Thomson Reuters Institute

Financial Institutions & Know Your Customer Rules

From security to solutions

THOMSON REUTERS®

Financial Institutions & Know Your Customer Rules: From Security To Solutions

To paraphrase a great speaker, your reputation and integrity are more important than money. This has never been more accurate.

Beyond the security of their liquid capital, financial institution, in order to thrive, must have a reputation to grow customer trust and the integrity to act in accordance with compliance regulations in order to not run afoul of rule and to prevent massive fines.

Increasingly, global regulators are focusing on a certain aspect of this dynamic, know your customer (KYC) rules, as a way to ensure financial institutions across the world are not offering their banking services to illicit actors. As global financial crime only increases worldwide, with a big boost in such illegal activity seen during the years of the global pandemic, more and more scrutiny will be placed on how financial institutions determine the real identity, suitability, and financial sophistication of their banking customers.

> ***KYC is here to stay, and its compliance likely will only become more stringent.***

In a new white paper published by the Thomson Reuters Institute and Thomson Reuters Regulatory Intelligence, we look at how KYC rules are playing a bigger role in the compliance and security of financial institutions and the challenges that institutions are facing in getting in compliance with KYC rules both in the United States, the United Kingdom, and around the world. Finally, we'll see how some institutions and financial third parties are looking for solutions, either by creating new tech products or by outsourcing, to make their KYC challenges more efficient and cost effective.

Indeed, KYC is here to stay, and its compliance likely will only become more stringent. Financial institutions who fail to take this message seriously are in for a mess of consent orders, bad publicity, and fines, among other negative impacts.

KYC gains bigger national security role

While it is always important to follow proper protocol, during in a time when political controversy, social responsibility, and strong sanctions are at peak visibility it becomes especially critical. Anti-money laundering (AML) authorities around the world are in the midst of a push to enhance KYC measures as Western nations seek to use economic sanctions to hold Russia accountable for its invasion of Ukraine. The sanctions are an unprecedented move to isolate Russia from the world economy, and such a massive response in tight timeframe increases the risks and responsibilities that financial institutions face.

KYC measures include requiring that financial services firms and other professionals work to reveal the true, or beneficial, owners of legal entities used in transactions, and a common key to their success is preventing Russia from using shell companies to obscure the ownership of Russian-linked firms. The KYC measures pursued by the U.S. government and international bodies aim to pierce the vast network of shell companies and hold their enablers liable.

Institutions are aware of not only the ever-growing financial crimes and sanctions risks they face, but also the reputational damage that could ensue if KYC missteps help fuel Russia's war machine or enable the flow of corrupt funds.

Institutions are aware of not only the ever-growing financial crimes and sanctions risks they face, but also the reputational damage that could ensue if KYC missteps help fuel Russia's war machine or enable the flow of corrupt funds. Against this backdrop, firms' KYC efforts have attained geopolitical importance and become crucial to national security.

Further, these new responsibilities are being imposed on a changing financial services industry, with cryptocurrency players and other financial technology firms seeking to make payments happen more and more quickly, despite yet-to-be-addressed compliance challenges, as well as AML and sanctions compliance. Indeed, some traditional financial services firms are still struggling to meet existing KYC obligations even as the international Financial Action Task Force (FATF) is pushing for more exacting standards and regulation.

"Many financial institutions struggle to access a single source of information that helps them develop a comprehensive view of each client," SWIFT, the international system for financial messaging and cross-border payments, states on its website when describing challenges associated with KYC information. This can lead to significant costs associated with satisfying regulatory requirements and may also affect risk, SWIFT adds.

The United States, which has led the sanctions effort against Russia, is now drafting rules to improve the identification of the true ownership of tens of millions of legal entities, in a push to combat criminal abuse of shell companies. In late September, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a final rule laying out which legal entities will be required to report their beneficial ownership data to a U.S.-established registry, beginning on January 1, 2024.

The rulemaking push was required by the U.S.'s Corporate Transparency Act, part of the Anti-Money Laundering Act of 2020, with the Ukraine crisis giving the requirement new urgency.

The legislation had suggested that financial institutions would be able to access the non-public registry with their customers' permission — which could make it easier for them to understand their customers' true ownership. FinCEN, however, has yet to issue rules outlining such access. Nor has the agency said how the new database will affect financial institutions' own obligations to collect beneficial ownership information from customers, as required under an earlier customer due diligence (CDD) rule. And it has been suggested that FinCEN may not amend the CDD rule, which took effect in 2018, until 2025.

Some AML compliance professionals had been optimistic after the Corporate Transparency Act was passed that they would be relieved of their requirement to collect beneficial ownership information or at least would be granted unfettered access to the registry to aid their KYC collection efforts.

More recently, however, sanctions evasion by Russia and its public- and private-sector allies has landed squarely in the crosshairs of U.S. law enforcement authorities. Some AML professionals are now concerned Treasury's beneficial ownership database may ultimately *add* to their compliance burden. For example, they wonder what their additional obligations will be if there are discrepancies between the beneficial ownership information clients provide and the data they report to Treasury.

Push for transparency

The U.S. financial crimes agenda is part of a wider international push toward greater transparency.

In October, FATF members released draft guidance for implementing an international standard on beneficial ownership transparency. And U.S. Treasury Secretary Janet Yellen touted FATF's plans as "vital steps to combat corruption, strengthen recovery of assets stolen by corrupt officials and other illicit actors, and improve beneficial ownership transparency."

Advances in technology may help firms mend their KYC nets to a degree, but regulatory pressure — and, indeed, financial penalties — will only grow, along with pressure to increase transparency and root out corruption and other illicit activity.

Banks' AML & KYC efforts hampered

Banks' failure to collect basic KYC data and their tendency to track and manage high-risk customer due diligence manually using spreadsheets is hampering their AML efforts across the world.

Banks are also performing poorly on financial crime risk assessment, and that has led to mistakes when risk-rating clients. It also means that the automated systems they do have for transaction monitoring are unable to adapt to detect new risks.

> ***"We also see instances where there are significant discrepancies in how the rationale for specific risk ratings are arrived at and recorded by firms."***
>
> ***– U.K.'s Financial Conduct Authority (FCA)***

Deficiencies highlighted

In Europe, the U.K.'s Financial Conduct Authority (FCA) has highlighted deficiencies in client onboarding, client due diligence and enhanced due diligence, as well as risk assessment and more in the last 18 months. Business-wide risk assessments the FCA reviewed were "generally poor", with insufficient detail on the financial crime risks to which the business was exposed. The FCA observed a lack of consistency in customer risk assessment.

"We also see instances where there are significant discrepancies in how the rationale for specific risk ratings are arrived at and recorded by firms," the FCA said in 2021. "There is often a lack of documentation recording the key risks and the methodology in place to assess the aggregate inherent risk profile of individual customers."

For example, the FCA's 2017 final notice fining Deutsche Bank for AML systems and controls failures related to laundering $10 billion through Russian mirror trades illustrated shortcomings that still linger today. The bank's customer and country risk-rating methodologies were "inadequate," the FCA said. And the bank had underestimated customers' AML risk, categorizing fewer than 5% as high-risk, which the FCA said was "significantly out of line with its peers."

Further, Deutsche Bank's U.K. team developed its AML country risk ratings using an "informal and opaque methodology and the ratings were then implemented globally," the FCA said. Such "home-cooked" risk-rating methodologies of this kind are far too common, AML officials said. Deutsche has since changed its methodology.

Manual processes

The 2017 final notice also found that Deutsche Bank lacked automated AML systems for detecting suspicious trades. Its AML team took steps to investigate the mirror trading but did not obtain all the relevant trading data that would have "shown the full extent of the trading and the potential for mirror trades to be used to facilitate large-scale money laundering" because of their over-reliance on manual processes.

In fact, banks' continued reliance on spreadsheets and other manual processes means their approach to financial crime compliance and detection lacks coherence and consistency. Tracking thousands of high-risk clients on a spreadsheet and then relying on it to drive continuing CDD contributes to poor outcomes.

> ***Spreadsheets are not conducive to tracking changes in client behavior or bringing any consistency to continuing due diligence.***

"We often identify instances where CDD measures are not adequately performed or recorded," the FCA said in 2021. "This includes seeking information on the purpose and intended nature of a customer relationship (where appropriate) and assessments of that information."

Some banks have moved only relatively recently from relying on boxes of paper client records to spreadsheets. Management tends to opt for the manual approach to save money, AML officials said.

It is not possible to track clients effectively using spreadsheets for AML and KYC purposes, however. For one, spreadsheets are not conducive to tracking changes in client behavior or bringing any consistency to continuing due diligence. Yet few banks have invested in workflow technology that could bring more consistency and assurance to client on-boarding, KYC obligations, or continuing due diligence and client management, particularly when it comes to high-risk clients.

Managing financial crime policies through spreadsheets and static documents such as PDFs posted on an intranet portal means policies and guidance are difficult to access or may not be current. Those bank officials who are in charge of on-boarding customers might not be aware of new guidance or policy changes, and there can be confusion between jurisdictions. This makes it hard to take a consistent approach to financial crime risk assessment, KYC, and client on-boarding.

Proper sanctions screening

Manual processes have come up again in recent months, this time related to sanctions screening. The FCA found "varying levels of adequacy" when assessing firms' sanctions compliance, and much of that hinged on whether firms are using manual or automated screening systems.

"Issues we have identified tend to be around the effectiveness of firms' customers' sanction-screening processes, at on-boarding and on an ongoing basis, with some weaknesses also found in firms' approach to real-time payment screening," Nikhil Rathi, the FCA's chief executive, wrote to the Treasury Select Committee in July.

The FCA had written to firms that use manual sanctions-screening tools to remind them to have "well-established and well-maintained systems and controls to counter the risk of their business being used to further financial crime, including evading sanctions," Rathi said.

Seeking solutions

As KYC and its obligations become a growing compliance challenge, some financial institutions and others are looking for solutions — either by creating new technological products or innovative processes, outsourcing, or by establishing dedicated KYC units, in order to more easily and cheaply address their KYC challenges.

THE COST & EFFICIENCY OF OFFSHORING FINANCIAL CRIME SYSTEMS

Among potential solutions, another controversial option is sending much of the financial crime work offshore. It is seen as a quick fix. Institutions wish to simply "throw bodies" at the problem and have a huge staff with the assumption that the proper screenings will be done. Without proper training and other checks and balances, however, this solution can cause more problems than it fixes.

Firms have underestimated the challenges attached to delivering effective financial crime systems and controls from low-cost centers offshore. It is slowly dawning on some that throwing bodies and money at the problem has not achieved the desired results.

In many cases, the move to offshore centers did little more than industrialize firms' inadequate financial crime risk management frameworks.

Regulators have noticed as well. They point to a lack of consistency in checking suspicious transaction alerts and say client on-boarding safeguards are poor. In response, some firms are now seeking to standardize their offshore financial crime capability to achieve greater consistency and higher-quality outcomes.

In many cases, the move to offshore centers did little more than industrialize firms' inadequate financial crime risk management frameworks. In addition, offshore teams — largely used to check suspicious transaction alerts and conduct KYC checks — do not always receive adequate training. High staff turnover is another problem.

It is not enough simply to set up an offshore center and leave it to run. Financial crime risk requires constant reassessment, and risk management frameworks often need to be recalibrated.

Standardizing capabilities

Now, some financial service firms have begun to study ways to improve processes and performance in offshore centers.

"The standards vary a lot between people, teams, and from one center to another, and especially for a large organization this creates significant inefficiencies, rising costs, and represents a serious problem," said Gabriel Cozma, head of Lysis Financial and Fintech at the Lysis Group in the U.K. "This is a trend that is going to continue in the market, which calls for the standardization of capabilities."

Firms wishing to standardize their offshore financial crime capabilities need to measure teams' performance, daily, if necessary, to ensure they are performing close to their best, Cozma said. Once firms can measure performance, they can intervene and, where necessary, reshape the way people and teams work, and how they themselves interact with offshore centers, he added.

Firms also should take time to analyze problems, such as systems access and resilience, which may be hindering analysts' ability to get through their allotted workload. Illness-related absences — an outbreak of COVID-19, for example — could require a quick shift of resource from one center to another. Also, analysts may suffer from screen fatigue after looking at alerts all day, so one solution might be to vary tasks.

As noted above, the FCA has pointed out retail and challenger banks' deficiencies in checking suspicious transaction alerts twice in the last 16 months. Many of these transactions will have been checked by employees based in offshore centers, some of whom are expected to check alerts within 18 seconds.

FCA reviews found inadequate handling of transaction monitoring alerts, including "inconsistent and inadequate rationale" for discounting alerts, a lack of holistic reviews, and a failure to record basic information in investigation notes.

Turnover, personality type & training

For many working in offshore centers, it is their first job in financial crime detection. Not all these hires, even if they eventually come to have a good knowledge of the task at hand, will be suited to this work. It is repetitive and frequently boring, which probably contributes to high turnover, making it difficult to retain continuity and expertise.

Firms seeking to bring standardization and consistency to AML and KYC should also look at the types of people they hire and whether there are certain people who may be better suited to perform these tasks, Cozma said, adding that Lysis's financial crime operations in Cape Town, South Africa will often hire candidates with psychology backgrounds, for example, because they are good at picking up behavioral patterns.

The level of inconsistency creates hazards and, in many ways, does little to properly identify KYC information or track the concerns from an AML perspective. In fact, even after you consider all these methods of tracking, identifying, and screening KYC information, a gap remains in finding a way to properly "de-bank" entities or deciding if that is even the correct course of action. De-banking denotes a situation in which a large financial institution withdraws banking services to a business for any number of reasons — commercial, or regulatory, such as compliance with counter-terrorism financing or AML laws.

NEW YORK FACIAL RECOGNITION COMPANY LAUNCHES KYC TOOL

With increase regulatory oversight and financial risk, the financial sector is looking for new and innovative solutions to minimize risk and gather a full picture of their customers. Some companies are looking at options that include more thorough screening of the data that is provided by the customers, while other entities are looking at the individuals who are providing the data. This leads to in-depth discussions of technology that uses facial recognition, which stirs its own controversy.

A New York facial recognition technology company fined by data privacy regulators in the European Union (E.U.), U.K., and Australia is trying to turn the corner by relaunching as a KYC, anti-fraud, and security tool. However, the bid by the company, Clearview AI, for a fresh market faces legal risks posed by an ongoing class action privacy complaint for its use of facial images to train the artificial intelligence (AI) behind its tool.

The controversy calls into question whether the new product's algorithm was trained on improperly obtained data, although the company denies it was. These legal and ethical questions highlight risks that many financial firms may face as they turn to technology solutions and vendors to assist with KYC compliance and other security tasks.

In May, Clearview AI was banned from selling its faceprint database commercially throughout the United States after it settled a lawsuit brought by the American Civil Liberties Union (ACLU), which argued that Clearview's practices violated Illinois' Biometric Information Privacy Act (BIPA).

Clearview Consent, a facial recognition algorithm, was launched less than two weeks after the Illinois/ACLU settlement. The algorithm is being marketed on a standalone basis for uses including travel identity checks, in-person payments, online identity verification, and fraud detection.

It would be logical to assume that Clearview trained the algorithm on the unique database of faceprints it had amassed, in which case national or state regulatory authorities should order Clearview to delete their algorithm and start again with clean data, said Nathan Freed Wessler, deputy project director of the ACLU Foundation's speech, privacy, and technology project in New York.

Clearview said, however, that its algorithm had been trained on publicly accessible images from the open internet. "No private data has been used to train Clearview AI's bias-free algorithm, and no personally identifiable information is used before or during the training process," said Hoan Ton-That, Clearview's chief executive. "After the algorithm has been created, no personally identifiable information or photos are included with it."

Many data-privacy regulators consider it impermissible to scrape photos from the public internet without consent. They view photos posted online as personal data, subject to data privacy laws. Facebook and other social networks have asked Clearview AI to stop scraping data from their sites because the process does not comply with their terms of use.

If Clearview Consent's algorithm was trained on improperly collected facial images, there is legal precedent for the U.S. Federal Trade Commission (FTC) to order the algorithm to be wiped. In 2021, an FTC settlement with a company called Everalbum alleged the company had misled its app users by saying that it would not apply facial recognition technology to user content unless they "affirmatively chose to activate the feature." Instead, the company automatically activated the feature regardless, and it also failed to delete photos and videos after users deactivated accounts.

Choose third-party solutions with care

Financial service firms should consider privacy, operational, reputational, and compliance risks associated with facial recognition technology firms in addition to the legal risks. They should only be using face-recognition technology if they have the expressed consent of the people upon whom it is being used, Wessler said.

Facial recognition technology remains controversial, particularly because it tends to perform poorly when identifying non-white, non-male faces. Clearview claims to be bias-free and rates itself as highly accurate, citing U.S. National Institute of Standards and Technology's benchmark test results.

Enforcement action as well as Clearview's own attempts to comply with local data privacy laws demonstrate the difficulty of auditing its database, which cannot prove or guarantee requests to delete personal data submitted by data subjects or regulators. For example, if a data subject is in a jurisdiction that permits requests to opt out of the database, they must provide a photo for the company to check against the database. A Californian data subject, for example, would then receive a message sent on behalf of Clearview saying the company had processed the request successfully. It does not show what images have been deleted.

The problem is that Clearview indiscriminately scrapes personal data from the internet, Wessler said. The company in February told investors it was aiming to have 100 billion facial images in its database within a year.

"If the deletion requests are to have any durability, then they need to be able to screen all the newly downloaded photos to see if they're getting new photos of somebody who has tried to opt out," Wessler explained.

Under the terms of the Illinois settlement, Clearview keeps the uploaded photos, and segregates them from its national database that police or other government agencies could use. That allows the company to scan periodically against the new images to check it is not adding images of people who are in Illinois.

Financial resilience is another consideration when assessing third-party vendors.

Clearview has incurred about $31.5 million in fines for data-privacy regulation breaches. Italy's data privacy authority fined Clearview €20 million in March, while in May the U.K.'s Information Commissioner's Office fined it £7.5 million. Clearview has also been sanctioned by Australian and Canadian data privacy regulators and is also facing a class action complaint based on Illinois' BIPA, initiated by a Macy's department store customer from Chicago.

Remediation and legal costs will also eat into its capital. Public records indicate it has raised about $40 million in venture capital.

Considering how controversial and extensive this innovative technology is, it is not surprising that it is one of the many reasons there are large screening gaps. Depending on the institution, the reasons vary — from not having the budget to not being willing to spend the money as it is not a priority — for failing to adequately address this problem. And unfortunately, this lack of prioritization comes at a large cost.

AUSTRALIAN BANKS EYE NEW FINANCIAL CRIME UTILITY

In another solution to KYC compliance challenges, Australian banks are planning a new financial crime compliance utility to tackle de-banking, while also cracking complex money laundering threats. Support for such a utility from some of the country's largest banks may help the initiative succeed where previous attempts have failed.

The push follows the success of Fintel Alliance, the country's first private-public partnership launched by Australian regulator AUSTRAC to combat money laundering and terrorism financing. Fintel Alliance's success has broken new ground in the fight against financial crime by bringing together a tight-knit group of public and private sector partners.

Information and data sharing are critical to the success of modern AML efforts, said Caitlin Tanumyroshgi, head of financial crime intelligence at ANZ Banking Group in Melbourne. A financial crime compliance utility would allow anonymized information to be used by different entities to get a broader perspective and form a higher-level view of a problem or threat, she said.

There had been concern that the introduction of an AML utility could compound the de-banking problem, with information-sharing leading to people being locked out of the system. The opposite was likely, Tanumyroshgi explained, because access to more data would reduce de-banking by giving banks a more accurate view of what was happening. Decisions are often based on limited information because criminal entities bank at many several different banks.

Better risk assessments

A financial crime utility would also enable banks to make more accurate customer risk assessments. They could ask questions about pre-reporting and pre-suspicion before the de-banking stage.

The Fintel Alliance is limited to a small group of sophisticated participants but the push to develop a financial crime utility would enable the benefits to be shared across the reporting entity population. The main benefits would include collaboration to beat organized syndicates, using analytics and pooled data, streamlining regulatory processes, reducing costs, and sharing knowledge.

It would also provide reporting entities with a forum through which to present a shared industry perspective on legal or regulatory reforms, said Neil Jeans, founder of consultancy Initialism in Melbourne.

A financial crime utility would be able to combine data across multiple financial institutions, Jeans said, adding that the anonymized nature of the information-sharing meant the proposed utility model would be unlikely to aggravate customer de-banking.

"I don't think we'd be looking for particular customers across multiple institutions unless there's an issue that's being identified," Jeans said. "That data is anonymized, so nobody knows who the customer is... they simply know there's a problem that multiple organizations have."

Benefits of cooperation

Recent Fintel Alliance projects have demonstrated what information-sharing can achieve. The organization has led projects on child sexual exploitation, fraud against the National Disability Insurance Scheme, preventing domestic payment abuse, identifying forced sexual servitude, and illegal phoenixing activity, in which a new company, for little or no value, continues the business of an existing company that has been liquidated or otherwise abandoned to avoid paying outstanding debts, said Nicole Rose, AUSTRAC's chief executive.

The Fintel Alliance also established a project working in partnership with the Department of Agriculture, Water and the Environment which provided opportunities to identify, target, and disrupt wildlife trafficking in Australia. All customer data used in the wildlife project was de-identified, enabling the sharing of ideas, methodologies, and locations, Tanumyroshgi said.

Conclusion

KYC rules are gaining in importance as a way to ensure financial institutions all over the globe are not doing banking business with organized crime syndicates or other illicit actors. Indeed, global regulatory agencies are placing more scrutiny on how financial institutions determine the real identity and other characteristics of their banking customers.

In this new white paper, we see how KYC rules have become a bigger part of financial service firms' compliance and security functions. We also saw how some firms are looking for solutions, through technology or other means, to alleviate the burden of these KYC compliance challenges.

KYC rules have become a bigger part of financial service firms' compliance and security functions.

Whatever the future holds for financial service firms, KYC likely is going to become a permanent feature of their compliance process, even as regulators become more serious and stricter about KYC disclosures. And any firm that doesn't listen to what regulators and industry sources are saying about the validity of KYC compliance, does so at its own risk to its reputation and bottom line.

Credits

Thomson Reuters Regulatory Intelligence Reporters:

Rachel Wolcott in London, UK

Nathan Lynch in Perth, AU

Brett Wolf in St. Louis, MO

Thomson Reuters Regulatory Intelligence Editors:

Alexander Robson in London, UK

Randall Mikkelsen in Boston, MA

Thomson Reuters Institute Editors:

Rabihah Butler in Charlotte, NC

Gregg Wirth in Bloomsburg, PA

Thomson Reuters

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.

For more information on Thomson Reuters, visit **tr.com** and for the latest world news, **reuters.com**.

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans blog commentaries, industry-leading data sets, informed analyses, interviews with industry leaders, videos, podcasts and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institute** for more details.

THOMSON REUTERS®