NTT DATA Services

WHITE PAPER | FINANCIAL SERVICES | BUSINESS PROCESS OUTSOURCING

Know Your Customer

Strategies for a successful due diligence program during the COVID-19 pandemic

JULY 2020

NTT DATA

Table of Contents

Introduction

The COVID-19 pandemic has changed the way we work and live. It has upset the U.S. economy and sent nations across the globe into financial turmoil. Globally, an estimated 300 million office workers have been asked to work from home, 90% of whom work in banking and insurance.[1] Most workers use a variety of devices, including personal computers, laptops, tablets and phones, to connect to their corporate networks and collaborate with their co-workers.[2] This increase in almost everyone's online presence has led to more, and often more naïve, targets for cybercriminals and online fraudsters. Money laundering is on the rise, too.

According to the World Bank, money laundering and terror financing may harm the stability of both individual financial institutions (FIs) and an entire country's financial sector through reputational, operational, legal and concentration risks. Globally, the estimated amount of money laundered in a year is 2% to 5% of gross domestic product (GDP) — in current U.S. dollars, that $800 billion to $2 trillion.[3]

Action Fraud, the U.K.'s national reporting center for fraud and cybercrime, warned the public to remain vigilant after statistics showed that more than 16,000 people fell victim to online shopping and auction fraud and lost over £16 million to online shopping fraud during the lockdown.[4] According to the Federal Trade Commission, COVID-19 scams related to travel and vacations, online shopping, bogus text messages and imposter scams have cost more than 18,000 Americans a total of $13.4 million since the beginning of 2020.[5]

A recent report by the Financial Stability Institute points to an increase in money laundering and terrorist financing risks as a result of crimes related to COVID-19.[6] To promote a strong and sound financial sector during the pandemic and in the next normal, all FIs need to fight against money laundering and terrorist financing by enabling a robust know your customer (KYC) and client due diligence (CDD) practice. Getting to know the customer is the first step in safeguarding against the risks of money laundering and other financial crimes. CDD as a practice must find a prominent place in organizations' strategies to mitigate risks.

FIs often bear the brunt of financial crimes, racking up hundreds of millions of dollars in fraud-related losses every year. Online fraud is one of the most difficult problems to predict and control, and this has become more difficult during the pandemic. Trillions of dollars pass through global financial networks, and industry leaders are always looking for more efficient and effective ways to mitigate the risks of being exposed to money laundering. Entities or parties that engage in financial crimes often create a web of networks.

A robust CDD process traces these networks to identify and screen the ultimate beneficial owners, related parties and key stakeholders, alerting decision-makers even before they can engage with such parties. Regulatory controls, increasing penalties and reputational risks have renewed investments to ensure due care is taken to scrutinize new customers and monitor them continuously for any suspicious activity, especially during uncertain times like this.

Regulatory landscape

Regulatory bodies across the world periodically bring in new regulations to combat money laundering and mitigate risk. Examples in the European Union include the Fourth European Money Laundering Directive and the Fifth European Money Laundering Directive. In the U.S., the Financial Crimes Enforcement Network in May 2016 issued rules under the Bank Secrecy Act to clarify and strengthen CDD requirements for banks.[7]

The set of reporting and compliance requirements of the U.S. is the most influential internationally, as it affects all FIs doing business or transacting with a U.S. legal or natural person or through the U.S. or (generally) in U.S. dollars.[8]
On a global scale, countries cooperate through international organizations (such as the Organization for Economic Co-operation and Development, the Financial Action Task Force and the Wolfsberg Group) on due diligence standards and exchange of tax information.[9]

New regulations by governments also mean an increase in compliance requirements. Financial institutions are regularly required to make significant changes in compliance in response to stringent regulatory actions. Even with regulatory bodies all over the world trying to intercept illegal funds with anti-money laundering (AML) standards and legislation, the global interception rate for these efforts remains low.

Rising costs of compliance

The costs and complexity of KYC compliance continue to rise rapidly, according to global surveys, and negatively impact businesses. The top 10% of the world's FIs spend at least US$100 million on CDD annually.[10] Without an international standard for KYC/CDD procedures it is difficult for banks to remain compliant both locally and globally; they must follow different regulations in the countries in which they operate, so KYC programs are nonstandard, further driving up costs.[11]
In September 2019, Celent estimated that spending on technology used in AML-KYC compliance will reach US$8.3 billion and that spending on operations will reach US$23.4 billion globally per year.[12]

Rising penalties by regulatory authorities

In general, banks and FIs were penalized by regulators to the tune of more than US$320 billion between 2008 and 2016, according to estimates by Boston Consulting Group.[13] The US$9 billion in fines that Paris-based BNP Paribas paid was, at the time, a record for money laundering/sanctions compliance.[14] Penalties related to KYC and AML — estimated to be $26 billion — are significant, considering that the rigor around KYC/CDD gained momentum only in the last decade.[15]

A number of global banks, and even smaller regional banks, have faced the wrath of regulators over KYC/AML noncompliance. In 2019, 58 AML penalties totaling $8.14 billion of fines were handed down globally. This is nearly double the amount handed down the prior year. These penalties were assessed by regulators across multiple jurisdictions, including those in Belgium, Bermuda, France, Germany, Hong Kong, India, Ireland, Latvia, Lithuania, the Netherlands, Norway, Tanzania, the U.S. and the U.K. Regulators in the U.S. handed out 25 penalties totaling US$2.29 billion. The U.K. followed with 12 fines totaling US$388.4 million. The largest monetary fine was US$5.1 billion and originated in France.[16]

Risk protection

FIs are exposed to a multitude of risks due to internal and external factors. One of the key external factors impacting risk is a company's clientele. Robust CDD processes reduce this risk by identifying customers who are more likely to be involved in money laundering:

- **Reputational risk** can arise when a bank becomes a vehicle for illegal activities that attract adverse publicity to its business practices and associations, often resulting in lasting damage to its reputation.
- **Operational risk** occurs when institutions sustain direct or indirect losses due to inadequate or failed internal procedures, often as a result of neglecting to practice due diligence — for example, a fraudulent account that obtains credit facilities.
- **Legal risk** is the risk of legal action, adverse judgments or unenforceable contracts that can disrupt and adversely affect a bank's operations. An example of this type of risk is failure to observe mandatory CDD standards or privacy regulations.[17]

Digital transformation drives advancements in financial services but also introduces new risks. The General Data Protection Regulation (GDPR) includes a risk-based approach to data protection. It requires organizations assess the "likelihood and severity of risk" of their personal data-processing operations against the fundamental rights and freedoms of individuals. GDPR makes it mandatory for organizations to modulate their data protection compliance according to the level of risk their personal data-processing operations pose.[18]
On January 21, 2019, Google faced a financial penalty of €50 million, imposed by France's National Data Protection Commission (CNIL) in accordance with the GDPR, for lack of transparency, inadequate information and lack of valid consent regarding the personalization of ads. Banks will be next in line if they ignore the new risks.[19]

New risks from COVID-19

The Financial Action Task Force points to an increase in the following money laundering and terrorist financing risks due to crimes related to COVID-19[6]

- Bypassing of CDD measures
- Misuse of online financial services and virtual assets to transfer and conceal illicit funds
- Exploitation of economic stimulus measures and insolvency schemes to conceal and launder illicit incomes
- Misuse of the unregulated financial sector to launder illicit funds
- Diversion of domestic and international financial aid and emergency funding to other shell company accounts
- Exploitation by criminals and terrorists of COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries

Due to the social distancing norms dictated by the pandemic, financial institutions have started adopting remote onboarding and identity verification. This has created multiple loopholes through which criminals can exploit gaps or weaknesses in the AML defenses of financial systems. Today, there is a great need to use current technologies and the collective knowledge from around the globe to create a practical framework for a robust CDD solution amid the pandemic.

Technology

In the last decade, the pace of disruptive digital technological change has advanced rapidly. This has brought about a host of new technologies with promise for AML compliance. Among them are:

1. Data analytics
2. Continuous risk assessment
3. Blockchain (incremental risk assessment)
4. Artificial intelligence (AI)
5. Natural language processing
6. Digital ID

The financial sector is rapidly innovating with the help of digital technologies. Fintech, short for financial technology, is driving innovation in financial literacy and education, retail banking, investment and financial compliance, as well as defining a new level of competitiveness and service excellence in the financial sector today. These innovations have significant potential to dramatically increase the efficacy of financial crime-prevention initiatives.

Data analytics

Data analytics plays a key role in uncovering hidden patterns and correlations and gaining valuable information that can be used to make decisions regarding the risk assessment of customers. Data-driven risk assessment is used to calculate normalized customer risk scores (generally rated as low, medium or high) by applying specific tolerance limits.

Continuous risk assessment

Automated risk assessment benefits from data analytics and machine learning capabilities by continuously evaluating the changing characteristics of the customer. For example, a company previously rated as low risk because it trades locally and has cash transactions below 5% generates a higher risk rating when it starts trading with agencies in high-risk countries.

Blockchain

Blockchain technology enables incremental risk assessment, eliminating the need to review historical evidence. Distributed ledger capabilities also help consortium-based CDD by collectively owning and validating clients. For example, once a KYC assessment is performed, it can be accessed by other financial institutions with unique authorization from the client. This makes the KYC process much simpler, less time consuming and more cost effective. The KYC data is replicated across various nodes, making it immutable and traceable, and blockchain's append-only data structure makes it very secure.[20]

Artificial intelligence

AI-enabled systems embed intelligence that sifts through a large number of data sources, aggregating and identifying patterns, and predicting relationships. The accuracy of such a system is significantly higher than that of a rules-based system. Machine learning naturally extends AI by giving computers the capability to learn without being explicitly programmed. This partnership enables rapid, iterative expansion of the AI model, applying decisions geared toward improving business outcomes.

Natural language processing

Enhanced optical character recognition, with contextual capabilities and natural language processing capabilities, offers a huge advantage by sifting through multiple pages of documentation and extracting only the information relevant for CDD. When combined, intelligent character recognition and mobile document scanning capabilities make a powerful solution for remote customer identification and authentication.

Digital ID

Digital IDs are more accurate, reliable and independent than traditional paper-based CDD procedures, and they do not have the same weaknesses.[21]

Digital ID systems could facilitate customer identification and verification during onboarding, support ongoing due diligence and scrutiny of transactions throughout the course of the business relationship, facilitate CDD measures, and aid transaction monitoring for the purposes of detecting and reporting suspicious transactions, as well as in general risk management and anti-fraud efforts.

Reliable, independent digital ID systems can also contribute to financial inclusion by enabling unserved and underserved people to prove official identity in a wide range of circumstances, including remotely, to obtain regulated financial services.[22]

To combat COVID-19 costs and the economic downturn, digital IDs can be used to increase regulated entities' efficiencies and reallocate resources to other AML and combating financing of terrorism (CFT) functions.

Dimensions of a robust KYC/CDD solution

CDD processes are at the forefront of the fight against money laundering, bringing together the best of technology and human expertise. A sound technology platform, combined with a high-caliber operation backed by established support systems, will ensure that CDD objectives are met in the most efficient manner.

Data

Ensuring rich, reliable, real-time data is the foundation for a consistent CDD processing operation. The key is to bring together myriad document registries, customer databases, alert lists and other trusted sources and then arrange them in a structured format without any deficiency or inconsistency. Real-time connectivity is essential to make sure CDD reviews are completed in the shortest possible time.

Technology platform

Digital technology strengthens the KYC/CDD process and vastly improves efficiency by combining the power of AI and human expertise.

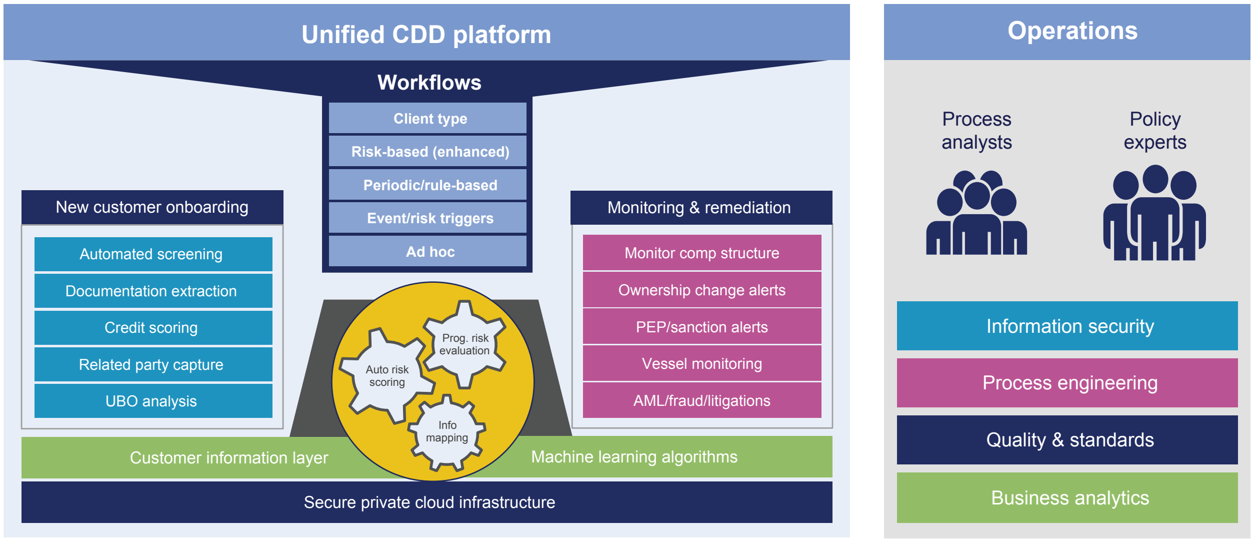

Figure 1: A comprehensive KYC/CDD solution

A successful CDD platform will be:

- **Scalable.** The technology platform should have a robust user management tool that helps scale to large volumes and seamlessly expand to accommodate a huge user base.
- **Customizable.** The technology platform should be customizable to accommodate the process variations each bank or FI accommodates while maintaining the structural base framework.
- **Secure.** Client data security should be the top-most consideration for a KYC/CDD platform. The platform should be equipped with the latest security and encryption technologies.

It will feature:

- **Robotics/analytics.** Incorporating robotic process automation (RPA) and personal robotics assistants (PRAs) as standard features in the platform will help banks and FIs perform CDD analysis more accurately and with less human effort. RPA/PRAs can work with predetermined logic/machine learning.
- **Dynamic workflows.** With a customer base that can have global roots, as well as different types of entity structures, account types and products, the need to have a dynamic workflow capability that changes according to regulatory and product/client requirements cannot be understated.
- **End-user interface.** Customer interaction capabilities allow end customers to update key changes and upload additional documentation required to complete the review.

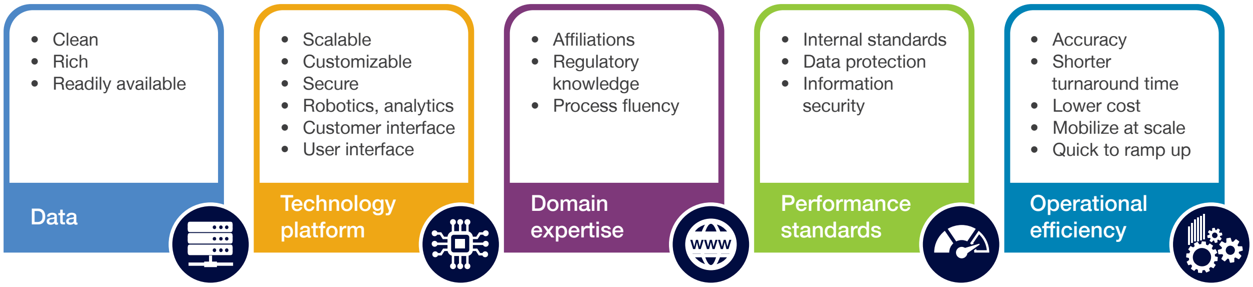

Figure 2: Client due diligence success factors

And it will be able to perform:

- **Automated processing.** An important measure of any KYC/CDD platform will be its ability to process cases with no or minimal human intervention.
- **Simulation/scenario analysis.** Regulatory changes are to be expected with every new year. The ability to measure compliance against different standards enhances the robustness of the platform and its ability to identify potential deficiencies in CDD.
- **Real-time analytics.** Embedded analytics within the platform should be capable of delivering operational dashboards, business insights and portfolio analytics.

Domain expertise

Talented resources and domain knowledge underpin a sound CDD program. It takes continuous effort and nurturing to develop a team that can work with predefined processes but be able to identify hidden risks. Skilled resources should be conversant with KYC/CDD procedures as well as have the skills to identify potential risks. It is also important that the resources be aware of the regulatory landscape and able to make appropriate decisions. Proficiency in regulatory requirements across different countries and the ability to define processes/procedures to comply with them is an essential skill to develop.

Performance standards

A successful program can thrive only in an environment supported by strong organizational standards that has a zero-tolerance information security policy, a quality and standards framework, and a continuous process improvement character.

Operational efficiency

Operational standards and continuous improvement initiatives are crucial to ensure quality and operational excellence. This includes:

- **Accuracy.** Lapses in CDD can lead to high risk exposure if there are errors in case processing. CDD operations typically operate with accuracy scores greater than 99.5%.
- **Turnaround time.** While the focus of CDD is primarily managing risk, the underlying objective is to add new customers and expand the business. Delays in CDD will have an impact on downstream systems and would prove to be a bottleneck if due diligence is not completed on time. Typical turnaround times could range from 20 minutes for a personal customer to two business days for a complex review.
- **Handle time.** Average handle time is a measure of the time spent processing a case. Reduced handle times are achieved by automating and engaging PRAs where applicable.
- **Cost efficiencies.** Continuous process improvements should be part of the operations culture to improve efficiencies and reduce costs. Six sigma approaches can be applied for large-scale operations to ensure process stability and measured benefits.
- **Flexible staffing.** The capability to scale to meet business requirements is necessary to maintain cost at optimal levels. The ability to scale up and down to meet changing requirements can be met by cross-training other teams.

Conclusion

A successful CDD program is the key to protecting banks and FIs from present risks, as well as those arising from the current pandemic, and to setting up these organizations for success in the future. A well-established partner like NTT DATA can help businesses meet their goals of achieving regulation and risk compliance while keeping costs low. NTT DATA's rich expertise in managing KYC/CDD, enhanced due diligence and screening alerts investigation, along with pioneering technology strengths in intelligent workflows, RPA, AI and analytics, come together in one unique offering — end-to-end CDD support from program set up to global resourcing.

About the authors

Shabi Christopher is a management professional with over 20 years in corporate planning, technology implementation, solution design and analytics, with demonstrated value additions in global project implementations and bottom-line impact of over $80 million. A key contributor to financial strategy, he played a critical role in architecting $100+ million deals. Shabi directs KYC/CDD/EDD/banking operations for financial services clients in EMEA, including service design, delivery, partner management and coordination with global teams.

Dr. Clifford Paul is a financial strategist with more than 14 years of experience as a finance controller and director of management studies. He has authored research articles in many peer-reviewed journals, as well as presented papers at both national and international conferences. Clifford has eight years of experience in the financial planning and compliance industry.

Sources

1. Juan Carlos Crisanto and Jermy Prenio. “Financial crime in times of Covid-19 – AML and cyber resilience measures.” Financial Stability Institute. FSI Briefs No. 7. May 2020. https://www.bis.org/fsi/fsibriefs7.pdf
2. James Mirfin. “The perfect storm: COVID-19 risk shaping digital transformation.” Refinitiv. April 16, 2020. https://www.refinitiv.com/perspectives/financial-crime/covid-19-and-fighting-financial-crime/
3. United Nations Office on Drugs and Crime. “Money-Laundering and Globalization.” https://www.unodc.org/unodc/en/money-laundering/globalization.html
4. ActionFraud. “Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk.” June 19, 2020. https://www.actionfraud.police.uk/alert/over-16-million-lost-to-online-shopping-fraud-during-lockdown-with-people-aged-18-26-most-at-risk
5. Greg Iacurci. “Americans have lost $13.4 million to fraud linked to Covid-19.” CNBC. April 15, 2020. https://www.cnbc.com/2020/04/15/americans-have-lost-13point4-million-to-fraud-linked-to-covid-19.html
6. Financial Action Task Force. “COVID-19-related Money Laundering and Terrorist Financing, Risks and Policy Responses.” May 2020. http://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html
7. Department of the Treasury Financial Crimes Enforcement Network. “Customer Due Diligence Requirements for Financial Institutions; Final Rule.” Federal Register. May 2016. https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf
8. IIF Regtech Working Group. “Deploying Regtech Against Financial Crime.” March 2017. https://www.iif.com/portals/0/Files/private/32370132_aml_final_id.pdf
9. Yvonne Lootsma. “Blockchain as the Newest Regtech Application — the Opportunity to Reduce the Burden of KYC for Financial Institutions.” Initio. September 2017. https://www.initio.eu/blog/2017/9/26/blockchain-as-the-newest-regtech-application-the-opportunity-to-reduce-the-burden-of-kyc-for-financial-institutions

10. John Callahan. “Know Your Customer (KYC) Will Be A Great Thing When It Works.” Forbes. July 2018. https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#74ee995e8dbb
11. IIF Regtech Working Group. “Deploying Regtech Against Financial Crime.” March 2017. https://www.iif.com/portals/0/Files/private/32370132_aml_final_id.pdf
12. Arin Ray and Neil Katkov. “IT and Operational Spending in AML-KYC: A Global Perspective.” Celent. September 11, 2019. https://www.celent.com/insights/900750380
13. Gerold Grasshoff, Zubin Mogul, Thomas Pfuhler, et. al. “Global Risk 2017: Staying the Course in Banking.” Boston Consulting Group. March 2017. https://www.bcg.com/en-gb/publications/2017/financial-institutions-growth-global-risk-2017-staying-course-banking.aspx
14. Richard L. Cassin. “BNP trampled compliance officers, pays record $9 billion penalties for sanction offenses.” The FCPA Blog. May 2015. http://www.fcpablog.com/blog/2015/5/4/bnp-trampled-compliance-officers-pays-record-9-billion-penal.html
15. Jaclyn Jaeger. “Report: Financial firms fined $26B for AML, sanctions, KYC non-compliance since 2008.” Compliance Week. September 2018. https://www.complianceweek.com/report-financial-firms-fined-26b-for-aml-sanctions-kyc-non-compliance-since-2008/8088.article
16. IBS intelligence. “Money laundering (AML) fines total $8.14 billion in 2019.” January 13, 2020. https://ibsintelligence.com/ibs-journal/ibs-news/money-laundering-aml-fines-total-8-14-billion-in-2019/
17. Basel Committee on Banking Supervision. “Customer Due Diligence for Banks.” Bank for International Settlements. Guidelines originally published in October 2001. https://www.bis.org/publ/bcbs85.htm
18. Centre for Information Policy Leadership. “Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR CIPL GDPR Interpretation and Implementation Project.” December 2016. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf
19. CNIL. “The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.” January 2019. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
20. University of Luxembourg Publications. “Blockchain Orchestration and Experimentation Framework: A Case Study of KYC.” 2018. http://publications.uni.lu/bitstream/10993/35467/1/blockchain-orchestration-experimentation.pdf
21. Hogan Lovells. “COVID-19 and online KYC: an Italian picture.” Lexology. May 26, 2020. https://www.lexology.com/library/detail.aspx?g=c69a2a57-96b9-4677-b259-9e8f001a0100
22. Financial Action Task Force. “Digital Identity.” March 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf