INTERNATIONAL INSTITUTE FOR ANALYTICS™

RESEARCH BRIEF

RESEARCH & ADVISORY NETWORK

Fighting Money Laundering with Intelligent Automation

CHRISTOPHER GHENNE

Global Lead, Banking Compliance Solutions, SAS Institute

BETH HERRON

Americas AML Lead, SAS Institute

DAVID STEWART

Director, Financial Crimes & Compliance, SAS Institute

ROBERT MORISON

IIA Lead Faculty

FEBRUARY 2021

A Fast-Changing Scene

The world of money laundering and other financial crimes – and they do span the globe – continues to reshape rapidly. The amount of money laundered is estimated at between 2 and 5 percent of global GDP. The midpoint of that range has over $3 trillion in illicit funds moving annually through the financial services industry. That's several million dollars a minute. If the money laundering "industry" were a country, it would have the fourth or fifth largest GDP in the world.

Fraudsters and launderers keep getting more sophisticated, changing their mechanisms and making transactions and money movements more complex. They are also becoming more digitized, taking advantage of synthetic identities, data breaches, the dark web, and faster funds movement. As evidence of their capabilities, consider that only about 1 percent of illicit financial assets are frozen or seized.

Monitoring the movement of funds and other transactions, and identifying the suspect ones, is extremely difficult and costly. Some 95 percent, and sometimes more, of the events flagged by institutions as suspicious are false positives. Investigating them consumes enormous time and effort and reduces speed and service to law-abiding customers. The banking industry's effectiveness rate in detecting true suspicious activities is under 5 percent, and its total AML compliance cost is estimated at over $180 billion annually.

The COVID-19 pandemic is increasing the opportunities for financial fraud and thus the volume of subsequent money laundering. As consumers stay close to home, they order more goods and services online and they move more of their financial activities and management online. Those who are new to operating online or not technologically savvy to begin with are especially vulnerable to frauds and scams.

As governments began distributing pandemic-relief financial aid to businesses and individuals, often hastily and without tight controls, the fraudsters sprang into action. A U.S. Small Business Administration report found that, as of July 31, 2020, the agency had distributed $13.4 billion to accounts that differed from the bank accounts listed on the original loan applications, and $58 billion to applicants using the same IP addresses, email addresses, businesses addresses, or bank accounts. Potentially fraudulent claims numbered almost a million. When such widespread fraud happens, the financial institutions disbursing the funds can be held partially accountable, even when it's the governmental controls that were lax.

The pandemic has also disrupted the operations of financial institutions as staff in many roles shifted to working from home. Financial crimes investigators, accustomed to being co-located, had to adjust their workflows and communications. There's some good news here, however. Institutions were forced to take more advantage of technology, and the speed and effectiveness with which they adjusted to remote work shows resilience in maintaining business continuity. Maintaining the status quo, however, is never enough.

Detecting and preventing financial crimes is a high-speed game of chess, where the institution has to anticipate the opponents' moves and think several moves ahead. Here financial institutions are at a disadvantage because their fraud and money-laundering detection and prevention processes are slow, even after spending billions on technology and staff for monitoring and compliance.

Today, continuous and sometimes radical improvement has become a business imperative.

Institutions must rethink and accelerate their processes, become both more efficient and more nimble, and react faster to the changing schemes of financial crime.

The means of improvement is *intelligent automation*. Increasing automation is necessary just to handle the growing numbers of transactions and cases. AI, machine learning, and predictive analytics give the automation greater intelligence through both accuracy in flagging potential cases and visibility into emerging patterns. Advanced analytics also add new dimension to detection and investigation, for example when network analysis reveals the connections among perpetrators and their activities over time.

Starting with Data

These opportunities for more intelligent automation start with data – the amount, variety, and quality of data available for analysis. The data platform's core job is in technical parlance "ETL." *Extract* data from the typically several and siloed systems where source data is generated and stored. *Transform* the data to make it more complete, consistent, and integrated. This includes resolving and matching entities such as individuals, organizations, and transactions that may have been represented in different ways in different source systems. Analytics plays a growing role in the transform step. Finally, orchestrate the data to *Load* it at the right times into analytical models, investigator applications and workflows, and management visualization and reporting systems.

The data management platform must also have the flexibility to expand in several ways:

- Incorporate external data as it emerges. For example, European enforcement agencies are updating their registries of the Ultimate Beneficial Owners (UBO) of financial accounts and forcing companies to reveal their ownership interests. The data assists in the analysis of company connections, subsidiaries, and risk.

- Generate useful new data. Most financial institutions' AML processes could make more aggressive use of the digital trails and biometric data they are already capturing, as well as expand their use of geo-location and device identification data.

- Leverage historical data. Institutions that have been tagging all of their historical outcomes in AML and financial fraud detection have a rich store of information to model and analyze, and they can automate the detection process with a high degree of confidence.

Opportunities for Automation

With extensive amounts of useful data at hand, analytics-enabled automation can take a variety and combination of forms.

First, automate repetitive, manual, error-prone, and low-value tasks to free investigators' time to focus on high value work. Targets for automation start with high-volume areas such as the cash book or wire book and anyplace with high false positives rates. But automation can go well beyond the scanning and monitoring of financial transactions. For example, the trade risk analysis department of a top-ten global bank uses text mining and natural language processing to automate the review of complicated letters of credit and amendments to international trade finance documents. This work is repetitive and fatiguing for analysts, who are then prone to missing

things. The initial rollout of automated scanning in 2020 saved analyst time equivalent to 15 FTEs, and the global rollout in 2021 will save the equivalent of 65. It's a win/win – time and cost savings in the investigative process, and faster approval of letters of credit and amendments for the customers.

Second, screen and score transactions and entities in more accurate and sophisticated ways, reducing false positives and enabling investigators to focus on the most likely instances of money laundering and fraud. This moves beyond robotic screen-scraping to grab data, and beyond reliance on simple typologies and business rules that often yield arbitrary results. Automated analytical screening and scoring finds more patterns and anomalies. It traces and notices changes in behaviors. Transactions, individuals, and organizations are scored for probability of fraud and collusion, and prioritized for deeper review – how likely is each case to result in a SAR? What indicates and constitutes suspicious activity keeps changing, and behavioral analysis is the only way to keep up.

Third, have cases follow the most efficient paths of investigation, thus streamlining investigators' workflows and improving speed and service to customers. This goes beyond the strict escalation process of first-level review, second-level review, manager review, QA, and SAR. Instead, green-light the simple cases and move high-risk cases more directly into closer analysis. This is another way to focus investigators' attention on the cases most likely to reward their effort. What's the best workflow and path for each individual case?

Fourth, employ network analysis to trace and evaluate the connections among entities and transactions, thereby painting a more complete, holistic, and insightful picture of illegal activities. This goes far beyond cursory views of entities and their activities in isolation, making it a key technique for AML. Most financial crime is committed by people and organizations conspiring and acting together, not by lone wolves. Trying to trace the connections manually can be painstakingly slow, complex, and error-ridden. Analytically connecting the dots improves accuracy, accelerates investigation, and puts the activities in motion across time. With the aid of easily-generated visualizations, investigators can see and assess more complete pictures of financial crime in action.

These types of automation work together to improve the speed, accuracy, and value of the monitoring and investigation processes and to make the best use of the human resources performing them. Better scoring enables better pathing, for example. And automated scanning of transactions provides the basis for automated discovery of networks. Overall, investigators can spend less time gathering data and looking for patterns manually, and more time assessing cases and making decisions on them.

Integration Enables Automation

Intelligent automation depends on integration across several fronts.

Data needs to be better integrated than most institutions have managed to date. Most still struggle with siloed data and decisioning systems, well aware that they are unwieldy, expensive, and inefficient. There's too much data movement and data duplication, and the ETL process is too complex. So institutions are developing better data reference architectures, stewardship, and governance to help them establish "single versions of the truth." That means consistent and shared versions of the source data and facts about important entities and transactions. Then combining good data from traditionally siloed areas of compliance enables more

advanced analytics to assess more complex threats and to provide more comprehensive pictures of risks.

Software and hardware technology needs to be better integrated, not necessarily as consolidated systems and databases, but through a flexible and coherent architecture. Flexibility is essential because the technology industry has reached a strategic inflection point with respect to cloud services and open source software. With more reliance on the cloud, institutions can better cope with growing transaction and analytics volumes, meet customer expectations for more speed and immediacy in digital interactions, and often reduce costs. With selective use of open source tools and algorithms, institutions are supplementing their home-grown and commercial systems capabilities, experimenting more, and adapting faster.

Meanwhile, technology coherence is essential to the efficient and effective development, deployment, operation, and maintenance of business applications, data products, and analytic models. When there is a single environment for building, testing, deploying, and managing models, they deliver value and adapt to change faster.

With better integrated data and technology, the processes of investigation and the people who perform them can become more integrated, collaborative, capable, and flexible. Investigators and their workflows have more complete and holistic views of money movement and other financial crime activity. Staff can more readily cross-train, including between fraud and AML. They can learn to handle more challenging cases, and they can be deployed in areas of greatest need.

A financial institution ultimately needs people who understand the varieties and tactics of fraud, people who understand money mule and other complex money laundering behaviors, and people with information security skills who can help make sense of the different digital trails and fingerprints left behind by fraudsters and launderers. And it needs them working together, equipped with data and analytics. The future will see the convergence of fraud and AML practices into “fusion centers” where sharing of data to support complex investigations is made easier through automated workflow and network analytics.

The integration we’ve described ultimately creates a more complete and coherent platform to support fraud, AML, risk, and compliance activities. Not as a piecemeal collection of systems, but a more flexible, scalable, and clearly architected arrangement of components. Platform capabilities are interoperable and shared, under the philosophy of “build once and use many.” Platforms are also adaptable, supporting innovation and open to change. The word “platform” makes many people think of technology infrastructure. We’re talking about a much broader and multi-dimensional approach to managing data, technology, processes, people, and the analytical models and software for intelligent automation.

The magic of a platform approach is that it makes things both more efficient and more flexible. It enables both streamlined workflows and rapid incorporation of new investigative techniques. It enables more unified case management, with cross-domain data providing an enterprise view of risks. Investigators have a more comprehensive and capable environment for doing the work and making the decisions around financial crimes anticipation, detection, and reduction.

Intelligent Automation in Action

A global bank knew that its rules-based transaction monitoring system was biased toward known risks. In a supplemental analysis of nearly two billion

transactions, a supervised machine learning AML algorithm found 416 suspected money service businesses, 89 of them previously unknown or unregistered as such.

A retail and commercial services bank in Asia Pacific was struggling with the volumes of transactions and alerts and high false-positive rates. A new ensemble of analytics models incorporated transaction, entity, network, scenario, and customer risks. The fully automated alert review process reduced false positives by 33 percent, for major cost and time savings.

A regional U.S. bank is replacing its rules-based cash activity scenarios, which consider only 6-12 variables, with advanced models that can consider 75-80 variables to detect suspicious activity. The initial replacement of ten scenarios tripled the SAR conversion rate and reduced work items by half. Some 200 more rules-based scenarios will be replaced by around three dozen analytical scenarios for high-risk typologies.

One institution has been deploying machine learning models on top of continuous transaction monitoring for three years. The models are in their sixth iteration, guided by a simple strategy: “Find out what’s changing and adjust. Leave the rest alone.” Through sophisticated distribution and clustering techniques, the models can highlight groups where three in ten entities are ending up in a SAR – an extraordinary rate.

Intelligent automation in cases like these has been shown to deliver up to 80 percent reduction in false positives, a fourfold increase in SAR conversion rates, and a decrease in alert volume by over 50 percent. It also rapidly discovers hidden threats, provides holistic views of customers, and lowers the cost of compliance. These benefits in turn improve customer service while protecting brand and shareholder value.

Implementation Success Factors

The implementation process for intelligent automation naturally starts with the data. What data does the institution have, and is there enough history to model what normal customer behavior looks like? What data will be needed to really “know your customer” by developing more complete profiles and more predictive models of their behavior?

The data journey happens in stages. First a focus on basic data availability and quality, then on data completeness and integration to develop comprehensive views of customers, and then on enriching those views digitally with, for example, device ID, device reputation, and geolocation.

Institutions must recognize the value of this data. Financial crimes detection functions may in fact have the most complete and holistic view of customer behavior available in the enterprise. Making use of that data may require a cultural change. Many business compliance staff have legal or law enforcement backgrounds, so they take a policy-oriented, find-the-answer approach to data. Capitalizing on advanced analytics requires a more exploratory, connect-the-dots, see-what we-can-learn orientation.

To implement intelligent automation with speed and success, most institutions need to supplement their business and technology capabilities, and they should avoid the trap of trying to do too much on their own. Both compliance and IT organizations tend to be stretched thin and under pressure to demonstrate their value, and they err on the side of trying to do too much too soon, and too much in house, even when

they lack necessary expertise and experience. Assistance can come in several forms:

- Enlist the help of experienced partners who bring both technology and AML domain expertise, including analytical models and software, business processes and methods, and implementation playbooks.

- Leverage open-source tools and software. This assumes, of course, that technology staff have the associated development skills, analytics professionals can handle off-the-shelf algorithms and models, and the technology platform can readily incorporate new tools and analytics and applications modules.

- Band together with other institutions to share infrastructure and expertise, with AML operating as a shared and managed service. For example, in the Nordic region, 120 small banks share one data center and core AML software and analytics installation. A major bank in France is taking a similar approach to AML across 14 large-themselves subsidiaries.

Smaller institutions and late adopters that are just ramping up their capabilities can take these approaches to accelerate implementation, establish capable and flexible platforms, and control costs, while performing AML and fraud detection and analysis with levels of completeness and sophistication higher than their size would suggest.

Larger institutions are more likely to have fragmented data and technologies that they're striving to integrate, especially if they have grown via merger and acquisition. Their approach involves a combination of augmenting their capabilities and gradually replacing assets that have gone obsolete. When it comes to modernizing and automating AML methods, most employ a hybrid strategy. Continue to use rules-based alerts where they work. Develop more advanced algorithms where the rules don't work. And augment rules-based alerts with scoring algorithms to triage the alerts further for probability of suspicious activity. Again, a platform architecture can help simplify the environment, incorporate augmentations, and roll off legacy systems and technologies over time.

Looking deeper in the implementation process, we see four keys to success:

- ***Iteration***. The introduction of new analytical models is an iterative process. It's not a linear specify-build-and-deploy. Instead it's experiment and innovate, then test and run in parallel with existing methods, then refine the model and repeat as needed. Advanced organizations also experiment with different models, using champion-challenger techniques to identify the best.

- ***Collaboration***. That iterative approach demands close collaboration. Investigators and analysts work with model builders to assess results, adjust assumptions, refine methods, and anticipate the operational effects of the innovation. What are the best ways to package the new analytics, and what training is needed to use them?

- ***Transparency***. When transitioning from rules-based alerts to more behavioral and probabilistic scoring, investigators have to learn to trust the new outputs, not just use them. Models can't be black boxes – they need to trace or explain their decisions with much the same clarity as do rules-based alerts.

- ***Feedback***. The accuracy of analytics, outcomes of decisions, and results of investigations are captured rigorously for the purpose of

continuously improving predictive models and the case management process. The collaborative communication and feedback among investigators and analytics professionals is also continuous.

The financial crimes scene may be moving fast, and models today can be deployed quickly, but patience is still essential. How long new models run in parallel depends on the organization's risk appetite, but it can be several months. The overall process of modernizing and augmenting the platform will take time, especially the introduction of the most advanced machine learning, text mining, and network analysis techniques. The commitment to stay-up-to date with skills, methods, and technology can never wane. As a very practical matter, the determined-yet-patient institution avoids the all-too-common pitfall of sending an AI solution in search of a problem before data and other key ingredients are available, and before ambition is clear.

Along the way, however, there should be ample low-hanging fruit. And that's important when institutions are cost and value conscious and eager to improve detection rates. Focusing first on automating repetitive and manual work can gain a lot of operational efficiencies and free investigators for more value-added work. Even rudimentary scoring of entities and events can significantly lower the false positives rate, and automated triage of cases frees more investigator time. As more complete views of customers and their behaviors coalesce, better insights keep improving decisions.

What Success Looks Like

By way of summary, we can ask: How do institutions know they are succeeding? Their transaction scanning and other high-volume activities are well automated. They can deploy advanced analytics to improve the most challenging facets of AML and fraud investigation. There are results to show – they really understand the customers, false positives decline, and more investigated cases yield results. Decision-making data is at hand, and the investigation process accelerates with efficiency.

What characteristics underlie such success? The institutions take a platform approach to improving and integrating data, technology, processes, and people. They have cultures of analytics, collaboration, fact-based decisions, and continuous improvement. They know that they'll be consuming more and more data, and they follow the best data practices, but they also know that data doesn't have to be perfect to do the job. They iterate in the collaborative development and deployment of data and models. And they have a strong working relationship between the business and IT, with the business in the lead.

Finally, they don't look at compliance as a cost to be minimized, but as a necessary and strategic investment that delivers business value. They recognize the impact of compliance on customer experience, brand, and shareholder value. Compliance is not a tick-the-box exercise, but a process of understanding financial risks and how they are changing, and continuously improving the methods for mitigating those risks. Intelligent automation raises the ROI of investments in compliance.

Additional Information

To learn more about this topic, please visit: www.sas.com/AML.

About the Authors

CHRISTOPHER GHENNE

GLOBAL LEAD, BANKING COMPLIANCE SOLUTIONS

SAS INSTITUTE

Christopher Ghenne is a financial crime specialist with over 15 years' experience in the field. He has worked in the banking, insurance, government and telecommunications sectors helping organizations comply with Anti-Money Laundering regulations and protect their customers and shareholders from losses. Based out of Belgium, he owns the responsibility of enablement and presales support worldwide.

With his team, he is also developing compliance propositions for specific markets working to strategically develop financial crime capabilities for SAS (AML transaction monitoring, KYC, CDD and Sanctions). Christopher has been a Certified Anti-Money Laundering Specialist for more than 12 years and holds a master's degree in Finance from the University of Brussels (ULB) – Belgium.

BETH HERRON

AMERICAS AML LEAD

SAS INSTITUTE

Beth Herron is a Principal Industry Consultant within the SAS Security Intelligence Practice, providing domain expertise in the development, sales support and implementation of financial crime banking solutions. Beth leads a team of subject matter experts who support tier 1 and 2 financial institutions with AML, CDD, CTR and Next Gen Analytic solutions.

In her prior role, she worked within the Financial Intelligence Unit at one of the world's largest banks. As the subject matter expert for analytics, monitoring and case management, she provided responses to AML audit and exam inquiries in more than 40 countries throughout Europe, the Middle East and Africa, Asia Pacific and the Americas. Her experience also focused on the strategy and transformation of customer risk assessment, Fraud and AML system integration, and data management. Beth holds a master's degree in Industrial Organizational Psychology focusing on research in behavior prediction and modification. Beth has been accredited as a Certified Anti-Money Laundering Specialist (CAMS).

DAVID STEWART

DIRECTOR, FINANCIAL CRIMES & COMPLIANCE

SAS INSTITUTE

David Stewart is responsible for the development of strategy, guiding product management and supporting the marketing of SAS' fraud and financial crimes solutions for the banking industry. Stewart is responsible for coordinating best practices among SAS' global subject matter experts in combating financial crimes. He works closely with many of the world's most innovative financial services institutions, regulatory agencies, SAS research and development, implementation teams, and alliance partners to deliver superior solutions for fraud detection and complying with anti-money laundering regulations.

Previously, Stewart served as a SAS Business Manager at one of the world's largest financial institutions. He has worked exclusively with financial services companies over the last 20 years on various consumer risk, marketing and compliance initiatives. Stewart is a Certified Anti-Money Laundering Specialist, serves on the North Carolina ACAMS board, and holds a bachelor's degree in economics from North Carolina State University.

ROBERT MORISON

IIA LEAD FACULTY

Robert Morison serves as Lead Faculty with IIA. He is an accomplished researcher, writer, speaker, and management consultant, and an authority on what happens at the intersections of business, technology, and people management. He has been leading breakthrough research for more than 30 years, collaborating with eminent academics, thought leaders, and management innovators. He has written on topics ranging from business innovation, reengineering, and analytics to workforce management, demographics, and retirement.

Bob is the coauthor of three books: *What Retirees Want: A Holistic View of Life's Third Age (Wiley, 2020), Analytics at Work: Smarter Decisions, Better Results (Harvard Business Press, 2010), and Workforce Crisis: How to Beat the Coming Shortage of Skills and Talent* (Harvard Business Press, 2006). His 2004 *Harvard Business Review* article, "It's Time to Retire Retirement," coauthored with Ken Dychtwald and Tamara Erickson, received a McKinsey Award. He holds an AB from Dartmouth College and an MA from Boston University.

IIANALYTICS.COM