Modernize AML compliance: How five institutions are preparing for next decade of financial services
The only constant in the current risk and compliance environment is change. Since the financial meltdown more than a decade ago, institutions have been trying to anticipate the next shift in regulatory requirements as well as threats to their organization. Instead of controlling costs as originally intended, this short-term strategy has resulted in a patch-work of point solutions, large analyst workforces and unsustainable spending, reaching above $1 billion annually for large institutions¹.

As the financial industry heads into the next decade removed from the Great Recession, the need to reassess the existing approach to financial crime and compliance management is paramount. It is critical to control soaring costs and gain the effectiveness and accuracy needed to keep pace with regulatory expectations today, as well as anticipate the global proliferation of real-time payments and a future of payments across connected devices in years to come.

The following report will cover several institutions that are already reinventing their approach to financial crime risk, starting with how they understand, investigate and resolve alerts from collection of customer due diligence (CDD), anti-money laundering (AML) transaction monitoring and sanctions screening systems. Using IBM Financial Crimes Insight with Watson (FCI), these institutions are leveraging the latest advancements in machine learning, cognitive analysis, artificial intelligence and robotic process automation to transform their approach to financial risk for the better.

Top 20 US bank conducts 60% faster EDD investigations

Business challenge

A large, regional financial institution was dealing with a two-fold challenge in their enhanced due diligence (EDD) process. First, their review process was highly manual, lengthy and required too much data entry. Second, due to the subjective nature of these investigations, the results were inconsistent from analyst to analyst and had a high number of errors. In addition, understanding the outcome rationale during the audit process presented a time-consuming ongoing challenge.

The bank turned to IBM Financial Crimes Insight with Watson (FCI) to help create an EDD process that was more efficient, accurate and standardized.
Top 20 US bank conducts 60% faster EDD investigations

Transformation

- **Automate data gathering and prioritization:** Instead of requiring analysts to gather data, the solution automatically started gathering information on the entity once the alert was triggered, aggregating information from structured and unstructured data sources, including sanctions lists, business directories and search engines. The solution then ranked and categorized the data based on its relevance and source.

- **Analyze information using NLP:** Next, FCI used natural language processing (NLP) to understand the context and sentiment of articles and other information related to the entity being reviewed. These were then prioritized and annotated for analyst review, helping him or her more quickly understand relevant risk as well as why each article was chosen.

- **Investigation and audit reporting:** As a final step, the solution collected the information used to make the customer risk decision into an automated dossier for easier reference during the audit review, which often takes place weeks or months later.
Top 20 US bank conducts 60% faster EDD investigations

Results

- **60% faster reviews:** Reduced investigation times from more than 13 minutes to just over five minutes by automating much of the manual search and data entry process

- **50% reduction in rework:** Minimized the need to retrace investigation steps by collecting comprehensive information automatically in the investigation dossier

Business impact

- **Increased analyst productivity:** By reducing the amount of time for each investigation, analysts complete more investigations and focus their efforts on analysis instead of data entry

- **Improved outcome consistency:** Using NLP, FCI can apply the same logic across any written information source, eliminating subjective interpretation due to analyst fatigue or varying interpretation

- **Reduced audit effort:** With an automatically-created dossier, the typical time and effort to understand and recreate the analyst’s decision rationale is virtually eliminated
Top 10 global bank speeds AML investigations 200%

Business challenge

This multi-national financial institution was dealing with a typical challenge in their approach to AML compliance. The institution had existing transaction monitoring systems that were producing an unwieldy number of alerts. In addition, after several mergers with and acquisitions of other financial institutions, they had a patchwork of data sources and little insight into whether a single customer appeared in multiple systems as an accountholder in legacy institutions. As a result, AML analysts spent much of their time data gathering and attempting to corroborate alerts that resulted in 99% false positive outcomes.

At this point, the institution leveraged IBM Financial Crimes Insight with Watson (FCI) to reduce the time and effort spent on data gathering, improve prioritization of the highest risk alerts and speed decision making by providing analysts with better insight on customer risk.
Top 10 global bank speeds
AML investigations 200%

Transformation

- **Analyze existing alerts:** As a first step, IBM reviewed the last 12 months of AML alerts to uncover areas of improvement. From the output, it was discovered that 7% of alerts were duplicates, a result of the inconsistent data sources at the bank.

- **Understand fragmented data:** Next, IBM assessed 1.7 million customer records against eight key fields to determine if necessary information was present and being pulled from the correct source systems. The result showed that only 52% of records were deemed “healthy”, meaning all necessary information was present and accurate from source systems. As a result of the health check, potentially 1.6 million false hits could be avoided by addressing these discrepancies.

- **Speed investigations with context:** Lastly, to help the bank increase the speed and accuracy of complex sanctions and transaction monitoring investigations, IBM found ways to gather and combine data to help the analyst make better decisions faster. By pre-aggregating data such as related alerts, cases and SARs; comparing a subject’s KYC profile against his/her actual profile; and analyzing negative news related to the entity, the analyst is provided with the right information to make a more informed decision.
Top 10 global bank speeds
AML investigations 200%

Results

- **50% Reduction in alerts:** Lowered false positives from existing AML transaction monitoring system by applying additional layers of advanced analytics

- **200% Faster reviews:** Increased investigation efficiency by using relationship analysis and text mining to automatically collect data

Business impact

- **Better use of limited resources:** By providing greater insight and eliminating duplicates, analysts can focus on the truly suspicious behaviors and quickly resolve low-risk alerts

- **Increased customer visibility:** With a consolidated view of customer accounts, the bank has improved their understanding of customer behavior and risk

- **Faster response to emerging risks:** By proactively collecting and presenting contextual information to analysts, risks can be prioritized and resolved more quickly
Top 4 Chinese bank identifies 65% false positives

**Business challenge**

This international Chinese financial institution had a high number of false positives from its correspondent banking division in the US and a lack of consistency and standardization in reviews. Given the limited visibility into correspondent banking relationships, the bank’s existing AML transaction monitoring system was producing alerts at a 99% false positive rate.

The institution chose IBM Financial Crimes Insight with Watson (FCI) to help it reduce the number of false positives and gain greater insight on its correspondent banking alerts.
Top 4 Chinese bank identifies 65% false positives

Transformation

- **Resolve entities and individuals:** As a first step, FCI applied entity and address resolution to consolidate duplicate alerts and customer ID's as well as provide a greater insight into traditionally limited customer behavior.

- **Create features from historical outcomes:** Next, leveraging machine learning and statistical models, FCI created hundreds of features and prioritized them by how closely they predicted historical outcomes.

- **Categorize alerts based on scoring:** Using the scoring methodology created, the bank could rank alerts based on their predicted outcome, with more than half resulting in no SAR and close to 5% recommended for SAR submission.
Top 4 Chinese bank identifies 65% false positives

**Results**

- **65% Identified as false positives:** Reduced the number of alerts by demonstrating that these would not result in a SAR being filed.

- **72% of SARs in top 5%:** Pinpointed the highest risk transactions in the top 5% based on scoring methodology, ensuring the analysts immediately focused on these transactions.

**Business impact**

- **Reduced wasted efforts:** By focusing analysts on the highest risks and de-prioritizing the lowest risks, the bank can better manage its AML program and available resources.

- **Enhance customer understanding:** By aggregating information into a single view, the bank has greater visibility into a given entity as well as its relationships.

- **Greater investigation automation:** Using data science techniques, the bank enabled a standardized detection methodology, focusing analysts on decision-making rather than information gathering.
Large UK bank lowers false positives 70%

Business challenge

A large financial institution based in the United Kingdom was dealing with a triple threat of AML inefficiency. First, their AML transaction monitoring system was generating 99% false positive alerts, leading to wasted analyst effort. Second, they had multiple data sources across multiple lines of business with inconsistent data, leading to lengthy reviews to understand which data was accurate, and which was outdated. And third, compounded by the prior points, they had high costs to conduct customer list screening across their large customer base.

The bank looked to IBM Financial Crimes Insight with Watson (FCI) to streamline their AML investigations and better understand where their process could be improved.
Large UK bank lowers false positives 70%

Transformation

- **Start with the data:** Over a two-week period, IBM connected to the bank’s disparate data sources across multiple lines of businesses. From this consolidation effort, subsequent analysis provided insight into previously unknown relationships and behaviors.

- **Identify entities and networks:** With this combined data set, IBM found more than 20,000 alerts that were connected with entities that had more than one customer ID. In addition, by better understanding individuals, previously hidden relationship networks were exposed, providing not only fewer false positives, but fewer false negatives as well.

- **Improve accuracy and outcomes:** Lastly, using machine learning and statistical models, IBM scored alerts based on past dispositions to improve risk prioritization and eliminated time wasted on low-risk investigations. Using this priority ranking, the highest risks were sent directly to senior investigators.
Large UK bank lowers false positives 70%

Results

- **70% Fewer false positives:** Eliminated false positive alerts using a combination of strategies to better understand individuals as well as underlying risk

- **50% Less false negatives:** Improved accuracy and reduced overlooked risks by better understanding connections between entities and relationship networks

Business impact

- **Better use limited resources:** By providing greater insight and eliminating duplicates, analysts can focus on the truly suspicious behaviors and quickly resolve low-risk alerts

- **Increased customer visibility:** With a consolidated view of customer accounts, the bank has improved their understanding of customer behavior and risk

- **Respond to emerging risks faster:** By proactively collecting and presenting contextual information to analysts, risks can be prioritized and resolved more quickly
Top 20 Asia-Pacific bank cuts sanctions workload 50%

Business challenge

This large, international financial institution needed a solution to its growing number of sanctions alerts from its inaccurate, legacy watch list screening solution. With more than 600,000 alerts and a 99% false positive rate, the bank was spending most of its analysts’ time on alerts that should never had been created.

The bank chose IBM Financial Crimes Insight with Watson (FCI) to eliminate these false alerts and help their analyst focus on the true risks to the organization.
Top 20 Asia-Pacific bank cuts sanctions workload 50%

Transformation

- **Apply layered analytical techniques:** Scrutinized historical alert outcomes using a combination of statistical, linguistic, cultural, temporal, geographical, entity, machine learning models and expert rules to better understand the factors that led to high false positive rates versus legitimate risks.

- **Understand entities in context:** Instead of a name match across any available field, FCI analyzed alerts for the individual’s name, company name or place against the appropriate field in the sanctions lists. This way, a person or business with the name that happens to match a sanctioned country could be understood in that context and suppressed as an alert.

- **Automate outcome transparency:** The solution recorded the information and methodologies used to make the risk decisions for straightforward review by analysts or auditors.
Top 20 Asia-Pacific bank cuts sanctions workload 50%

Results

- 50% of alerts as low risk:
  Identified half of sanctions screening alerts for special handling, meaning they could receive a fast track review or be closed automatically

- $3 Million savings:
  Estimated financial benefit to the bank from the elimination of unnecessary work to be $3 million in net present value (NPV)

Business impact

- Reduced wasted efforts:
  Increased analyst productivity by focusing resources on legitimate risks instead of false positives

- Improved client experience:
  Reduced unnecessary customer friction and transaction holds from high number of false positives

- Enhanced cost effectiveness:
  Produced immediate positive impact on the institution's bottom line
Conclusion

Using layered analytical techniques and investigation-specific automation provided by IBM Financial Crimes Insight with Watson, these financial institutions are fundamentally reinventing their decades-old approaches to financial crime investigation and AML compliance management.

While the initial benefits to many of these institutions has been efficiency, as artificial intelligence grows in use and acceptance across the financial industry, the need to remain both transparent and augment rather than replace human decision-making will be paramount. IBM Financial Crimes Insight with Watson is built on these key principles, and will continue to provide both banks and regulators with solutions that improve customer insight and uncover the hidden risks that were previously undetectable by legacy technologies.

To learn more about how IBM Financial Crimes Insight with Watson can update your approach to financial crimes management, visit ibm.com/regtech.
About IBM Watson Financial Services

IBM works with organizations across the financial services industry to use IBM Cloud™, cognitive, big data, RegTech and blockchain technology to address their business challenges. Watson™ Financial Services merges the cognitive capabilities of IBM Watson® and the expertise of Promontory Financial Group, an IBM company, to help risk and compliance professionals make better-informed decisions to manage risk and compliance processes. These processes range from regulatory change management to specific compliance processes, such as anti-money laundering, know your customer, conduct surveillance and stress testing.

© Copyright IBM Corporation 2018
IBM Global Business Services Route 100
Somers, NY 10589
Produced in the United States of America, December 2018

IBM, the IBM logo, ibm.com, IBM Cloud and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.