NTT DATA

WHITE PAPER | FINANCIAL SERVICES | BUSINESS PROCESS OUTSOURCING

"Know Your Customer" Strategies in a Post-2020 World

Insights from our 2021 Global Threat Intelligence Report

SEPTEMBER 2021

NTT DATA

Table of Contents

Introduction	3
Regulatory landscape	4
Rising costs of compliance	5
Rising penalties by regulatory authorities	5
Risk protection	6
New risks from COVID-19	6
Technology	7
Dimensions of a robust KYC/CDD solution	9
Conclusion	12
About the authors	12
Sources	13

Introduction

The COVID-19 pandemic has upset the global economy and sent nations around the world into financial turmoil due to recurring lockdowns designed to mitigate the spread of the disease. Businesses continue to operate, albeit in a different world order compared to two years ago.

Globally, an estimated 300 million office workers have been asked to work from home, 90% of whom work in banking and insurance.[1] It's a drastically changed business environment, and companies are still adapting. According to the NTT 2020 Intelligent Workplace Report, 54% of organizations surveyed were planning to move to remote working or using a hybrid operating model with expanded flexible working.[2] For most workers this means using a variety of devices, including personal computers, laptops, tablets and phones, to connect to their corporate networks and collaborate with their co-workers.[3] The increase in almost everyone's online presence has also led to more, and often more naïve, targets for cybercriminals and online fraudsters.

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 — in current U.S. dollars, that's $800 billion to $2 trillion.[4] A recent report by the Financial Action Taskforce points to an increase in money laundering and terrorist financing risks because of crimes related to COVID-19.[5] On a more personal level, 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.[6] In the U.S., the Federal Trade Commission reported that 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.[7] Organizations have prioritized providing information and communications technology (ICT) support, but security initiatives are lagging.

An approximately 50% increase in attack volume made finance the most attacked industry in 2020, according to the 2021 Global Threat Intelligence Report, accounting for 23% of all that year's attacks.[8] The industry's unique position motivates attackers to steal data, modify data integrity and commit direct financial theft. Although these three goals haven't changed much over the past year, the targets have. COVID-19 forced many bank lobbies to close, redirecting FIs' foot traffic to digital services. Hostile threat actors recognized customers' increased use of online and mobile banking services and capitalized on this shift to more web-enabled apps. Attackers continue to value financial data despite the industry's security posture and heavy security apparatus. FIs rack up hundreds of millions of dollars in fraud-related losses every year, often bearing the brunt of financial crimes. Adding to that, online fraud is one of the most difficult problems to predict and control. It remains so as the pandemic continues, with trillions of dollars passing through global financial networks.

Industry leaders constantly look for more efficient and effective ways to mitigate the risks of being exposed to money laundering. One way for FIs to promote a strong and sound financial sector during the pandemic and in the next normal, as well as continue the fight against money laundering and terrorist financing, is to adopt 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.

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 these.

Regulatory landscape

Regulatory bodies across the world periodically bring in new rules to combat money laundering and mitigate risk. 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] In the European Union (EU), examples include the Fourth European Money Laundering Directive and the Fifth European Money Laundering Directive. Through the Financial Crimes Enforcement Network the U.S. in May 2016 issued rules under the Bank Secrecy Act to clarify and strengthen CDD requirements for banks.[10] This set of reporting and compliance requirements 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.[11] Within the U.S., California leads all states in data protection rights, enacting the California Consumer Privacy Act (CCPA) in January 2020, followed by the California Consumer Rights Act (CPRA).

Since the EU's General Data Protection Regulation (GDPR) revision in 2018, many other countries have made amendments. When the New Zealand Privacy Act 2020 was enacted on December 1, 2020, effectively repealing and replacing the 1993 Privacy Act, it gave new regulatory powers to the New Zealand Privacy Commissioner. It mandated notification of a data breach if a risk of harm exists and established new criminal penalties, including fines of up to NZD 10,000. In addition, overseas organizations that conduct business in New Zealand must now comply with the country's new privacy laws because of the extraterritorial effect.[8] In South Africa, any organization that processes personal data must comply with the Protection of Personal Information Act (POPIA), which went into effect July 1, 2020. Singapore updated its Personal Data Protection Act (PDPA) in November 2020 to introduce the "legitimate interests" principle so organizations can process personal data without consent, but it only applies if organization can ensure its overall benefits don't outweigh any possible adverse effects to the individual from whom it is collecting information. Maximum fines also increased, so a data breach could cost an organization up to 10% of its annual turnover or SGD 1 million, whichever is higher.[8]

These and other regulations add to the pressure organizations face. Among respondents in the 2021 Global Threat Intelligence Report, 46% said compliance regulations would necessitate hiring additional skills in governance, risk and compliance, as well as data protection and risk auditing. And 76% of organizations said that at some point within the next year they would be unprepared to meet compliance obligations.[8]

New government regulations, amendments and data protections will continue to be enacted, so local and global compliance requirements will continue to increase. FIs 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 impact businesses negatively. The top 10% of the world's FIs spend at least $100 million on CDD annually.[12] Without an international standard for KYC/CDD procedures, it's 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 the technology used in AML-KYC compliance will reach $8.3 billion and that spending on operations will reach $23.4 billion globally per year.[13]

COVID-19's significant impact on existing challenges has increased due diligence times and costs. The "True Cost of Financial Crime Compliance Study" projected the total global cost of financial crime compliance across all financial institutions as $213.9 billion.[14]

Rising penalties by regulatory authorities

IIn general, banks and FIs were penalized by regulators to the tune of more than $320 billion between 2008 and 2016, according to estimates by Boston Consulting Group.[15] The $9 billion in fines that Paris-based BNP Paribas paid was, at the time, a record for money laundering/sanctions compliance.[16] Penalties related to KYC and AML — estimated to be $26 billion — are significant, too, considering the rigor around KYC/CDD gained momentum only in the last decade.[17]

Numerous 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 in fines were handed down globally. This is nearly double that of 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 $2.2 billion. The U.K. followed with 12 fines totaling $388 million. The largest monetary fine was $5.1 billion and originated in France.[18]

In 2020, global AML fines for financial institutions increased again, to more than $10.3 billion.[19] This trend will continue in 2021 due to the increased compliance scrutiny by regulators worldwide.

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. Other types of risk include:

- 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 can occur when institutions sustain direct or indirect losses due to inadequate or failed internal procedures, often because of neglecting to practice due diligence — for example, a fraudulent account that obtains credit facilities.
- Legal risk can disrupt and negatively impact a bank's operations due to potential legal action, adverse judgments or unenforceable contracts. An example of this type of risk is failure to observe mandatory CDD standards or privacy regulations.[20]

Digital transformation may also introduce new risks, despite the advancements it drives in financial services.

The GDPR includes a risk-based approach to data protection. It requires organizations to assess the "likelihood and severity of risk" of their personal data-processing operations against the fundamental rights and freedoms of individuals. Under GDPR organizations must modulate data protection compliance according to the level of risk each company's personal data-processing operations pose.[21] Not complying can be costly. 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 for the personalization of ads. Banks will be next in line if they ignore the new risks.[22]

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:[5]

1. Bypassing CDD measures
2. Misusing online financial services and virtual assets to transfer and conceal illicit funds
3. Exploiting economic stimulus measures and insolvency schemes to conceal and launder illicit incomes
4. Misusing the unregulated financial sector to launder illicit funds
5. Diverting domestic and international financial aid and emergency funding to other shell company accounts
6. Exploiting — by criminals and terrorists — COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries

The pandemic's social distancing norms forced FIs to adopt remote onboarding and identity verification. This practice creates multiple loopholes through which criminals can exploit gaps or weaknesses in the AML defenses of financial systems. Amid the pandemic, current technologies and collective knowledge from around the globe create a practical framework for today's robust CDD solutions.

Technology

The last decade has seen a rapid advancement in the pace of disruptive digital technological change. It's also brought about a host of new technologies with promises 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

Digital technologies help the financial sector innovate rapidly. Fintech, short for financial technology, drives innovation in financial literacy and education, retail banking, investment and financial compliance, in addition to 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 (ML) 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 replicates across various nodes, so it's immutable and traceable, and blockchain's append-only data structure makes it very secure.[23]

Artificial intelligence

AI-enabled systems embed intelligence that sifts through many 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. ML 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 don't have the same weaknesses.[24]

A digital ID system could facilitate customer identification and verification during onboarding, support ongoing due diligence and scrutiny of transactions throughout the business relationship, facilitate CDD measures and aid transaction monitoring not only to detect and report suspicious transactions but also in general risk management and anti-fraud efforts. Reliable, independent digital ID systems can contribute to financial inclusion by enabling unserved and underserved people to prove their official identity in a wide range of circumstances, including remotely, to obtain regulated financial services.[25] 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 activities and help combat the financing of terrorism functions.

Dimensions of a robust KYC/CDD solution

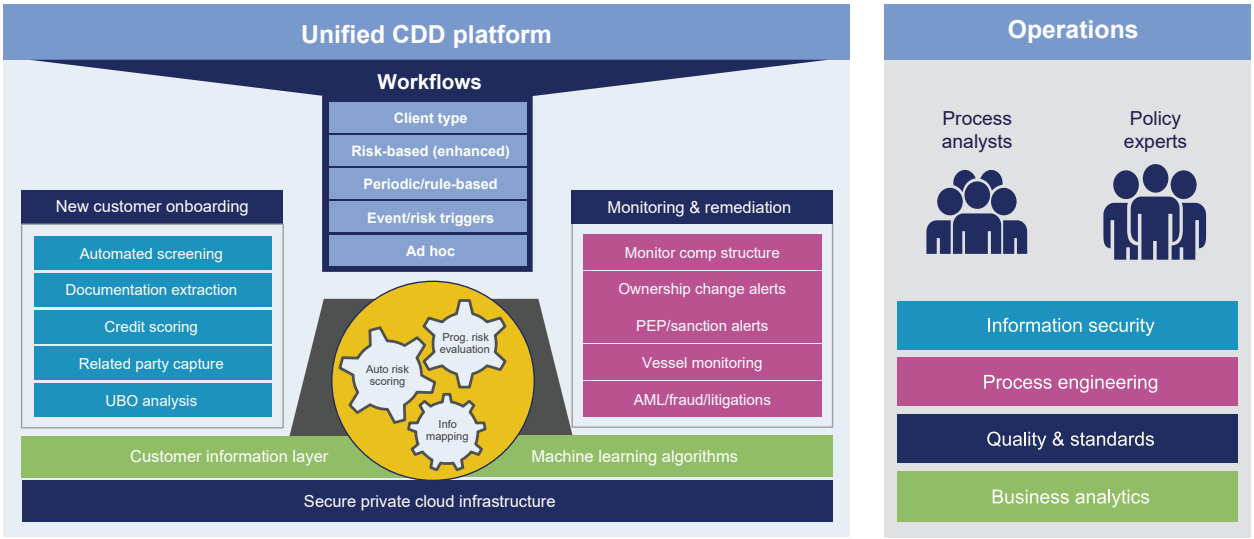
CDD processes are at the forefront of the fight against money laundering, bringing together the best of technology and human expertise. A sound technology platform, combined with a high-caliber operation backed by established support systems, will ensure CDD objectives are met efficiently.

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.

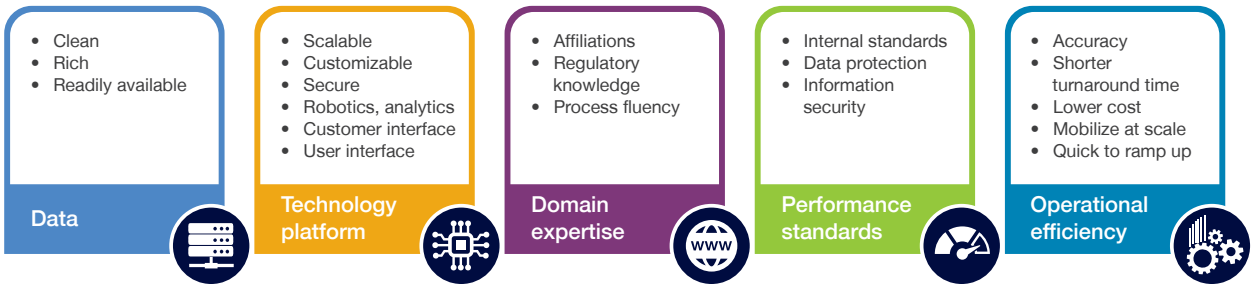


A successful CDD platform will be:

- **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:** The technology platform should be equipped with the latest security and encryption technologies, as client data security should be the top-most consideration for KYC/CDD.

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/ML.
- **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 can't be understated.
- **End-user interface:** Customer interaction capabilities allow end customers to update key changes and upload additional documentation required to complete the review.



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 and have the skills to identify potential risks. It is also important that 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 that is supported by strong organizational standards and 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 isn't 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 future success.

A well-established partner like NTT DATA can help your business achieve regulation and risk compliance while keeping costs low and strengthening your CDD process with dynamic risk management and monitoring. By introducing dynamic risk management with deep learning techniques into your CDD program, you'll be able to take a proactive approach to risk management and be better prepared for what lies ahead.[26] 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, Business Consulting Director, Analytics and FinTech Programs, NTT DATA
Shabi is a management professional with over 24 years in corporate planning, technology implementation, solution design and analytics, with demonstrated value additions in global project implementations and bottom-line impact valued at over $80 million. A key contributor to financial strategy, he has played a critical role in architecting more than $100 million in deals. Shabi directs KYC/CDD/enhanced due diligence/banking operations for global financial services clients, including service design, delivery, partner management and coordination with global teams.

Dr. Clifford Paul, Business Process and Strategy Senior Manager, NTT DATA
Dr. Paul is a business process and strategy senior manager in the compliance arena who has more than 19 years of experience. He is responsible for tracking the company's financial performance against budget, analyzing business performance and market conditions to create forecasts, and helping senior management make tactical and strategic decisions by providing periodic reports. Dr. Paul has authored research articles in many peer-reviewed journals, as well as presented papers at both national and international conferences.

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.
2. NTT Ltd. "2020 Intelligent Workplace Report." https://interactive.hello.global.ntt/story/2020-intelligent-workplace-report/page/4/3
3. James Mirfin. "The perfect storm: COVID-19 risk shaping digital transformation." Refinitiv. April 16, 2020. https://www.refinitiv.com/perspectives/financialcrime/covid-19-and-fighting-financial-crime/
4. United Nations Office on Drugs and Crime. "Money-Laundering and Globalization." https://www.unodc.org/unodc/en/money-laundering/overview.html
5. 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
6. 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
7. 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
8. NTT Ltd. "2021 Global Threat Intelligent Report" https://hello.global.ntt/en-us/insights/2021-global-threat-intelligence-report/
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/blognavigation/2017/9/26/blockchain-as-the-newest-regtech-application-the-opportunity-to-reduce-the-burden-of-kyc-for-financial-institutions
10. 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

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. 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
13. 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
14. LexisNexis Risk Solutions. "True Cost of Financial Crime Compliance Study." June 2021. https://www.law360.com/articles/1391228/attachments/0
15. 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
16. 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
17. Jaclyn Jaeger. "Report: Financial firms fined $26B for AML, sanctions, KYC non-compliance since 2008." Compliance Week. September 2018. https://www.complianceweek.com/reportfinancial-firms-fined-26b-for-aml-sanctions-kycnon-compliance-since-2008/8088.article
18. 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/
19. Charlie Steele, Sarah Wrigley, Selma Della Santina and Deborah Luskin. "Anti-Money Laundering Trends and Challenges." June 21, 2021. https://globalinvestigationsreview.com/review/the-european-middle-eastern-and-african-investigations-review/2021/article/anti-money-laundering-trends-and-challenges
20. 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
21. 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
22. 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
23. 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
24. 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
25. Financial Action Task Force. "Digital Identity." March 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf
26. NTT DATA. "A Quick Guide to Dynamic Risk Management and Monitoring." 2021. https://us.nttdata.com/en/-/media/assets/white-paper/whitepaper-a-quick-guide-to-dynamic-risk-management-and-monitoring-ebook-march-2021.pdf