INTELLIGENT AUTOMATION AND ADVANCED ANALYTICS
To Power Financial Crime Compliance
Financial crime poses significant challenge to financial institutions globally, in the form of monetary loss, reputational damage, customer loss and regulatory fines.

To combat the challenges posed by financial crime, institutions around the world are making huge investments in people, systems and processes. Various reports estimate that the cost of AML compliance was more than $110 billion in 2018 across financial institutions in U.S., Europe and Asia Pacific.

While this investment has yielded results and has helped address regulatory challenges, it is imperative for financial institutions to now focus on leveraging new age technologies such as artificial intelligence (AI) and cognitive automation and to adopt a more risk-based approach to drive greater efficiencies and effectiveness in their Financial Crime Compliance (FCC) function. The use of the appropriate technology solution can help institutions reduce manual and duplicative processes, shift staff from low-value transactional activities to areas requiring judgment, and introduce a more innovative risk-based approach in their financial crime operations.

Financial institutions around the globe have already started ramping up the use of intelligent automation and advanced analytics to make the FCC processes more efficient, focusing on reducing risks as well as the overall cost of compliance. While the results have been mixed, one of the large global banks has enhanced its Know Your Customer (KYC) process by leveraging a combination of machine learning (ML), natural language processing (NLP), intelligent automation and advanced analytics technologies and capabilities. This has resulted in an 80% decrease in onboarding time for a commercial client (from 41 days to 8 days), while another large global bank has witnessed a 20% drop in alert volumes without any change in its risk appetite. Recently, U.S. regulators issued a statement encouraging financial institutions to use innovative approaches such as AI to combat money laundering. This provides the much-needed impetus to the industry to leverage new technologies in FCC.
To combat the challenges posed by financial crime, institutions around the world are making huge investments in people, systems and processes. Various reports estimate that the cost of AML compliance was more than $110 billion in 2018 across financial institutions in U.S., Europe and Asia Pacific.


Intelligent Automation and Advanced Analytics in FCC

Intelligent automation and advanced analytics show tremendous potential to transform the FCC process by enhancing the quality of investigations, reducing false positives and operating costs, and by making the process more efficient. We are seeing more and more client use cases leveraging these technologies across the following FCC areas:

- KYC onboarding and refresh
- Sanctions and transaction monitoring detection
- Sanctions and transaction monitoring investigation

As outlined in Figure 1, technologies like ML, NLP, natural language generation (NLG), entity resolution, graph analysis, and network analysis can derive new relationships from data, detect unknown patterns, understand sentiments and generate coherent context that make them ideal for FCC process transformation.

These powerful technologies can be implemented across the FCC process to drive greater efficiencies and enhance effectiveness.
### FINANCIAL CRIME COMPLIANCE TRANSFORMATION

<table>
<thead>
<tr>
<th>KYC Onboarding and Refresh</th>
<th>Sanctions and transaction monitoring investigation</th>
<th>Sanctions and transaction monitoring detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>• NLP</td>
<td>• Entity resolution</td>
<td>• ML models (e.g., Random Forest, Support Vector Machine)</td>
</tr>
<tr>
<td>• Coreference resolution</td>
<td>• Network graph analysis</td>
<td>• Coreference resolution</td>
</tr>
<tr>
<td>• Agglomerative hierarchical clustering</td>
<td>• NLG</td>
<td></td>
</tr>
<tr>
<td>• Bayesian network and dynamic graphical modeling</td>
<td>• Bayesian network</td>
<td></td>
</tr>
<tr>
<td>• Optical character recognition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Benefits for KYC onboarding and refresh
- Reduced operating cost
- Faster onboarding times
- Improved efficiency

#### Benefits for sanctions and transaction monitoring investigation
- Reduction in overall investigation times and operating cost
- Enhanced investigation quality
- Improved regulatory reporting (e.g., Suspicious Activity Reports (SARs), Sanctions reporting, etc.)

#### Benefits for sanctions and transaction monitoring detection
- Reduced number of false positive alerts
- Enhanced investigation quality
- Increased staffing capacity

Source: Accenture, August 2019
Intelligent KYC Processes

The key steps in a typical KYC process include capturing customer data, enriching the data, performing due diligence, and making decisions on next steps.

After onboarding, financial institutions generally complete a periodic review, depending on the risk rating of the customer and, where required, an investigation of the account. Intelligent automation and advanced analytics can help introduce operational efficiencies at each step of the process. This allows onboarded customers to stay within the financial institution’s stated risk appetite levels and remain compliant with regulations. We see significant potential to use the technologies outlined in Figure 1 in conducting ongoing periodic reviews and customer refresh activities (see Figure 2 below).

These intelligent technologies also play an important role in the following KYC activities:

**CUSTOMER ONBOARDING**

In straight-through processing to capture and enrich data, the integration of Customer Relationship Management (CRM) and Customer Lifecycle Management (CLM) systems can create operational efficiencies by streamlining KYC case creation followed by data enrichment.

---

**Figure 2. KYC Process Overview**

<table>
<thead>
<tr>
<th>Capture</th>
<th>Enrich</th>
<th>Due Diligence</th>
<th>Periodic Review/Customer Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Client self-service&lt;br&gt;• Digital onboarding, approvals and notifications&lt;br&gt;• Sales system integration&lt;br&gt;• Data validation&lt;br&gt;• All requests—products, services, multiple regions&lt;br&gt;• Bulk onboarding of intermediary clients</td>
<td>• Automated routing to sales assistants and middle office&lt;br&gt;• Data/document collection rules and requirements&lt;br&gt;• Retrieve third-party data&lt;br&gt;• Situational rules by booking entity, line of business, products driving the appropriate data enrichment rules at the opportune time</td>
<td>• Dynamic and situational KYC and Customer Due Diligence (CDD), regulatory rules by product, line of business, geography&lt;br&gt;• Re-use of due diligence globally, with the ability to segregate based on privacy rules&lt;br&gt;• Manage regulatory rule changes within the system</td>
<td>• Periodic screening of high risk customers&lt;br&gt;• Review of risk rating&lt;br&gt;• Verification of customer’s updated jurisdiction</td>
</tr>
</tbody>
</table>

Source: Accenture, August 2019
A key element in the enrichment of data is having a central and unified data pooling capability accessed through straight-through processing between internal and external data sources. This allows high speed processing and data annotation that permit data-driven context sensitivity. And, depending on the category of customers, ML algorithms can help identify information for which outreach is mandatory. An attribute matching algorithm is used to compare details in the KYC profile with the information extracted from the Identification and Verification documents submitted.

CUSTOMER RISK RATING ANALYSIS

By using NLP techniques such as named entity recognition for due diligence, teams can identify the screening entity, while coreference resolution can be used to confirm that the entity is being properly referred to in the assigned areas. Relationship extraction can be used to establish links between different entities, and semantic role labeling to tag suspects. Sentiment analysis can be used to identify negative news and exposure to external risks of financial crime by using screening macros to read, analyze and summarize unstructured customer information from news websites/online databases such as Regulatory DataCorp, Inc. (RDC) and Lexis Nexis Group Inc.

ML FOR PERIODIC REVIEW AND INVESTIGATION

ML models can help understand customer behavior on an ongoing basis and use clustering techniques such as Agglomerative Hierarchical Clustering to group customers with similar risk profiles and automatically update their risk ratings accordingly. Screening macros can be used to read watch lists and actively screen customers. Bayesian networks and dynamic graphical models can be used to unearth opaque and previously unknown connections between entities or transactions and their remote linkages with suspect actors, money launderers and politically exposed persons (PEPs), and prohibited states, among others.

TEXT MINING FOR CUSTOMER REFRESH

Another key area of interest in the customer refresh process, in addition to the risk rating review, is to identify if the customer’s jurisdiction has changed since the last review. This requires enhanced due diligence on the part of the financial institution to validate if the jurisdiction has in fact changed. Techniques like text mining can be used to search through various data bases and data sources—both internal and external to identify a customer’s current jurisdiction.

The KYC process entails large investments in systems, data maintenance, as well as human resources required for the data entry, due diligence, risk rating analysis and customer onboarding. The use of Intelligent KYC creates efficiencies by enhancing the process and improving the quality of investigations through reduced human errors, as well as reducing the number of analysts required to conduct investigations.

Our experience indicates that onboarding costs as well as turnaround time can be reduced significantly with the use of these technologies, especially for corporate accounts, given the large number of documents that are reviewed manually.
Effective Sanctions Screening and Suspicious Activity Detection

The FCC process begins with the screening of customers—identifying whether an individual or corporate entity is part of a sanctions list or is a PEP, or if there is some negative news concerning the entity.

Financial institutions tend to use various string-matching techniques such as fuzzy logic in their screening applications.

Moreover, institutions continuously monitor customers’ transactions based on various typologies that give an indication of whether or not a specific customer’s activity is suspicious. A major challenge we have observed in conducting transaction monitoring is the effective detection of suspicious activity, with institutions having more than 95% of alerts turning out to be false positives. In the case of banks, many use fixed rules-based typologies that limit their ability to detect emerging money laundering patterns.

Various NLP and ML algorithms show tremendous scope in enhancing the screening and alert generation process. These include:

**NLP FOR SANCTIONS SCREENING**

Effective customer screening at the start facilitates subsequent steps in the investigation effort and positions financial institutions for greater effectiveness. Various techniques can be used to enhance the screening process, such as information extraction using NLP algorithms like named entity recognition to identify the alerted entity, coreference resolution to confirm that the same entity is being referred to in various places, relationship extraction to establish links with other entities, and semantic role labeling to tag suspects.

**ML FOR SUSPICIOUS ACTIVITY DETECTION**

The use of intelligent automation technologies such as supervised and unsupervised ML models can help better identify emerging money laundering patterns and thus provide a better view of what is a suspicious activity and what is not.

Figure 3 illustrates how a “Risk Prioritization” approach that leverages advanced ML models can be used to efficiently detect suspicious activity. Alerts generated using various scenarios are fed into ML models such as Random Forest and Support Vector Machine. The models then aggregate the alerts based on certain parameters such as country of origin, beneficiary’s name, geography, type of account and then assign them a risk score, which can then be used to prioritize the investigation.
AUTOCLOSURE AND HIBERNATION OF ALERTS

Certain low risk rated alerts can be automatically closed after an initial review period. This helps validate if the alerts are false positive. Low to medium risk-rated alerts can also be hibernated for future review. And if a customer’s activity triggers an alert within a certain period, these hibernated alerts are then categorized as high risk. These supervised ML models also permit dynamic fine tuning of scenarios by providing continuous feedback on which alerts were false positives and what could be a better threshold.

Using advanced ML models for alert detection can significantly reduce the number of false positives. With the use of efficient algorithms, we have seen financial institutions significantly reduce the number of false positives, in some cases by over 90%. Fewer alerts allow investigators to direct their focus and attention to more complex alerts, thus enhancing the overall quality of investigations. A smaller number of alerts can free up precious resources that can be redeployed to other critical areas within the organization.

Figure 3. Suspicious Activity Detection using Risk Prioritization Approach and Advanced ML Models (Illustrative)

<table>
<thead>
<tr>
<th>SCENARIOS</th>
<th>ALERTS</th>
<th>ML MODELS</th>
<th>MODEL OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Movement of Funds</td>
<td><img src="image1" alt="Alert" /></td>
<td>SUPPORT VECTOR MACHINE</td>
<td>SUGGESTION</td>
</tr>
<tr>
<td>High Risk Geography</td>
<td><img src="image2" alt="Alert" /></td>
<td>DECISION TREE</td>
<td>Investigate</td>
</tr>
<tr>
<td>Potential Cash Structuring</td>
<td><img src="image3" alt="Alert" /></td>
<td>SUPPORT VECTOR MACHINE</td>
<td>Hibernate</td>
</tr>
<tr>
<td>Avoidance of Reporting Threshold</td>
<td><img src="image4" alt="Alert" /></td>
<td>RANDOM FOREST</td>
<td>Autoclosure</td>
</tr>
</tbody>
</table>

Fine-tuned scenarios are executed. Alerts are generated based on the scenarios. Various modeling techniques are used, e.g. Decision Tree, Logistic Regression, Random Forest, Support Vector Machine, to analyze these alerts and assign them a risk rating. Each and every alert/case is given a risk score using ML techniques and cases with the highest score are prioritized for investigation. Low risk alerts can be autoclosed, medium risk can be hibernated while high risk alerts are sent for investigation.

Source: Accenture, August 2019
**Efficient Alert Investigations**

The traditional alert investigation/transaction monitoring process involves an initial review to discount false positive alerts, and, if required, this is followed by a detailed review of the customer and related entities.

The case is referred for additional review in case of suspicion wherein a SAR is filed with the regulator.

Figure 4 offers a view of how and where intelligent automation and advanced analytics can be leveraged in the process of alert investigations to discount false positives early on and detect hitherto unknown transaction patterns through which money laundering might be taking place.

The following identifies how automation and technology can enhance and drive efficiencies in the alert investigation and monitoring process:

1. **STRAIGHT-THROUGH DATA PROCESSING FOR CASE CREATION**

   Analysts today spend a significant amount of their time gathering, organizing and reviewing information from multiple systems, rather than focusing on core activities like risk mitigation. Straight-through processing of data between multiple internal systems (such as KYC, Core Banking and others) can simplify the process of data capture for case creation. The data gathered can be categorized and presented in a visual format (for example, by identifying outlier transactions) and in an automated manner to aid the investigation process. Models can also be leveraged to analyze the captured data (customer, transaction, KYC), assess the riskiness of the transaction and to speed up analyst review while improving escalation efficiency.

2. **NLP FOR SUPPLEMENTING AND ANALYZING EXTERNAL DATA (MEDIA SCREENING)**

   As discussed in the Sanctions screening section, several NLP techniques such as named entity recognition, coreference resolution, relationship extraction and semantic role labeling can be used to identify alerted entity and tag suspects. In addition to this, intelligent systems leverage pattern mining, theme mining to interpret data across transaction activity, customer onboarding, enhanced due diligence, previous alert and/or case resolution, external negative media and information services. While tools like World-Check®, Factiva, Inc. can be used to identify patterns that are new and fed into the models. This information can help the investigator make a better decision without the need to spend time on searching information on the alerted and related entities. There are many tools and solutions (such as the Labyrinth platform by Ripjar Limited) that can be easily integrated with financial institutions’ systems. These can help significantly reduce the time and effort required to scale up this capability.

3. **ML FOR DECISION MAKING**

   While the final decision would involve human judgment, ML algorithms such as a Bayesian network can review the triggered activity to automate aspects of the decision-making process, by building statistical models that
incorporate gathered data and calculate the likelihood of disposition of the alerted transactions, either for closure or escalation. This is supplemented by data visualization, which can be very effective for a majority of the false positive alerts generated—those that do not pose any risk to the financial institution.

4. NLG FOR NARRATIVE GENERATION

Once the investigation is complete, investigators should provide a review of their analysis in the form of a report for both reported (SAR) and non-reported transactions. For non-reported transactions—which represent the largest share of transactions—NLG can be leveraged to generate a case narrative by translating data into case summary. For this, techniques such as semantic text summarization are leveraged, wherein a semantic model is constructed using knowledge representation of objects to understand relationship structures between words and sentences. Informational content is rated based on information density metrics (such as the number of relationships with other concepts or the number of expressions showing occurrence of the concept). This is followed by the generation of a narrative that elaborates on the analysis and conclusions. This is one of the most challenging aspect in the entire investigation process, and it is critical for financial institution to focus on segments of alerts that can be effectively processed through NLG.

Efficient alert investigations can lead to a better quality of investigation as well as a reduction in the overall time taken to process the ever-increasing number of alerts. The use of these technologies can also lead to significant capacity creation in the operations team and can allow valuable resources to be reassigned to more critical activities in addition to a reduction in the time taken for conducting investigations.

Figure 4. Alert Investigation Process Flow with Intelligent Automation and Advanced Analytics

Source: Accenture, August 2019
Implementation Challenges

Some of the challenges faced by financial institutions when implementing intelligent automation and advanced analytics technologies and capabilities include:

**ADDRESSING REGULATORY EXPECTATIONS**
Regulators mandate financial institutions to have on hand precise documentation on the type of model used, data inputted, and results generated. Regulators often require a demonstration to validate the results using the same data input. This is not always possible when using ML models, since these models continuously evolve based on the feedback and output of the previous data input. This allows these models to detect unknown typologies and bolster the institution’s ability to counter money laundering effectively. A positive demonstration of the capabilities of these models can encourage regulatory authorities to enhance their model risk management guidance and audit requirements, with a focus on ML models.

**DEALING WITH LEGACY SYSTEMS**
The ability of financial institutions’ systems to interface with new age technologies like cloud, big data and automation can have a significant bearing on the effective implementation of cognitive automation and the institution’s ability to derive increased benefits.

**POLICY DESIGN AND GOVERNANCE**
Traditional modeling techniques involve robust governance policy frameworks for development, monitoring and use of the models. It is often challenging to have well defined policies on the use of ML models at the start of the process since the underlying techniques are quite complex when it comes to providing rationale for learned parameters. With regular user feedback, and the use of limitations assessment and benchmarking, an effective framework can be developed for policy design and framework.
Accenture has established relationships with numerous vendors with expertise and knowledge across the entire AML landscape, ranging from lifecycle management, workflow management, data enrichment, threat identification, entity resolution to visualization of reports using dashboards, as shown in Figure 5 below.

We integrate the capabilities of these firms with our in-house tools and services to drive resiliency, compliance and an enhanced client experience in combating money laundering.

Figure 5. Accenture Intelligent Automation and Advanced Analytics Ecosystem—Providing Automation Solutions across the AML Landscape

| **1 Digital ID** | Using technology to facilitate the use of a single customer ID. |
| **2 Data Enrichment** | Data aggregation for a unified view of all customer data from various sources. |
| **3 Entity Resolution** | Identification of the same entity to permit a single instance for simplified screening. |

| **Foundation Technology** |
| Supporting the new ecosystem are core technology stacks, particularly in cloud and advanced analytics. |

| **Lifecycle Management, Workflow and Intelligent Investigation** |
| Using cognitive intelligence and advanced workflow capabilities, financial institutions can automate investigations and case handling to permit investigators to focus on core risk-based decisioning. |

| **Threat Identification and Risk Scoring** |
| Analyzing a broad array of data, financial institutions can use advanced analytics and behavioral analytics to identify specific typologies of behavior and use advanced scoring mechanisms and risk tolerance to balance the entities that pose a threat to the organization. |

Source: Accenture, August 2019
Conclusion

With the rapid advances in intelligent technology, financial institutions have a tremendous opportunity to enhance their AML and KYC capabilities and functions.

The advances in ML and AI allow us to gather customer information from previously difficult-to-access sources, such as free text notes, images and video, from both internal and external data sources. This data provides a more complete view of the customer and the customer’s relationships with others and allows for an effective integration of customer risk assessment through KYC, adverse media, transaction monitoring and other methods. The ability of ML algorithms to continuously learn permits them to identify new patterns of risky behavior, eliminating the dependency on standard typologies.

New age solutions built on AI and ML are expected to be a game changer in the world of financial crime and compliance for financial institutions.
Accenture’s Approach to Financial Crime Transformation

Each organization tends to operate with multiple AML/KYC systems, each featuring different technological capabilities.

Such circumstances require an in-depth understanding of how the proposed solution to transform FCC processes can be integrated with existing systems to upgrade the organization’s ability to combat money laundering. With unique requirements and broad regulatory challenges faced by financial institutions across geographies, Accenture brings to the benefit of every institution our array of in-house tools, capabilities, services and knowledge—in addition to access to our ecosystem of intelligent automation and advanced analytics vendors, alliances and partners—for implementing innovative and powerful intelligent-based compliance solutions for clients across the globe.

Accenture is working with numerous financial services institutions to transform their existing financial crime and compliance functions by integrating intelligent automation and advanced analytics technologies and capabilities that can help improve the quality of all FCC processes, reduce the volume of false alerts, improve the organization’s global compliance capabilities and increase the efficiency of compliance operations teams. In one of our engagements with a large global bank, the implementation of intelligent automation technologies resulted in an increase of 30% in the rate per hour (RPH) of reviews along with a 20% reduction in false positive alerts. The enhancement of the bank’s transaction monitoring processes helped reduce operational costs and enhanced their compliance function and capabilities.

To find out more on how Accenture can help you introduce intelligence-based automation and advanced analytics within your organization or our ecosystem, please contact one of the authors.
ABOUT THE AUTHORS

Philippe Guiral
Philippe Guiral is a Managing Director with Accenture Finance & Risk and is based in New York where he leads the North America Financial Crime group. Philippe has over 15 years of experience in large-scale change programs, working with some of the world’s leading retail, commercial and investment banks. Philippe can be reached at: philippe.y.guiral@accenture.com.

Heather Adams
Heather Adams is a Managing Director with Accenture Finance & Risk where she leads the Financial Services Resilience Risk group in the United Kingdom and Ireland. She works with financial services clients to mitigate internal and external threats via anti-money laundering, anti-fraud and operational resilience controls. She is experienced in shaping and delivering large scale transformation programs that leverage new technologies and techniques and for over 20 years, Heather has worked with many global banks to improve their organizations, processes, systems and data. In recent years, this has extended to using advanced analytics, machine learning and artificial intelligence. Heather can be reached at: heather.d.adams@accenture.com.

Bharat Mittal
Bharat Mittal is a Managing Director with the Accenture Finance & Risk practice. With more than 15 years of experience, Bharat has worked with a large number of banks and financial institutions on strengthening their risk and compliance transformation programs. He has also advised leading banks on how they can leverage artificial intelligence and automation to enhance efficiency and productivity in their financial crime function (anti-money laundering, sanctions, fraud, payments screening) and drive their implementation. Bharat can be reached at: bharat.mittal@accenture.com.

Nirmal Khachane
Nirmal Khachane is a Senior Manager with Accenture Finance & Risk and has over 12 years of experience delivering risk and regulatory projects across North America, Europe and Asia. He has deep knowledge and experience in driving strategy design and implementation for risk management functions and running large-scale, regulatory driven transformation programs. Nirmal brings his skills in areas of regulatory compliance, risk management and emerging technology solutions to help global financial institutions overcome challenges and develop robust risk management capabilities. Nirmal can be reached at: nirmal.khachane@accenture.com.

ACKNOWLEDGMENTS
The authors would like to thank the following Accenture employees for their contribution to this document:

Yuvaraj Kandasamy
Sumit Arora

ABOUT ACCENTURE
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

STAY CONNECTED
Accenture Finance and Risk

Finance and Risk Blog
financeandriskblog.accenture.com

Connect With Us
www.linkedin.com/showcase/16183502

Follow Us
www.twitter.com/AccentureFSRisk

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Copyright © 2019 Accenture
All rights reserved.

Accenture, its logo, and New Applied Now are trademarks of Accenture.