—require evolved software solutions to increase efficiency, provide better detection, and improve alert workflows and other functions.

Source: Aite Group

Interviews of more than 50 vendors and AML executives at financial firms provide insight into the top three improvements sought by financial services providers to meet their evolving needs:

- Improved analytics to reduce false positives, including matching techniques and software that automates alert management
- User-controlled configuration of rules, settings, thresholds, and workflows, which also includes sensitivity settings, alert prioritization, and workflow controls to improve watch list program effectiveness and efficiency
- Sandbox functionality (i.e., an integrated test environment with associated tools to provide an ability to immediately see the impacts of proposed changes)

The threat of enforcement is still a strong motivator in AML compliance; as a result, compliance managers have increased support in efforts to advocate for change. Keeping up with improvements in automation is critical to avoiding compliance issues. While watch list capabilities are improving, the best solutions are those that not only perform better but are also able to integrate within the user environment more easily and effectively. The ability to make a business case in compliance is becoming easier due to continuously increasing regulatory pressures and complexities as well as the ability of newer technologies to reduce compliance costs while improving overall program effectiveness.

ADVANCED TECHNIQUES

Hyperbole about technology benefits is everywhere. Artificial intelligence (AI) is a bucket term used to reference three technology approaches: machine learning (ML), natural language processing (NLP), and robotic process automation (RPA).[3] Each has distinct purposes and expected benefits. While many vendors and users talk about AI, the greatest practicality for watch list can be found in improved text matching and alert scoring. However, each of the three techniques provides unique potential that should be understood and weighed as the next generation of watch list solutions evolves.

MACHINE LEARNING

The use of ML analytics for AML is gradually gaining traction in financial services. The volume of payments and the burden of regulatory expectations are growing too quickly for the legacy approaches that rely on rules and scenarios to be effective. In addition, the volume and breadth of data available for analysis is expanding as FIs build massive data lakes fed by cross-product and cross-channel data.

ML provides benefits in alert management, especially when outcomes are made available to the software so that its output can be improved. The system can suppress, disposition, and score alerts to prioritize workflow. Alert review can be set based on user choices; an alert could be dispositioned by the software or scored/prioritized for investigator review. Other examples of benefits from ML include an ability to improve matching on specific data and to suppress alerts based on predefined user criteria or previous outcomes.

Many people think ML is synonymous with unsupervised learning, but that is not the case. There are a few ways in which analytics models are trained:

- **Supervised learning:** Supervised models are created using labeled training data, i.e., data that has been specifically identified as fraudulent or good transactions. This approach is ideal to use when a good amount of historical data is available to train the analytics. As a result, supervised models typically have lower false positive rates than do unsupervised ones.
- **Unsupervised learning:** Unsupervised models do not have the benefit of the labeled training data and are useful when the organization doesn't have a lot of history to use for modeling (e.g., with new payment methods, such as faster payments). The

3. Note that most applications of RPA do not have cognitive capabilities; however, in the context presented, RPA is included in the bucket term "AI" regardless of this distinction.

answers are not known in advance, so the system is learning to detect outliers based on their similarity to prior transactions. Unsupervised models are more prone to false positives, since a portion of good customers will inevitably have outlier characteristics.

- **Semisupervised learning:** Semisupervised learning falls somewhere in between. It leverages both labeled and unlabeled training data to inform the models, and, as is to be expected, the false positives rate also tends to fall somewhere in between.

Unsupervised and semisupervised techniques are often the best suited to AML, since AML departments don't always have the benefit of a high volume of known outcomes that their fraud counterparts enjoy. Once an SAR is filed, there is usually little to no feedback loop about the final disposition. However, regulators' expectations around model governance can make it challenging for FIs to use unsupervised analytics, since it can be difficult to clearly document and explain outcomes. In addition, with more efficient and effective analytics, an FI will begin filing fewer SARs. Unfortunately, regulators often use the number of SARs filed by an FI as a metric for evaluating compliance, so a dramatic reduction in SARs can result in a difficult conversation at the next regulatory exam.

That said, some individuals at regulators, such as FinCEN's new director Ken Blanco, have been vocal in public forums that they recognize the need for the AML function to use more advanced technologies, especially as organized crime rings are using these same technologies to perpetrate criminal acts. Some regulators have brought data science experts onto regulatory exam teams so they can better understand how these technologies are being used, signaling a continued warming to the use of advanced analytics for AML detection.

NATURAL LANGUAGE PROCESSING

Not to be confused with transliteration or phonetic heuristics, NLP converts text or speech into structured data that can then be read by software. Transliteration is the conversion of text from one script to another that involves swapping letters in predictable ways (e.g., Latin to Cyrillic); an example of phonetic heuristics is a proprietary algorithm that substitutes numeric values for letters (to perform analysis). For AML, NLP can be used for automated summarization, language translation, keyword tagging, real-time social media analysis, and grammar analysis. NLP, transliteration, and language heuristics are all potential tools for watch list text matching processes, each with its own uses and benefits.

Natural language generation is essentially the converse of NLP. In this case, the machine converts structured data into narrative text. Natural language generation can thus assist investigators in filling out SARs. It enables compliance teams to identify the most relevant and important information that can otherwise be hidden in structured data and then produces human language narratives inclusive of data context and explanations. The typical SAR has five components, and while the first four fields can be auto-populated by many case management systems, the most important part of the SAR, the case narrative, cannot be prefilled. Using NLG, the SAR narrative can be automatically generated, while communicating the key "who, what, when, and where" aspects of the suspicious activity. Rather than spending 20 to 30 minutes composing the SAR narrative from scratch, the investigator can instead spend just five to 10 minutes reviewing and tweaking the auto-generated narrative.

ROBOTIC PROCESS AUTOMATION

RPA is the software equivalent of an assembly-line robot. It can significantly reduce the time an analyst has to spend on routine tasks, such as these:

- Gathering information to work an alert or perform an investigation
- Sending requests for information internally or externally
- Processing trigger-based events such as information searches regarding ultimate beneficial ownership

Computer processing “bots” are often created with simple process configuration tools on existing technology to robotically automate repetitive and manual human tasks. It may incorporate ML techniques. RPA technology performs well in people-intensive operations, scenarios with a high volume of transactions, and repetitive tasks. For example, bots easily cut and paste name and address data to multiple systems, gather client and portfolio information from myriad sources, escalate client complaints, and enable routing of work through complex hierarchies.

RPA is the technology in use for chatbots through text or voice recognition. It can function in a fully automated mode (unattended), initiated by a human (attended), and in tandem with a human (hybrid mode).

This technology is scaling up over the next few years and will become prevalent. It works with application programming interfaces and generally costs less than business process management tools. RPA can significantly decrease the amount of time needed to work watch list hits and decrease the amount of time a payment is held in a work queue for human review.

CONCLUSION

Turn compliance into competition.

- An understanding of the latest compliance technologies is important for supporting compliance program effectiveness, improving financial reporting efficiency measures.
- Whether defined as ML, NLP, RPA, or other components, AI is here, and peers that have taken the step up will enjoy better profitability and examinations, which makes upgrading a competitive factor. It's not just about compliance anymore.

Get informed.

- Talk to vendors to keep abreast of new capabilities.
- Advancements are occurring at an increasing pace; knowing when a technology change should be made requires continuous monitoring of the compliance program ecosystem.

Bring regulators on the journey.

- Many regulators are making a concerted effort to educate themselves on new technologies; as new technologies are engaged, keep an open line of communication with regulators.
- Be sure to make transparency part of any change process; document scenarios and be sure to understand how technology works and why.

Don't wait.

- Before increasing investment in personnel, look to automation to contain costs. In the process, employee satisfaction can rise as the mountains of alerts to review reduce to just the more interesting or real investigations.
- The watch list compliance function is at a breaking point for regulated organizations across industries; faced with mounting and increasingly complex regulation, rising costs, and diminishing gains, AML practitioners by necessity must embrace advanced technologies.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Tony Kaus
+1.617.398.5057
tkaus@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT COMPUTER SERVICES INC.

CSI is a full-service financial technology and regulatory compliance provider serving customers nationwide. Headquartered in Paducah, Kentucky, we not only provide innovative solutions for financial institutions, we also serve the regulatory compliance needs for a variety of industries.

Offering dynamic technology solutions, from core banking systems and IT managed services to OFAC compliance software, we're one of the nation's largest fintech and regtech providers. And with more than 1,100 employees, our staff is here to help your business be competitive, compliant, and profitable.

For more information contact us at getresults@csiweb.com.