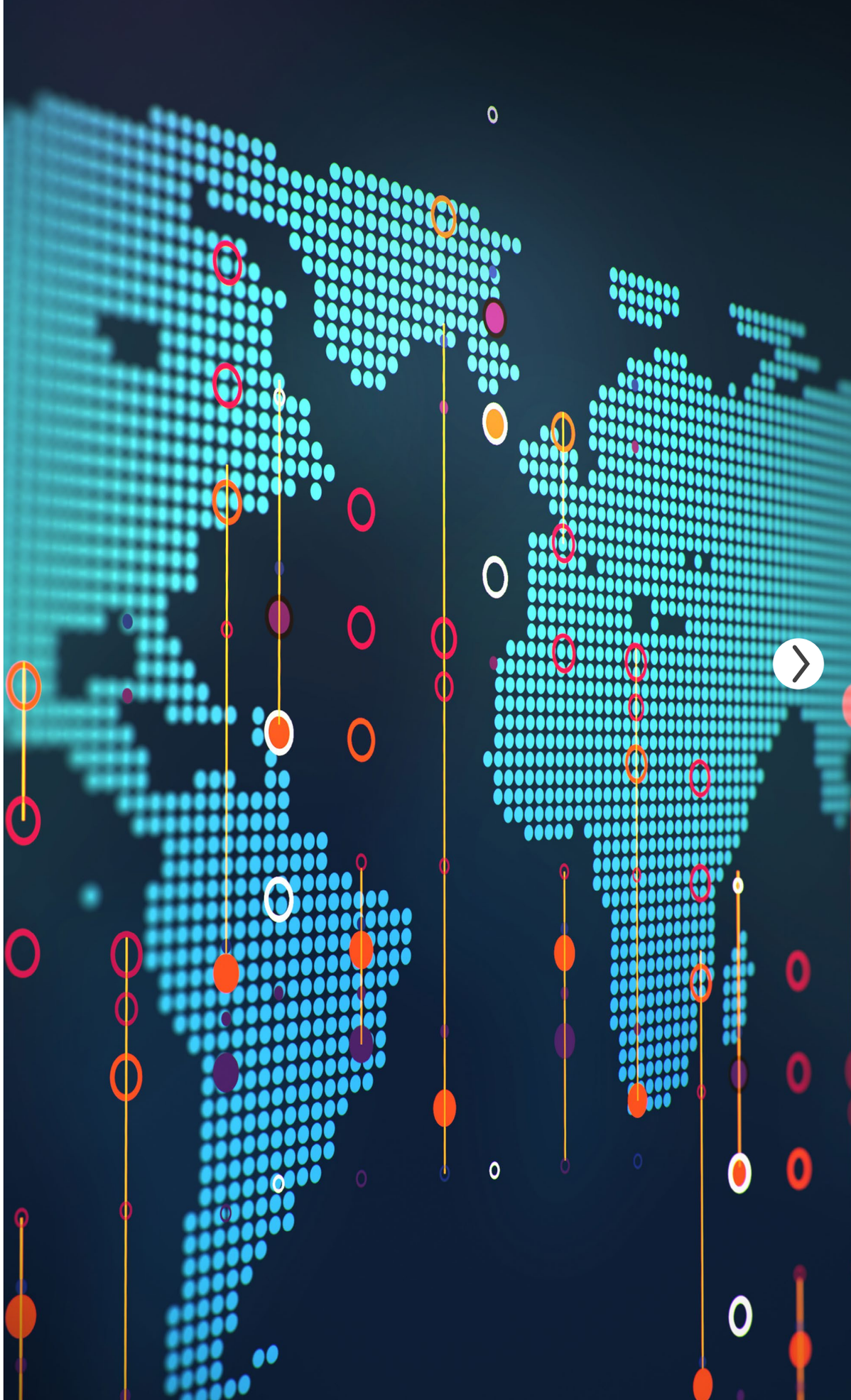
THOMSON REUTERS®

Advantages of a Unified, Automated System for AML/CDD Processes

CONTENTS



Advantages of a Unified, Automated System for AML/CDD Processes

For financial institutions, customer due diligence (CDD) and anti-money-laundering (AML) screening procedures are the first and best defense against criminal exploitation of the financial system.

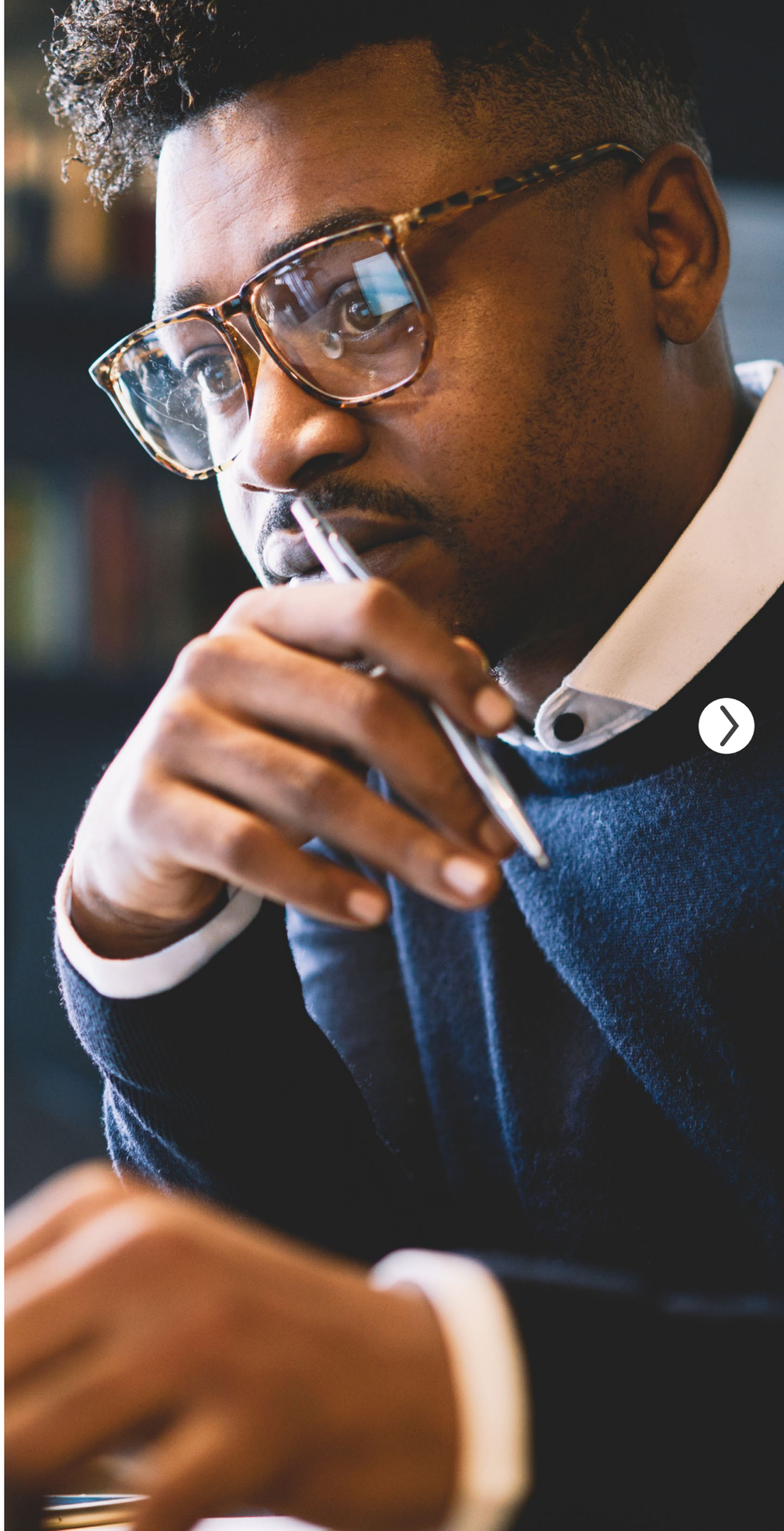
But there are many challenges facing AML compliance teams. In recent years, the digital transformation of global finance combined with regulatory reform, ever-changing sanctions, more severe penalties for non-compliance, and a more technologically sophisticated class of criminals, have all added to the pressures faced by compliance teams. Indeed, the risks associated with inadequate AML/CDD procedures and regulatory non-compliance are now so great that traditional manual processes for customer verification and monitoring are often inadequate.

The case for automation

To minimize these risks and keep pace with the technological evolution of global finance, institutions everywhere are incorporating automated screening technology into their AML/CDD compliance programs. Since passage of the Anti-Money Laundering Act of 2020 (AMLA 2020), the federal government has been requiring financial institutions to accept more accountability for the integrity and legitimacy of their customers, and automated screening technologies offer the means to manage these additional pressures and responsibilities.

Technically speaking, the Bank Secrecy Act (BSA) reforms included in the AMLA 2020 do not require financial institutions to gather any additional information on new customers beyond what is stipulated for normal CDD compliance, but they do significantly increase the penalties for BSA violations. Individuals who work at financial institutions — partners, directors, compliance officers, and other employees — can now be held personally responsible for BSA violations, and enhanced incentives and protections for whistleblowers make it more likely that violators will be caught.

The purpose of these new rules is to encourage financial institutions to treat the risks of money laundering and fraud more seriously, but the law itself does not provide any specific mechanisms for doing so. Procedurally, the important shift to note is a move away from simply reporting anomalous financial activity in suspicious activity reports (SARs) to identifying, monitoring, and managing institutional risk more or less continuously. To accomplish this, the expectation is that financial institutions will leverage available technologies to strengthen their AML/CDD protocols, thereby reducing institutional risk. Manual processes can still be used, but unless significantly more personnel and training are devoted to AML compliance, manual processes alone can't do much to reduce an institution's AML risk profile.



The benefits of automation

Human error is always possible with manual AML/CDD processes, of course, but they can also be time-consuming, expensive, and slow. Today's rapidly moving financial landscape often requires real-time data collection and analysis, which is why many forward-thinking institutions are supplementing their AML/CDD processes with automated screening technologies that provide continuous, comprehensive AML protection.

Now, most automated screening tools use some combination of machine learning and artificial intelligence to locate, collect, analyze, and display results, but this in no way diminishes the importance of human judgment in assessing risk and determining action. The proper role of automation in the AML/CDD process is to support and strengthen the efforts of an institution's compliance team, not replace it. Indeed, institutions that make the most effective use of automation are the ones that integrate it into their compliance processes as a reliable informational backstop, ensuring that nothing slips through the cracks.

Among the benefits of automated screening technologies are:

- 24/7 transaction monitoring
- Instant data extraction and analysis
- Automatic flagging of suspicious financial activity
- Reduced need for manual data entry
- Clean, accurate, curated data
- Ability to adapt and scale to request volumes
- Continuously updated global sanction lists
- Up-to-date risk assessment tools
- Flexible risk parameters
- Fewer false positives and other errors
- An audit-ready record of investigative activity

Trust but verify

Given the advantages of automated AML/CDD screening, one might be forgiven for assuming that all financial institutions use it — but they don't. According to a recent Thomson Reuters® poll of more than 250 AML/CDD professionals, about half (53%) of those surveyed use a third-party software solution for sanctions screening, and less than half (42%) use a third-party screening tool for searching public records and adverse media.

Today, as always, the most common way for financial institutions to gather AML/CDD information is through a personal dialogue between the customer and a bank employee. No machine can replace face-to-face interaction with a customer, nor should it. Nevertheless, the industry trend in risk management is toward less reliance on personal relationships with a customer and greater emphasis on multi-faceted assessments that include technological corroboration of customer-provided information. Indeed, only 44% of survey respondents in the 2021 survey reported relying on face-to-face encounters with customers as their primary form of AML/CDD information gathering, down from 53% in 2019.

Regardless, nothing can replace looking a new customer in the eye and, over time, developing a personal relationship with them. Among other things, the relationship between a customer and their bank is based on a certain amount of trust — trust that the customer is who they say they are, and that their finances are obtained legally.

Where third-party software screening can help is as a "trust but verify" tool to ensure that the information provided by the customer is true. If a customer is trustworthy, there should be no problems. But if the customer is in fact hiding information from their financial institution — particularly about where their money is coming from or ownership information about the business they claim to represent — then AML/CDD software screening can be the difference-maker between protecting the institution and being fooled by a clever criminal.

Streamlining verification

Interestingly, though adoption of third-party screening software is far from universal, almost half of respondents in the Thomson Reuters survey (43%) also said that "streamlining business processes" is their highest priority. And it so happens that one of the best ways to streamline AML/CDD verification is by implementing software screening at key junctures in the process, particularly at the beginning of a customer relationship, or onboarding.

In a manual onboarding approach, compliance personnel must spend time searching court and property records, business records, sanction lists, politically exposed persons (PEPs) lists, social media, and news sources for indications of criminal activity or suspicious financial behavior. If they find it, they must re-double their efforts and gather even more information to determine whether and to what extent the applicant represents a risk to the institution.

With automated screening software in place, bank representatives can simply type in a name and allow the software to search relevant records. In addition to being much faster, automated searches are much more comprehensive than manual searches, so compliance teams and regulators can be confident that no information was overlooked. Furthermore, the institution can set acceptable risk levels and the software will automatically score an applicant based on those risk parameters. If an alert is triggered, the problematic criteria are flagged, allowing compliance officers to focus further investigation on the areas in question.

Used in this way, screening software enables compliance teams to quickly identify legitimate applicants and free up more time to verify information on customers that have been flagged as higher risk. It also saves time and money by reducing the number of false positives (for suspicious activity) that a compliance team must investigate.

Additionally, customers who pose a higher risk of money laundering and terrorist financing trigger the need for enhanced due diligence (EDD), which requires reviewing and gathering even more information on the customer, more frequently, in order to understand the nature and purpose of their transactions. Screening software can't collect all the information necessary for EDD purposes, but it can scan for the legitimacy of business addresses, personal addresses, sanctions violations, evidence of synthetic identities and fraud, cybercrime, and other indicators of suspicious activity. Furthermore, it can continue to monitor all of these potential flags simultaneously, using real-time data, allowing examiners to respond immediately to any suspicious transaction activity.

Expanding options

Another way screening software can help financial institutions create more efficient processes is by giving the organization's management more options.

For example, many institutions channel all their AML/CDD work through a dedicated risk-management team. But in most mid-to large-size institutions, the majority of new customers represent little or no significant risk, so burdening the risk-management team with piles of routine verifications can be counterproductive. If the team is slow to respond, the customer experience may also be compromised. But if front-line employees and other departments are trained to use screening software, they can verify the legitimacy of most customers themselves, simultaneously improving customer service and allowing the risk-management team to focus its energies on the most alarming or problematic cases.

Broad-based use of screening software across an organization also ensures that everyone is using the same authentication criteria, whereas the accuracy and thoroughness of a manual search depends largely on the skill of the individual investigator, which varies. Furthermore, standardizing authentication criteria helps make the review process more consistent and allows for clearer, more accurate communication between departments. Over time, these criteria become so engrained in the culture that they serve as a kind of institutional shorthand, allowing everyone to operate more efficiently. If a review or audit is necessary, all the relevant customer information is also housed in one place, allowing for quick and easy report production.

Improved data quality

Another enormous advantage of a well-developed third-party screening program is the quality of the data it draws on for authentication. The best programs not only scan court records, watch lists, social media, and other publicly available information, they also have access to proprietary databases that include global corporate records, beneficial ownership information, and more, all of which is essential for a modern, state-of-the-art AML/CDD program.

At Thomson Reuters, for instance, the company's CLEAR investigative tool has access to proprietary databases that are continuously updated, allowing financial institutions and other corporate entities to assess their risk exposure more effectively across multiple parameters, and to comply with increasingly complex government regulations.

Sanctions, for example, are in constant flux around the world, so much so that keeping up with them is virtually impossible for even the most dedicated compliance officers. The same goes for PEPs lists, terrorist watch lists, Ultimate Beneficial Ownership (UBO) lists, and other key sources for identifying suspicious financial activity, criminal associations, and other risks. But with a program where all of this data resides in the background, users have at their fingertips a uniquely powerful and accurate tool for AML/CDD research and verification.

Beneficial ownership verification

For financial institutions, such capabilities are essential because of the increasingly complex nature of AML/CDD work and the growing technical sophistication of fraudsters, money launderers, and other criminals intent on exploiting weaknesses in the system. One of those weaknesses has to do with the use of shell companies to hide business-owner identities and/or associations with criminal and terrorist networks of various kinds.

In accordance with the AMLA 2020, financial institutions are now required to be much more diligent about identifying beneficial ownership of their customers' businesses, but that doesn't make the information any easier to verify. Indeed, because of the increased regulatory scrutiny around beneficial ownership, AML/CDD professionals in the previously mentioned Thomson Reuters survey confirmed that identifying beneficial ownership is now the most sought after information for reducing AML risk, followed by enhanced watch lists scans, PEP checks, and ongoing screening for adverse media. The U.S. government's Financial Crimes Enforcement Network (FinCEN) is in the process of creating a registry of legal entity beneficial owners that will eventually make confirmation of business ownership much easier — but until the registry is operational, financial institutions must rely on their own resources. And even so, the registry will require customers to give their consent before an institution can use it for verification, so third-party records will still be important in many instances.

Where a robust screening program can help is not just by checking beneficial ownership information provided by the customer, but also by scanning all available information sources for possible associations with known criminals or suspicious persons, or with people known to associate with them. In advanced programs, known associations can be plotted on a three-dimensional orbit chart to give compliance officers a visual representation of the frequency and type of interaction their potential customer has had with any suspicious persons.

Now, it is possible to access much of the same information through targeted standard searches if one knows where to look — but again, it can take several hours for a human being to hunt such information down, and even if they do, there is no guarantee that an important piece of information won't be missed. The advantage provided by screening software is that it can use advanced data analytics to drill down and identify patterns of suspicious financial behavior that may not be apparent at first glance.

For example, today's technology tools can instantly identify connections a subject has to others through shared connections in various records — e.g., phones, addresses, business holdings, shared executive leadership, real estate, and vehicles, to name a few. And because it can quickly analyze so many more data points than a human investigator using conventional search tools, screening software dramatically reduces the risk that a bad actor is going to succeed.

Monitoring for risk

Yet another requirement of regulatory authorities is that proper risk-based AML/CDD procedures should include ongoing monitoring of the customer relationship and, when necessary, updates of the customer's information. If any new information can potentially alter the customer's risk profile, the financial institution is obligated to reassess the customer's risk profile and, if necessary, change it.

One common reason for changing a customer's risk profile is if their financial activity is suddenly inconsistent with the institution's understanding of the nature and purpose of their business, or if any new information — such as a subpoena, adverse news event, or business ownership change — could have an impact on the customer's risk profile. Technically speaking, however, the requirement for "ongoing" monitoring does not mean that the monitoring has to be continuous, only that there are policies and procedures in place to determine whether and when periodic reviews to update customer information should be conducted.

Unfortunately, periodic reviews open windows of opportunity for bad actors to act badly, and manually revisiting data on things like court records and adverse media can turn into a cumbersome, fruitless search for needles of important information in haystacks of irrelevant material. Nevertheless, many financial institutions still rely primarily on manual AML/CDD verification for updates, potentially opening their organization to unnecessary risks.

If an automated screening program is incorporated into an institution's AML/CDD program, however, a customer's risk potential can be continuously monitored according to whatever risk parameters the user sets. If any suspicious or anomalous financial activity is detected, it is instantaneously flagged. If any court notices or other public information related to the customer or their business becomes available, it too will be flagged as soon as it is filed.

The fact is, always-on, 24/7 screening software can detect anomalous transaction patterns much sooner than a human being, and it can serve as the eyes and ears of the institution when its human eyes and ears are sleeping or otherwise engaged. And unlike periodic manual inquiries, screening software's access to real-time data makes it possible for institutions to stay ahead of potential risks rather than fall prey to them after the fact.

The CLEAR choice

If you've read this far, it should be obvious that automated screening software not only offers several advantages over manual AML/CDD screening procedures, it can also help compliance teams make the most of their limited time and resources. Efficiency and cost-effectiveness aren't the only benefits, either. Used as a complementary tool to reduce the time-intensive burden of conventional search engines, a well-designed screening program can and should enhance a compliance team's overall effectiveness, mitigating risks to the organization that might otherwise result in fines, penalties, or lost revenue due to fraud.

Not all screening programs are the same, however. Many are little more than conventional search engines customized for basic CDD compliance, and are only designed to perform basic search functions, not evolve with the needs of the organization.

Thomson Reuters CLEAR anti-money laundering tools are in another class altogether. Within the CLEAR suite are two AML/CDD modules, ID Confirm and Risk Inform, that utilize advanced machine learning to scan public and proprietary records, using live data for up-to-the-minute search relevance. These modules then employ sophisticated analytics to synthesize and display customer data in forms that are easy to understand at a glance.

For example, numerical risk scores are color-coded green or red to indicate whether a pre-determined risk threshold has been crossed, and alerts for every risk category — e.g., address confirmations, synthetic identities, adverse media, etc. — can be easily viewed on a single dashboard. Hard-to-find data from different search universes — e.g., live adverse media and financial crime/sanctions screening — can also be cross-referenced and scored for risk. Furthermore, drill-down options allow users to display individual, batch, and ongoing monitoring results in easy-to-read graphics, not just lists, saving investigators time and improving the accuracy of data interpretation.

Taken together, these features provide a thorough, multi-dimensional picture of each customer's risk profile, and all customer profiles are accessible through a single, easy-to-use interface.

Thomson Reuters programs aren't static, either — they are backed by teams of editors and engineers who work in the background to make sure that all state and federal laws are integrated into the system, all sanctions and watch lists are up to date, and all proprietary databases are continuously curated. Customizable design options and flexible search parameters also allow users to create a tool that fits their needs and integrates seamlessly with the institution's larger ERP systems.

The CLEAR choice *(continued)*

Important features of CLEAR:

- Reduces operational risk
- Protects against fraud
- Improves compliance team efficiency
- Detects suspicious transaction patterns 24/7
- Minimizes false positives
- Imports and analyzes data from multiple sources
- Automatically updates regulations, sanctions, and watch lists
- Utilizes proprietary databases
- Monitors live data in real time
- Creates a fully tracked investigation trail
- Generates a dynamic database of customer risk profiles
- Improves investigative speed and accuracy

There are other programs, but Thomson Reuters CLEAR is the best choice for financial institutions that need a state-of-the-art AML/CDD program capable of protecting the organization, improving compliance, and keeping pace with the increasingly complex technological demands of 21st-century finance.

THOMSON REUTERS®