COMPLIANCE WEEK

WorkFusion

Financial Services **Roadmap:** Know Your Customer

Gain keen insights on how to tackle a more robust sanctions compliance program while potentially reducing costs.

Inside this e-Book

Intelligent Automation in Economic Sanctions Compliance

The debate over whether banks and other organizations should pursue advanced technologies — including intelligent automation,artificial intelligence and machine learning — to drive sanctions compliance has shifted from "if" to "when, how, and on what scale?"

Kirill Meleshevich
Head of AML, WorkFusion

Already, this shift is proving to be good news for control coverage, employee productivity, job satisfaction, and customer experience. But is it also bad news for illicit actors seeking to overcome banks' compliance controls? These technologies redefine what is possible with sanctions compliance by helping to implement risk-management controls that would otherwise be impractical or impossible.

Sanctions risk is not restricted to a single governmental list, and effective compliance with embargoes typically extends beyond list screening. Many sanctioned entities are not explicitly placed on a list but must still be identified. Different governments' sanctions lists can provide critical due diligence, even if that does not create a legal prohibition. Organizations have typically sought to meet sanctions compliance needs through incremental technological improvements (such as a new, better screening system), large increases in hiring, and exiting high-risk business. However, current screening technologies may offer only marginal improvements in identifying sanctions risk or otherwise require drastic increases in resource needs; high rates of hiring can diminish banks' return on equity; and exiting risky but important business lines can decrease overall profitability and the ability to retain valuable customers. New technology platforms, such as WorkFusion's Intelligent Automation Cloud, meet these challenges head-on by complementing and improving existing controls and greatly expanding the aperture of risk identification — without introducing new permanent costs or complexities.

How can intelligent automation redefine sanctions compliance?

1. Incorporate sanctions evasion intelligence into screening
2. Identify and act on non-listed sanctions risk
3. Reduce false positives in sanctions screening alerts
4. Expand sanctions control coverage

Intelligent automation to incorporate sanctions evasion intelligence into screening

1

Improved Sanctions Evasion Identification • Enhanced Sanctions Screening • Improved Regulatory Compliance

Over the past several years, governments, think tanks, and supranational organizations have released a wealth of robust information on sanctions evasion. Since 2015, the U.S. government's sanctions administrator, OFAC, has released detailed accounts of how illicit actors seek to overcome Russian, Venezuelan, North Korean, and Syrian sanctions programs. Law enforcement indictments and administrative actions complement this information. In March 2019, the UN released a 150-page "panel of experts" report on North Korean sanctions evasion, which included not only lists of maritime vessels and companies used to evade sanctions, but also detailed schemes.1 Banks can do more to make use of this rich data set. Compliance teams typically review this guidance and include summaries in trainings and briefings to business lines. In rare cases, a bank may seek to tune a screening system in direct response to new guidance. Most often, this highly valuable intelligence is left unused. Conversely, intelligent automation can make effective use of these genuine and confirmed sanctions evasions examples to better equip banks to identify similar activity.

$3.59 billion USD

VALUE OF 79 SANCTIONS AND ANTI-MONEY LAUNDERING PENALTIES
ISSUED OVER THE PREVIOUS 12 MONTHS BY REGULATORS IN THE UNITED STATES, BELGIUM, ENGLAND, HONG KONG, LATVIA, INDIA, AND OTHER COUNTRIES.

> "Financial institutions around the world screen against the UN and OFAC lists. They also screen against other public lists, like companies identified in UN Panel of Experts reports. Those are good practices, but we encourage you to do more. We commend efforts by financial institutions to go levels deeper, asking for more information to help you conduct additional analysis to identify [sanctions evasion].
>
> — U.S. Treasury Department Undersecretary February 2018[5]

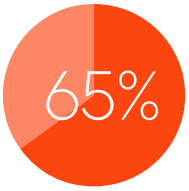
Whereas current sanctions screening is "list dependent" — relying largely on flagging specific names or slight variations in a transaction — intelligent automation and machine learning can search for more nuanced patterns of keywords, word omissions, combinations of names, and context that may reveal sanctions risk and exposure. For example, the use of "Dubai," "shipping" and "onward" in a wire transfer or trade finance transaction may reveal that goods shipped to the United Arab Emirates are destined for Iran, as cited in countless sanctions enforcement actions.2 The use of vague descriptions in trade finance activity, such as "any port" or "open sea," combined with context on the industry, countries involved and vessel behavior, may lead banks to identify indirect exposure to Syria, as cited in a recent law enforcement case.3 Detection of partial addresses, especially when funds are sent to Russian cities located near Crimea, an embargoed geographic territory, is a potential sanctions evasion red flag, according to an OFAC advisory.4 Keyword screening can also be a practical solution for securities-related sanctions prohibitions, like the Russian sectoral sanctions program, by identifying exposure to potentially prohibited debt and equity trading.

Intelligent automation to reduce false positives in sanctions screening alerts

2

Raised Employee Productivity • Reduced Alert Review Cost • Reduced Manual Effort • Improved Employee Satisfaction and Reduced Turnover • Higher Straight-through Processing

Across the banking, insurance, and securities industries, false-positive rates in the alerts generated by screening tools can exceed 99%, based on our ex-perience and data shared by clients. Banks directly employ or contract out dozens or hundreds of individuals to manually review these alerts. It is not uncommon that alert review teams sanctions and anti–money launder-ing combined° make up 75% of a bank's compliance staff. Nearly all banks perform some form of false-positive reduction. Currently, this is done either with "good guy" rules whitelisting words, careful selection of settings and algorithms, or raising screening thresholds to decrease the number of alerts generated. These methods are time-intensive, require ongoing refinement, and may call into question whether a bank is selectively eliminating alert volumes only because of resource concerns. Regulators have stated that eliminating lead information just to save money on hiring is not acceptable.



SANCTIONS SCREENING FALSE POSITIVES THAT WERE IDENTIFIED WITH WORKFUSION'S AUTOMATION AND MACHINE LEARNING PLATFORM IN A RECENT CLIENT ENGAGEMENT.

SANCTIONS SCREENING ALERT REVIEW TEAM PRODUCTIVITY INCREASE, FOLLOWING IMPLEMENTATION OF A FALSE POSITIVE REDUCTION SOLUTION.

Intelligent automation and machine learning go beyond "good guy" rules and system tuning to eliminate noise. The technology can be trained to study human behavior in identifying false positives and mimic cognitive decision-making. Whereas "good guy" rules need to be redesigned based on slight changes in the transaction text and can have infinite variations, machine learning can re-train itself to account for these changes. Sanc-tions compliance teams may have different resources reviewing identical or nearly identical transactions; machine learning can detect these similarities and group them together to realize additional efficiencies. In WorkFusion's direct experience implementing intelligent automation and machine learn-ing-driven solutions for multiple financial institutions, approximately 65% of false positives were identified, dispositioned with clear justifications, and either closed or routed to a human operator for confirmation, based on the risk threshold of the bank.

Whereas traditional sanctions screening tools largely treat all inputs identi-cally, intelligent automation for sanctions screening can operate customer, product, or transaction-specific nuances that help mitigate high false-pos-itives rates. For example, WorkFusion's false-positive mitigation tools make different decisions about alerts generated in a reference field, address field, or free-text field. This approach is being adopted by financial institutions. In a recent publication, Societe Generale noted that their approach to false-positive mitigation for sanctions alerts focused on product-specific rules.6

Eliminating clear false positives is not solely a cost-efficiency consider-ation. A range of academic research indicates that human operators make mistakes when faced with performing and re-performing identical, manual tasks. Using time and money to review thousands of false positives is an efficiency problem. Missing the "needle in the haystack," that rare true pos-itive, due to resource strain from reviewing thousands of false positives is a governance problem. Job productivity, satisfaction, and ultimately employ-ee retention can suffer when highly manual and repetitive tasks are part of "business as usual" for highly demanded resources.

Intelligent automation to identify and act on non-listed sanctions risk

3

Enhanced Sanctions Screening • Improved Regulatory Compliance

Sanctions risk is not defined by a binary presence or absence of a listed sanctioned entity being involved in a transaction. OFAC's guidelines are clear that an entity which is 50% or more owned by a listed sanctioned entity is considered sanctioned. For example, a November 2018 enforcement action highlighted that a U.S. company violated sanctions regulations when it engaged with a company that "was not explicitly identified on OFAC's List of Specially Designated Nationals and Blocked Persons, [but] was 51 percent owned" by a sanctioned entity.[7] The United Kingdom sanctions administrator is just as explicit that both ownership and controlling stakes in a non-listed entity by a sanctioned entity create a prohibition.8 While official figures are not available, it is likely that there are tens of thousands of companies that would potentially be considered sanctioned entities under the 50% rule. Furthermore, many institutions seek to understand exposure to companies that are owned less than 50% by a sanctioned entity, including to manage reputational risk. Banks currently do not have an efficient way to control for this indirect risk at scale. Incorporating lists of by-ownership sanctioned entities into screening tools can lead to spikes in alert volumes. Manually reviewing the owners and sanctions risk of each party in select transactions would be impossible without halting straight-through processing rates. However, intelligent automation and machine learning can be used to identify all entities in a transaction, retrieve open-source or subscription-based information on indirect sanctions risk, perform other targeted searches in corporate ownership databases, suppress close but not actual matches, and present to a human operator detailed and relevant risk information if exposure to a non-listed sanctioned entity is detected. Compliance with the 50% rule can become as standard as complying with traditional sanctions lists, without significant resource demands.

Intelligent automation can streamline compliance with the 50% rule by aggregating ownership data, validating links to sanctioned entities, and presenting actionable information to compliance teams.

-$15,634 USD

COST, IN PENALTIES, FOR EACH OF THE 159 TRANSACTIONS SENT BY A LARGE BRITISH BANK TO A NON-LISTED SANCTIONED ENTITY.10

Intelligent automation to expand sanctions control coverage

4

Raised Employee Productivity • Expanded Compliance Coverage • Reduced Manual Review Cost • Improved Accuracy • Faster Document Processing

Many banks can identify a non-electronic or paper-based financial product that is subject to minimal or incomplete compliance controls because of the manual, time-intensive, and error-prone work required to extract information. Most commonly, banks struggle with robust screening of commercial checks and trade finance letters of credit. However, certain securities trading processes, customer due diligence data, and credit card activity may fall outside robust screening controls due to the enormous volumes, lack of standardized data, and incomplete information to help disposition sanctions alerts. The decision to not perform screening is typically driven by a consideration that the ability to hire additional compliance staff is impeded by financial constraints. Intelligent automation and machine learning do not share the same constraints. A typical trade finance transaction will have 15 –75 pages of paper records, including the letter of credit, insurance guarantee, email exchanges, bill of lading, export permissions, and SWIFT message updates. Extracting key data from these papers and performing screening can take anywhere from 15 minutes to an hour. Error rates are typically high and can result in up to 10% of key data not being considered for sanctions compliance. Trained employees can miss obscure references to sanctioned entities, vessels, or jurisdictions, as was citied in an OFAC enforcement action several years ago.11 Intelligent automation-driven "optical character recognition" (OCR) — which digitizes text from paper records — can perform the same data extraction with accuracy rates that can exceed 95%, and improve over time through machine learning. This solution can operate outside of core working hours and submit the extracted information directly into a sanctions screening engine, further saving time and effort. Leading banks are already turning to intelligent automation for this application. For example, Citibank in April 2019 announced that it would digitize 25 million trade finance document pages through OCR for risk analytics, including sanctions compliance.12

For some institutions, robust and effective sanctions compliance may not be possible with existing technology. Unique risks stemming from product exposure, enormous transaction volumes, and manual processes often lead banks to "risk accept" certain compliance gaps.

12 weeks

FOR IMPLEMENTATION OF WORKFUSION INTELLIGENT AUTOMATION SOLUTION FOR DATA EXTRACTION AND SCREENING FOR TRADE FINANCE DOCUMENTATION.

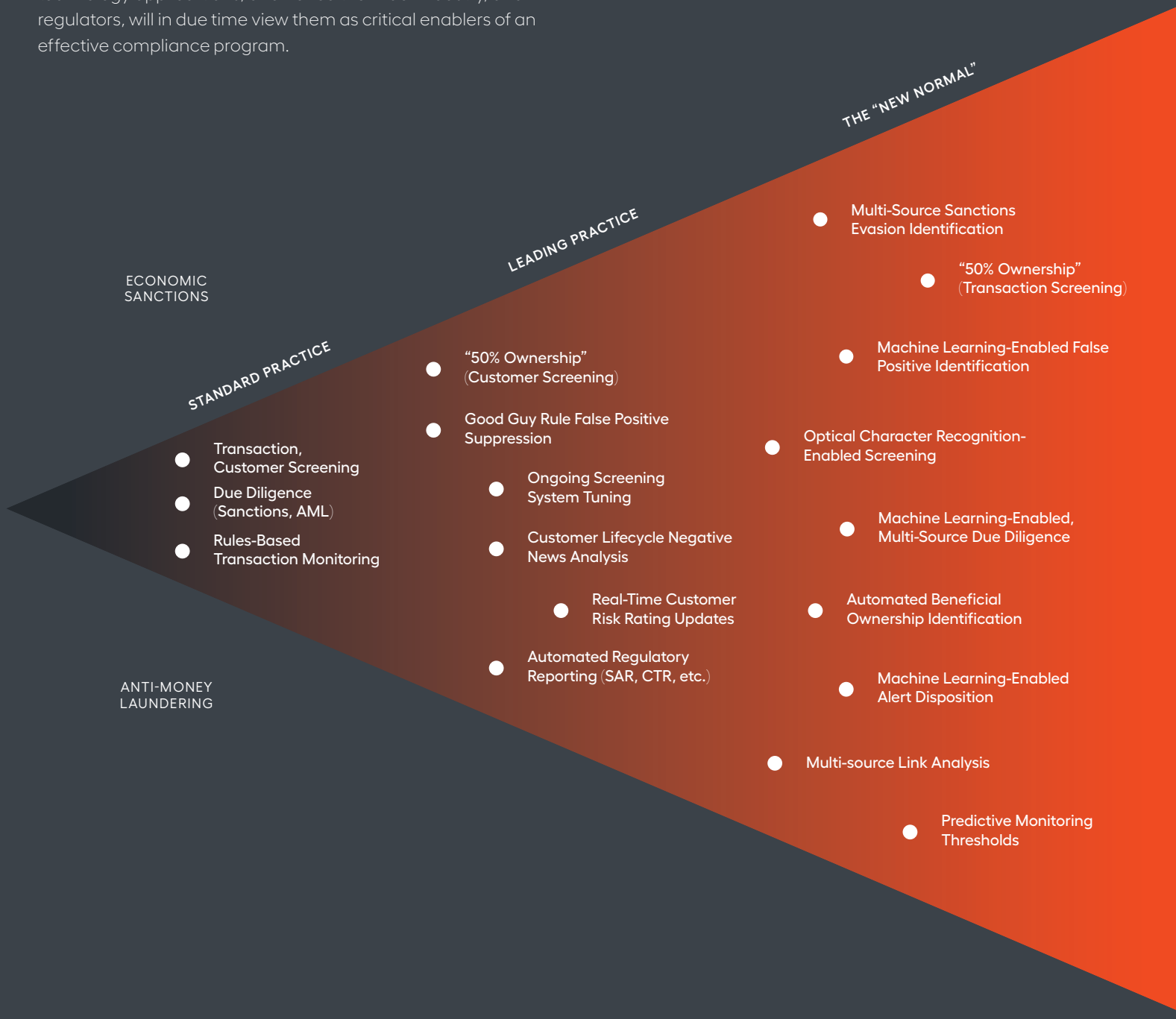
Achieving scale in AI-driven sanctions compliance

Banks' sanctions (and wider financial crime) compliance spending is outpacing revenue growth. Banking assets — a rough proxy for growth — increased by about 2.6% from January 2018 to June 2019. 14 Conversely, the number of entries on the U.S. government's sanctions list grew by about 13% during the same period.15 Continuing with "business as usual" sanctions compliance is not a practical option as resourcing needs will continue to grow and cut into profits. As mentioned at the opening of this article, implementation of intelligent automation solutions is moving from "if" to "when, how, and on what scale?" because banks view it as an answer to a difficult operational, business, legal, and compliance problem set. Sanctions compliance complexity seems set to increase over the next several years. The U.S. and other governments' reliance on economic sanctions tools is one factor; however, the expansion of different payment formats, banking of financial technology companies, supplier due diligence requirements, growth in trade flows, access and collection of "big data" due diligence on customers, and new regulatory expectations will also increase this complexity. As demonstrated over the past several years, added regulatory complexity translates directly into higher costs. Introducing artificial intelligence solutions for sanctions compliance at scale — across multiple business functions, countries, and control processes, and with training to identify additional uses — is one answer to this challenge.

Any of the artificial intelligence applications cited above can help strengthen a sanctions compliance program, but they can be most potent and transformative when working together. Achieving scale in sanctions compliance is not the same as automating one process for one team in one country through a bespoke solution. Simply automating sanctions-related searches escalates the number of alerts that require manual review. Solely introducing machine learning to suppress false positives may call into question a bank's commitment to identifying risks during regulatory exams. However, implementing a bank's end-to-end sanctions compliance vision and strategy through the lens of what is now possible using advanced technology helps to introduce scale — of automation, of risk identification, of program effectiveness, and of cost savings.

Sanctions Screening & Anti–Money Laundering Programs Are Being Redefined With Advanced Technologies

The introduction of new compliance technologies is shifting what was once considered new and "emerging" into standard industry practice. Real-time sanctions screening prior to payment settlement was once considered a novel technology — it is now a regulatory requirement. Banks are increasingly adopting these advanced technology applica-tions, and hence the wider industry, and regulators, will in due time view them as critical enablers of an effective compliance program.



What regulators want to know about KYC technology

So, you're updating your legacy know your customer (KYC) system. You've completed the internal diligence and collected the internal signoffs and approvals.Now, it's time to present your solution to the regulator.

No regulator will "approve" or endorse a vendor solution—instead it will review the new system to ensure it is commensurate with the risk profile of the institution and that it complies with regulator and the institution's internal policies.

Using artificial intelligence (AI) and robotic process automation, the new technology can often achieve higher auto-approvals and reduce false positives compared to a legacy system. In addition, KYC technology can mine billions of publicly available data points to provide a complete applicant profile and use facial recognition software to compare an applicant's submitted mobile phone selfie to an identification photo.

Financial institutions have been among the most eager first adopters of evolving KYC technology, applying tools that improve their ability to screen and verify loan applicants. But new tech can serve others as well: Casinos and online gaming platforms can use KYC tech to screen customers who might appear on sanctions or other watchlists, while online marketplaces and social networks use tech to weed out fraudulent vendors and scam artists.

Really, any business seeking to verify a customer's identity might find value in applying KYC technology to screen low-risk applications so its investigations team can focus its attention on the smaller, high-risk slice of the pie.

Begin at the beginning

Jason Somrak, chief of product for AML & Advanced Analytics at Oracle Financial Crime and Compliance Management, says the process of onboarding your KYC tech with regulators will take between 18 months and two years. Somrak's division works with banks to use advanced technology to fight financial crime and modernize risk and compliance operations.

"People won't be penalized for trying new things," he says. "But I think regulators will expect that firms won't throw everything away and start fresh." There will be a transition, where regulators will want to see that the new KYC technology provides better results than the firm's legacy system."

Regulators want to see your work; they want to see the long division and know that the bank understands how the system technology works—why it flags or alerts, why/how are the decisions being made," says Kimberly Hebb, who spent 20 years as a commissioned bank examiner with the Office of the Comptroller of the Currency (OCC) and is now chief risk officer of BillGO, a bill payment provider. "Many FinTech companies think that their technology is special and needs to be in a 'black box' system and don't want to discuss their processes."

Regulators want to hear from the financial institution that is planning to utilize new KYC technology—not the vendor, she says. They also want to understand the impetus driving the move to a new KYC solution. Is the proposal to use new KYC technology part of a planned strategy for growth or a reaction to a deficiency, violation, or past pattern or practice?

Whichever KYC program your institution uses, it "should be commensurate with the risk profile of that institution," Hebb notes. "It's not that regulators don't appreciate the need; there is still the expectation that the bank knows its customer base and provides internal controls." They also want to know that the new tool has been customized for the financial institution in question, that the results are being actively monitored, and that the processes are being updated as needed.

Regulators 'leaning in'

With KYC technology becoming a focus of many industries, many regulators, including the OCC and the Commodities Futures Trading Commission (CFTC), have to adapt regulations.

"We are seeing regulators lean in, even though they're not recommending particular tools or vendors. We are seeing a very strong adaptation of complicated analytics," says Johnny Ayers, co-founder and senior vice president of Socure, a FinTech company that provides digital identity verification and KYC solutions through AI, advanced logic, and machine learning.

"Regulators have gotten more comfortable with new KYC technologies, including machine learning (ML) and robotic automation (RA), but they require clear understanding of the model used. While stratifying data may be an easier model to verify, the large number of alerts can only be tackled effectively using ML and RA techniques," adds Piotr Jastrzebski, director of technology product management for the Financial Crimes Control group at Wolters Kluwer, a risk management and reg-ulatory compliance consultant to U.S. banks and credit unions.

In 2017, the OCC established its Office of Innovation, tasked with helping financial institutions sample FinTech solutions.

The agency's support of "responsible innovation" attempts to balance innovation with prudent risk management.

> Regulators want to see the long division and know that the bank understands how the system technology works—why it flags or alerts, why/how are the decisions being made

The agency has formed partnerships between financial institutions and FinTech vendors through an Innovation Pilot Program, created "to support the testing of innovative products, services, and processes that could significantly benefit consumers, businesses, and communities, including those that promote financial inclusion," OCC Chief Innovation Officer Beth Knickerbocker said in House testimony in 2019.

Similarly, LabCFTC helps "promote responsible FinTech in-novation to improve the quality, resiliency, and competitive-ness of our markets" as well as accelerating "CFTC engagement with FinTech and RegTech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently." The Consumer Financial Protection Bureau also has a program that attempts to "promote innovation, compe-tition, and consumer access within financial services."

Regulators in other countries have similarly embraced KYC technology. In 2019, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) announced it would allow for the use of digital documents to authenticate an individual's identity. This new policy allows individuals being vetted to supply their financial institution to scan their "government-issued photo identification document using the camera on their mobile phone or electronic device." The indi-vidual would then be required to take their own photo with their device and submit it to the institution.

But in order to verify the selfie and the photo on the identification match, the bank or credit union must have the technology to "apply facial recognition technology to compare the features of that 'selfie' to the photo on the authentic govern-ment-issued photo identification document," FINTRAC noted in its 2019 directive on identifying individuals and corporations.

"The tech demonstrated it was feasible," said Zac Cohen, chief operating officer of Vancouver, Canada-based Trulioo, a FinTech vendor that "delivers trust, privacy, and safety online through scalable and holistic identity verification." KYC tech vendors were able to prove to regulators the technology was accurate and produced verifiable results, he says.

European regulators seeking to sign off on KYC technology at companies that must comply with the General Data Protec-tion Regulation have sought to understand the "context" of its decision making—that is, how an AI tool arrives at its decisions, without focusing on the individual decisions themselves.

Factors such as the urgency of the decision, its impact, and significance might outweigh a data subject's wish to know more about the decision-making process, suggesting that a "one size fits all" approach to explaining AI-generated results is unworkable, according to U.K. data regulator the In-formation Commissioner's Office.

KYC Best Practices For When Your Client Is In The Headlines

The good news is your negative media screening is working; the bad news is your client is in the headlines.

The discipline of "know your customer/client" (KYC) has grown beyond the verification of a name, address, ownership, and control. Nowadays it is an ongoing process, a living thing. Many regulators now expect firms to apply ongoing negative media screening to all high-risk client relationships. Moreover, financial crime compliance officers and anti-mon-ey laundering (AML) professionals need to demonstrate that they react to and manage negative media alerts relating to their clients.

In a recent enforcement action against Commerzbank, the U.K.'s Financial Conduct Authority criticized the bank for poor AML controls applied to high-risk client relationships and stated, "almost all of the higher risk files had inadequate EDD [enhanced due diligence], with deficiencies such as: limited evidence of meetings with customers; and inappropriate disregarding of negative press coverage."

What is an appropriate process for considering neg-ative media alerts relating to clients? Furthermore, how does the financial crime compliance professional deal with relationship managers who seek to discredit such negative media alerts and defend their clients? It is one of those areas that commonly leads to confrontation and disagreement. While the AML professional suggests such negative media alerts give rise to suspicion, relationship managers demand facts and ask that their client be given the benefit of the doubt.

Innocent until proven guilty?

Many negative media alerts reference allegations or charges in advance of court proceedings and any findings of guilt. Thus, the relationship managers assert such allegations or charges are not proven and should therefore be disregarded. Often, they will say their clients are innocent until proven guilty, but is this actually correct? A person is guilty of com-mitting an offense at the time of doing so, not when a jury determines he/she did so. Prisons are full of people who were apparently innocent until they were proven to be guilty, but the fact is they were always guilty. Of course, there are in-nocent people who are wrongly accused and there are guilty people who escape justice because prosecutors fail to produce sufficient evidence to demonstrate their guilt.

I recollect an instance when upon assessing some nega-tive media alerts I challenged a private banker regarding his African-based politically exposed client, who had twice been acquitted of charges of corruption. His client was a parlia-mentary private secretary; a civil servant; a government em-ployee. In his bank account in London, he held excess of $2 million. I asked the banker if the money in the account was the missing evidence that would have convicted his client of the charge of corruption. The banker said it was family mon-ey but failed to produce any evidence of either the client's source of wealth or the source of the funds. I filed a suspi-cious activity report (SAR) and recommended the closure of the client relationship.

In another instance I was presented with negative me-dia reports that stated a beneficial owner of a correspondent banking client in Latin America had been charged with mon-ey laundering. I wrote to the relationship banker and U.S.-based compliance colleagues seeking a risk management proposal for

the client relationship. The head of correspon-dent banking for Latin and South America wrote back and immediately dismissed the allegations made within what he referred to as a "spurious media article." I replied that the ar-ticle was actually referencing the charges and quotes from a court extract in the United States. The head of correspondent banking did not reply. I closed the London accounts for this bank and filed another SAR.

So how do we, as AML professionals, assess, measure, and manage negative media alerts? Below are some questions you may wish to consider when you next confront a relation-ship manager who disagrees with you and seeks to defend his/her client:

- How old is the media report?
- How many media reports are there?
- What is the nature of the negative media?
- Does the media group have a known political bias that may be relevant to the assessment?
- What are the implications for your firm, if any allegations made within the media alerts are true?
- Are the media reports local, national, or international?
- What is the profile, standing, and reputation of the report-ing media organization/s?
- Has the media source previously been found to have pub-lished false stories or allegations?
- Is the client litigating the media source for publishing the negative media story or false allegations?
- What parts of the media alert align with what your firm knows about the client?
- Has any regulator or government agency taken any action pursuant to the negative media?
- Is there reference to any litigation against the client, either civil or criminal?
- Does the negative media alert propose funds your firm holds that may be subject of a third-party interest, such as the victim of a fraud?
- Has the client already brought the negative media and/or allegations to the attention of your firm and offered a log-ical explanation?
- Does the negative media suggest your firm does not know the client sufficiently?
- Does the negative media alert suggest the client may have misled your firm?
- Is it possible your firm is holding funds for the client that might be tainted by the negative media alert and/or alle-gations?
- Given these matters are in the media, in the public do-main, has the client satisfactorily answered any questions you may have posed, pursuant to the negative media alert and/or allegations?
- Does the negative media alert give you, the AML profes-sional, reasonable grounds to suspect the client may be using your firm to launder money?

Now ask yourself this question: What would you do if as an innocent party you or your firm were the subject of spu-rious, negative media reports and/or false allegations? Has your client done what you would do?

Doing nothing with negative media alerts is definitely not a good strategy. For sure, some reports can be expedi-ently dismissed, because of political motivation or the mi-nor nature of some allegations, but all negative media alerts need to be resolved and be seen to have been resolved, ap-propriately.

Common-sense KYC: Clients should supply the knowledge

I embarked upon a career in financial crime investigations a nd anti-money laundering compliance in 2001, assum-ing I'd be seeking a new role by 2006 because all of the issues would have been fixed by then. Well, it's 2020, and I am st fighting financial crime and money laundering alongside thousands of other people. So, what was wrong? Was it r calculation, or the way in which we have failed to deal wit financial crime and money laundering?

I perceived the business of "know your customer" (KYC) to be a very straightforward process that would logically place the onus upon the customer to provide the required data and keep it up-to-date. I also saw transactions as records connecting ac-counts, customers, and other parties, creating an easy-to-fol-low audit trail. I thought my approach was commonsense, and I have since learned it is ironically not so common after all.

I believe no one knows a customer better than a customer—thus, the customer should provide KYC data and keep it up-to-date. I can hear some of you saying, "But what if a customer lies?" I counter: Did you lie when you opened your bank account?

Let's compare financial services with the airline industry. Both businesses are regulated, accountable to shareholders, and driven by customers, but it is the relationship with the cus-tomers that is the difference. In the passenger airline industry, the airlines and the airports dictate the terms of the relation-ship with the customer, whereas in financial services we have allowed the customer to dictate the terms. We have pandered to their requests and bowed down to their money, hence we are still here wrestling with KYC and account frauds.

There is another area in which airports, airlines, and pas-sengers outperform financial service firms: collaboration. Can you perceive a scenario in which a passenger clears customs; has correctly answered the questions regarding luggage, which has been scanned; then prior to boarding

I am constantly challenged by the notion that as an AML compliance professional I cannot rely upon the KYC process undertaken by a regulator when providing a firm with a regulatory license.

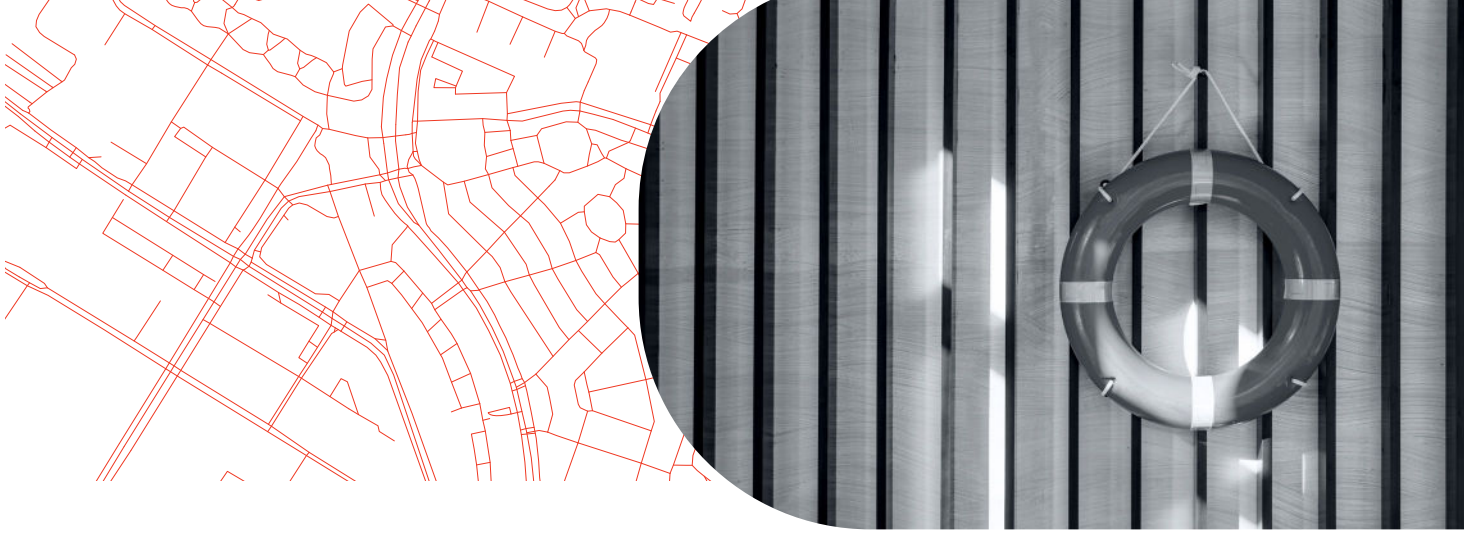
the plane, the cabin crew stops the passenger and poses the same questions regarding the luggage? This does not happen, because if the airline did not trust the airport, it would not land planes there.

In contrast, within the financial services industry, we have historically failed to adequately collaborate, and con-sequently, customers do sometimes face this duplication of questioning and KYC requests. All of which benefits money launderers, because our finite resources duplicate processes applied to legitimate customers.

It is as though we are hostages to a process and have failed to question the benefits and objectives of that pro-cess. I am constantly challenged by the notion that as an AML compliance professional I cannot rely upon the KYC process undertaken by a regulator when providing a firm with a regulatory license.

I reject this and have previously written to a regulator and advised that as the head of AML for a regulated business in London, I was relying upon its KYC of a firm regulated by them. Subsequently, an employee of that regulator telephoned me and stated I could not place reliance upon them. I replied that my letter was a statement of intent to rely upon them, not a question as to whether they would allow me to rely upon them.

The regulator did not expect this reply and protested. I said when I received a letter in which the regulator stated I could



Nothing More Key Than Knowing Your Risk Exposure

Increasingly, governments and regulators are warning firms about hidden and unacceptable risks within supply chains. Now more than ever, firms need to know who they are buying from and selling to, as well as who their vendors and customers are buying from and selling to. Then there are the literal supply chains of logistics: Who is delivering raw materials to you? Who is delivering your goods to the custom-ers and the marketplace?

What was once perceived as a simple bilateral relationship between buyer and seller or vendor and purchaser is no more, but just how far does a firm need to go down a supply chain? And how many chains are there? Retailers are commonly ref-erenced in media allegations of manufacturers paying less than the minimum wage, exploiting children, even slave la-bor. Such allegations are bad for a company's brand as well as its relationship with regulators.

In June, Pakistan International Airlines suspended a number of flights after having discovered that around 260 of the country's 860 active pilots had either fake flying li-censes or had cheated in their exams. Does your firm use this airline to supply goods or to move people from one business unit to another? Did you ever consider a training supply chain?

Of course, this is an extreme case, but it does highlight the primary issue: risk. Risk managers like certainty. Without it, the correct data risks cannot be measured, managed, mitigated, or rejected. It follows that adjacent to risk, there is confi-dence. Which of us has previously perceived there could be a risk within the training of the staff of a third-party supplier? Does anyone believe the Pakistan issue is an isolated instance?

How does this play out in the world of financial crime com-pliance? Does your firm's due diligence extend to the valida-tion of staff training within a respondent bank? Confidence can be provided when firms seek and secure International Organization for Standardization (ISO) ratings and approvals. ISO is a non-governmental organization with 165 member countries as of October that has issued nearly 25,000 interna-tional standards covering all aspects of manufacturing and technology. But do those standards work within your supply chains? Moreover, what and whom can your firm rely upon?

You will by now have noticed this article poses lots of questions and thus far has provided no answers. That is because supply-chain risk management is somewhat sub-jective. While U.K. anti-slavery laws demand firms under-take supply-chain due diligence, and some firms now apply robust know your supplier (KYS) and know your custom-er (KYC) processes, there is no one single answer to sup-ply-chain risk management.

Or is there? I posit that the answer is to take control of your supply chains and demand data from those within it. In the event participants are not prepared to provide any of the data you have requested, you would be wise to cut them out of your supply chain.

Where risk arises in relation to correspondent banking, this should extend to the provision of full KYC data for the

respondent bank's customer. Yes, this is bold, but it is about taking control, securing certainty, and dealing with risk. Notwithstanding the perceived obstacles of bank secrecy and customer confidentiality, this can be achieved by re-questing the respondent bank obtain their customers' con-sent to share the data. Should the request be refused by the respondent bank or its customer, the correspondent provid-ing the clearing services should demand the respondent no longer process transactions through the correspondent on behalf of that customer.

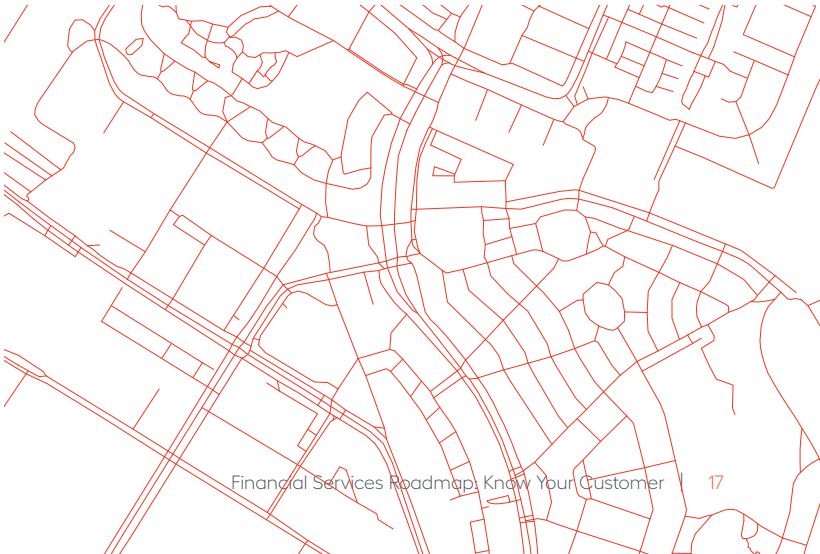
Supply-chain risk management is achieved by taking control, demanding data, and not being blind to any of the risks hidden behind a vendor; a vendor's supplier; a vendor's training provider; a vendor's logistics contractor; or a vendor's auditor.

In the event you determine you do not have control of the supply chain and cannot make such demands of others, identify what else or who else you and your firm might be able to rely upon. These may include the regulated status of third parties, public ownership, transparency, and the long-standing good reputation of a party.

How far up and down these supply chains do you go? That is a matter for you, but do not be intimidated into accepting no for an answer. Do not be deterred by the absence of a di-rect relationship with a party within the supply chain and beware of the usual red flags:

- Newly incorporated companies
- Offshore companies
- Companies providing consultancy services within the sup-ply chain
- Companies owned/controlled by governments/politicians
- Transactions that appear overpriced, underpriced, or illog-ical; or
- Companies in high-risk jurisdictions

In the parallel supply chains running between raw ma-terial providers, commodity brokers, manufacturers, their bankers, customers, regulators, and more you can facilitate the legitimate provision of goods, adjacent to confidence. Such confidence is often drawn from the brands and third parties your firm does business with, buys training from, and supplies services to. Doing business with cheap, but simultaneously nasty, third parties can cause a lot of dam-age to your reputation and your ability to participate in some supply chains.



Analysis: Following the phone trail to detect fraudsters

On July 2 the police in the United Kingdom an-nounced they had made over 600 arrests, seizing more than 70 illegal firearms, including machine guns, as well as 2,000 kilos of drugs and approximately €50 million (U.S. $57 million) in cash. A good day's work, but as with all successful operations, this took months of planning while the arrests took place over a period of just days.

The success of the operation was based on communication. Specifically, the sophisticated interception of the criminals' communications and the robust protection of the communica-tions related to this secretive operation, codenamed "Venetic."

It has now been reported European police forces targeted a communications platform called EncroChat and the devices used by organized crime groups to access and use the plat-form. Law enforcement infiltrated the platform and cracked the code, essentially, by modifying mobile telephones and selling them to criminal groups, who believed they could communicate freely without fear of their communications being intercepted. Wrong.

The recent arrests reminded me of an article I once wrote, which posited that having knowledge of the whereabouts of 100 kilos of cocaine could actually be more valuable than the cocaine itself. I proposed you could sell the cocaine once, but you could sell the knowledge multiple times to multiple buyers. It's a fact: Knowledge equals power and provides an advantage.

When parties are confident they are not being listened to and, more importantly, what they communicate is not being recorded, they talk more freely and often more directly, with code words removed and accuracy taking primacy over secre-cy. This same concept applies to money launderers and their professional enablers: When they believe their communica-tions are secure, they not only communicate more freely, they often do so far more arrogantly.

Nowadays the mobile telephone is central to almost all major criminal investigations, and law enforcement agencies around the world are becoming increasingly more adept with their use and application of data from mobile telephones. Many sophisticated organized criminals are aware of this, and consequently they relentlessly change their numbers and devices. Therefore, when a group of criminals offered a secure communications platform—one that not could not be intercepted—a number of established organized crime groups seized the offering and the handsets.

In the world of compliance, and in particular financial crime compliance and the discipline of "know your customer" (KYC), there is an increasing need to know and undertake due diligence on the mobile telephone numbers of high-risk cus-tomers, as well as other communications they use with your firm/bank. Fraudsters and money launderers may purport to operate from multiple addresses, using a series of false names supported by fake identity documents, but they cannot carry more than 20 mobile telephones with them. Often, the com-mon denominator linking a series of accounts and transac-tions is the mobile telephone and/or the telephone number.

By exploiting this data, firms and banks can better pro-tect themselves against fraud and money laundering; and, please be assured, big firms capture and retain big telephone communication data.

So, just as our governments are now looking at smart-phone applications to support the contact and trace process of coronavirus control, firms should apply similar thinking when the contamination of fraud or money laundering is dis-covered. Check for the mobile telephone numbers, then seek to establish how and when the number contacted the firm/bank and, in reverse, how/when the firm/bank contacted the number. In addition, establish the where and why; how long for; to whom; and by whom. Then isolate the contamination and ensure your systems for communication and KYC know not to do business with or become contaminated by the num-ber or device again.

You see, while names and addresses are often made up, phone numbers need to be accurate, because customers, fraud-sters, and money launderers need to communicate and be com-municated with. As was reinforced with the July 2 arrests, it is often communication that leaves fraudsters, money launder-ers, and other criminals weaker and more exposed.

This crucial weakness, when overseen accordingly, can be a company's greatest strength.

[<?>] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/028/82/PDF/N1902882.pdf?OpenElement
[<?>] https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx
[<?>] https://www.justice.gov/opa/pr/russian-and-syrian-nationals-charged-laundering-millions-us-dollars-designated-russian
[<?>] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/crimea_advisory.pdf
[<?>] https://home.treasury.gov/news/press-release/sm0286
[<?>] http://gtb.societegenerale.com/en/testimonial/future-trends-sanctions-automation-artificial-intelligence-outsourcing-resolve-inefficiencies
[<?>] https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181127_metelics.pdf
[<?>] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685308/financial_sanctions_guidancemarch_2018_final.pdf
[<?>] https://www.bvdinfo.com/en-gb/knowledge-base/videos/compliance-and-financial-crime/how-effective-is-your-sanctions-screening
[<?>] https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160208.aspx
[<?>] https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140903_citigroup.pdf
[<?>] https://www.citibank.com/tts/about/press/2019/2019-0429.html
[<?>] WorkFusion analysis, based on Federal Reserve Check Volume data (https://www.federalreserve.gov/paymentsystems/check_commcheckcolqtr.htm), estimates for non-screened checks and time expended per data extraction and screening.
[<?>] https://fred.stlouisfed.org/series/TLAACBW027SBOG
[<?>] WorkFusion analysis based on data released by the Office of Foreign Assets Control

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. Complianceweek.com

WorkFusion

WorkFusion is accelerating the world's transition to more meaningful work. Our Intelligent Automation solutions are powered by pre-built bots, proprietary artificial intelligence technology and advanced analytics, working together to automate a wide range of business processes. Leading organizations worldwide use WorkFusion to automate their operations with ease and speed, helping them up-skill employees, reduce costs and unlock growth like never before. WorkFusion is headquartered in New York City.

Learn more at **workfusion.com**.