The Honest Guide
to AI in Finance

The must-have guide to understanding why artificial intelligence is vital to financial institutions' anti-money laundering efforts

BABELSTREET

Evolving compliance mandates. More fraud. More competitors. Financial institutions (FIs) operate in an increasingly complex environment. Yet, hampered by legacy systems and a lack of in-house expertise, too few FIs invest in the one technology that can help them thrive in the current marketplace: artificial intelligence (AI).

This e-book examines the compliance and business challenges financial institutions face and the existing AI technologies that can help meet them.

Contents

Navigating the compliance labyrinth

The United Nations estimates that criminals worldwide launder between $800 billion and $2 trillion each year, representing anywhere from 2% to 5% of the world economy.[1] The money stems from, and funds, the most heinous types of crimes: terrorism, slavery, weapons trafficking, child exploitation, and the drug trade among them. Legislators believe that when the flow of money stops, instances of these crimes plummet. That's why nations worldwide have implemented stringent anti-money laundering (AML) laws. (See sidebar, *Anti-money laundering statutes: a brief history.*)

To comply with AML laws, financial institutions must meet stringent Know Your Customer (KYC) requirements — mandatory processes for verifying a customer's identity at account opening and periodically thereafter. (These activities are also often referred to as "customer due diligence" or "enhanced due diligence.")

AML KYC mandates vary from country to country. In the United States, comparing names of potential and existing customers against entities appearing on the Office of Foreign Assets Control's (OFAC's) Specially Designated Nationals and Blocked Persons list[2] is a significant aspect of this work. (See sidebar, *What is the SDN list?*) OFAC levies heavy fines against FIs that don't comply with these sanctions. In 2019, those fines totaled nearly $1.3 billion.[3]

Financial institutions work hard to meet AML KYC mandates, but they are caught in a vicious cycle of new crimes begetting new laws leading to ever-more-demanding requirements.

Anti-money laundering statutes: a brief history

The history of modern compliance in the United States dates to the 1970 Bank Secrecy Act. Its goal was to halt financial crime — most notably, money laundering. The Patriot Act of 2001, the Anti-Money Laundering Act of 2020, and other statutes augmented this effort.[4]

Governments across the globe have passed similar types of legislation. Most recently, the European Union's Sixth Money Laundering Directive broadens the definition of money laundering and increases penalties for offenders.[5] The 41 member states of the Asia/Pacific Group on Money Laundering strive to implement international AML standards in that region.

Consider this. Real estate has grown in significance as a money laundering vector.[6] Pricing is subjective, you can buy real estate in cash, and you can hide ownership behind a corporate veil. Criminals also increasingly use cryptocurrencies to launder money, and brokerages have arisen to make the cryptocurrency buying process easier.

New mandates arise to combat these burgeoning forms of money laundering. The proposed Establishing New Authorities for Businesses Laundering and Enabling Risks to Security (ENABLERS) Act[7], would subject professional service providers to KYC mandates. These professionals include investment advisers, certain lawyers, certain accountants, and others who act as "gatekeepers" to the United States financial system. The Act was introduced just three years after the sweeping reforms of the Anti-Money Laundering Act of 2020. In Europe, meanwhile, the Sixth Anti-Money Laundering Directive took effect in late 2020, *less than a year* after implementation of Europe's Fifth Anti-Money Laundering Directive.

To comply with these mandates, financial institutions have begun a new form of customer due diligence: adverse media screening. This process entails comparing prospects and customers against news sources to see if anything negative has been reported against a person or company. In the European Union, since 2017 due diligence mandates have required FIs to screen customers against reputable media.

The regulation cycle shows no sign of easing, and new anti-money laundering compliance processes must be undertaken to meet each new mandate.

What is the SDN list?

The Specially Designated Nationals and Blocked Persons (SDN) list names people, groups, businesses, countries, governments, and other entities who have been identified by the United States government as posing a threat to national security, foreign policy, or economic policy. OFAC uses the SDN list to keep these groups from accessing the United States financial system. The sanctions covered by the SDN list are extensive; entities listed appear in a multitude of languages; and the list is continually updated. OFAC compliance means financial institutions may not onboard customers whose names appear on the list and must stop doing business with existing customers should their names ever appear on that list.

Reach compliance and business goals

FIs play a significant role in safeguarding world financial systems from corruption. But they don't exist solely to keep bad guys from laundering funds. Like businesses everywhere, they want to increase profitability. Among the challenges FIs face in this arena are reducing fraud and improving the customer experience.

Instances of fraud are both increasing in number and growing more expensive to correct. Each $1 of fraud loss now costs FIs $4 to resolve, according to the "LexisNexis® True Cost of Fraud™ Study: Financial Services & Lending."[8] Reducing fraud losses can improve overall FI profitability. Many fraud prevention efforts now focus on mobile banking, which grew into an important banking channel for both customers and criminals during the COVID-19 pandemic.

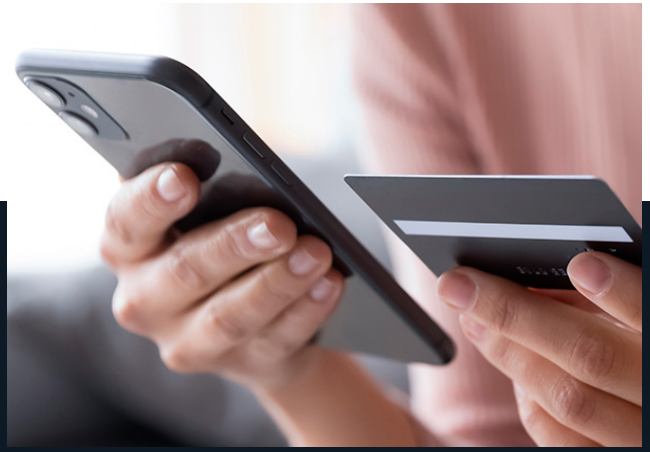
While improving the fight against fraud can help save money, boosting the customer experience (CX) aids FIs in meeting the challenges of customer acquisition and retention.

A better understanding of customers is the first step in improving CX. A single, holistic view of each customer can help FIs tailor the right experience to the right customer or prospect, improve marketing efforts, forge stronger customer relationships, and enable better decision making.

Artificial intelligence — particularly natural language processing capabilities applied in areas such as name matching, entity resolution, sentiment analysis, and adverse media screening — can help FIs reach both compliance and business goals.

So financial institutions everywhere must have wholeheartedly embraced AI, right?

Instances of fraud are both increasing in number and growing more expensive to correct.



The AI challenge

Wrong.

Only 56 percent of banks worldwide use any type of AI, according to the World Economic Forum.[9] More than half the banks surveyed in the "2021 Refinitiv Global Risk and Compliance Report" say they do not fully run KYC verification of client data.[10] Ninety-one percent of companies that use technology for KYC acknowledge they need to improve financial crime detection and mitigation over the next year.[11]

With so clear a need for AI capabilities, why haven't more FIs implemented it?

Financial institutions often face three stumbling blocks in the implementation of AI.

1. The expertise problem

First, many established FIs are hampered by legacy systems: outdated hardware and software, sometimes developed in-house. These systems still work but have significant difficulties interacting with newer technologies. Other FIs face issues of scalability. As smaller FIs grow, their KYC needs evolve — typically growing more complex. AML checks that worked fine for a bank operating in one state may not translate to a bank now serving an entire region.

AI can help in these cases, but a vast amount of specialized engineering expertise is required to build new AI systems and connect them to the data stored in legacy technology. FIs need machine learning coders, data scientists, and others. Many FIs don't have this type of team on hand. And those who do risk losing understanding of the workings of their AI systems when key people leave the company. For these reasons, FIs often find they cannot build AI systems in-house, and instead must find a trusted provider to customize, install, and co-manage these systems.

2. The data deluge

Second, FIs often feel overwhelmed by the sheer amount of data to be examined. Some institutions employ hundreds or thousands of people to oversee millions of customers and trillions in currency. Traders open accounts, trade, and close accounts. Customers onboard, deposit, withdraw. They take out mortgages and car loans and business loans. They pay salaries.

FIs typically store information related to all these activities in an array of siloed data warehouses, or in enormous, heterogeneous data lakes. All the customer insight needed for everything from SDN screening to targeted marketing is there, waiting to be examined. But obtaining insight from this data is a little like working a 2,000-piece jigsaw. You have all the parts you need, but it takes forever to get the full picture.

3. The regulatory challenge

Financial institutions are heavily regulated. In deploying AI and other new technologies, they must meet stringent and costly regulatory requirements.

The systems banks use to meet KYC standards not only have to work well — flagging bad guys while allowing good guys to bank freely — they must also be transparent enough to allow for compliance reporting. But the nature of AI makes it difficult to explain how AI programs arrive at their decisions.

These systems were built to learn, to mimic human thought processes. Before accepting a diagnosis, we don't typically ask a physician to pinpoint every pertinent piece of information gleaned during her med school classes and clinical experience that led her to reach the decision she did. We accept her diagnosis as the likely truth of our medical condition because she has learned a lot about biology and physiology.

We should have a similar trust in effective AI systems. They come to the conclusions they do because they have been well programmed and have learned from their experience. You may be proud of an AI solution effective enough to automatically close 75 percent of your KYC alerts as false positives. The industry understands that traditional screening systems produce a huge number of false positives. So a system that automatically closes those alerts is a good thing, right?

Not necessarily. Regulators may look at these automatic closures and wonder, *'How?'* How does AI know which alerts are false positives? How does the AI system know it's closing the right alerts?

Even the engineers who designed the AI system can't always say for sure. And that can be a problem. Just as physicians can give bad diagnoses, AI systems can make mistakes. Without understanding why the AI system has erred, it can be hard to update its programming so the errors don't recur — and harder to convince regulators of their efficacy.

That's why "explainable AI" is so important. This set of methods and processes offered by some vendors enables users to better understand what AI is doing, on what data it's basing its decisions, and how to retool the system when mistakes arise.

Clearly, AI is **not** a cure-all. Still, to thrive in an increasingly regulated, increasingly crime-prone, and increasingly competitive age, FIs must deploy artificial intelligence. They need to more efficiently and economically match names, resolve identities, and spot fraud. They need to fish customer insight from their data lakes and beyond.

$800 BILLION TO $200 TRILLION	$1.3 BILLION	$4	50+%	44%
Estimated amount of money laundered annually. This represents anywhere from 2%-5% of the world economy	Dollar amount of fines levied by OFAC against United States banks in 2019	Amount financial institutions spend to resolve each $1 of fraud loss	Percentage of banks worldwide that fail to fully run KYC verification of client data	Percentage of banks worldwide that use no AI at all

What AI can do for FIs today

Improve the fight against money laundering

FIs in the United States and Canada will spend more than $56.7 billion on AML this year, according to LexisNexis estimates.[12] In 2018, the same company estimated that the cost of AML compliance in France, Germany, Italy, Switzerland and the Netherlands hit €70.1 billion.[13]

FIs attribute the lion's share of these costs to the investigation of false positives.

Currently, most AML efforts rely on rules-based systems. In this approach, an AML specialist compiles and codifies a set of conditions that, if met by a particular transaction, causes the system to alert an investigator to potential money laundering. Transactional dollar limits are a classic example of this: AML systems note all transfers over a given amount, then alert an investigator to follow up. While a small fraction of these alerts may indicate criminal activity, PwC estimates that up to 95 percent of the millions of alerts sounded annually are false positives.[14] These false positives make AML detection vastly more expensive than it needs to be: live investigators must review each alert, often spending up to three hours to resolve every false positive.

Worse for society, criminals understand rules-based systems. They camouflage their activities to avoid the types of transactions that trigger an investigation. In the United States, for example, the Currency and Foreign Transactions Reporting Act requires FIs to report deposits and withdrawals of more than $10,000 to the Internal Revenue Services. You know this. Do you think criminals don't? Do you think a drug dealer doesn't know to launder $11,000 in proceeds by structuring deposits in increments: $4,000 at Bank A, $4,000 at Bank B, and $3,000 at Bank C?

Using AI for AML can help FIs stop the bad guys while saving untold millions in false-positive investigations. In fact, a recent "Chartis Research RiskTech100®" report indicates that AI systems can cut false alerts in half.[15] How much would that save *your* FI?

FIs in the United States and Canada will spend more than $56.7 billion on AML this year, according to LexisNexis estimates.[12]

Modernize KYC processes

With granular, varying and ever-evolving KYC requirements for new customers, existing customers, individuals, businesses, government entities and power-of-attorney accounts, it may sometimes feel easier for FIs to risk a fine then to attempt appropriate due diligence. Don't believe it? According to Chartis Research, "In September 2016 … the Hong Kong Monetary Authority issued a company circular warning against the potential negative effects of overly stringent onboarding and [customer due diligence] processes."[16] These disadvantages include long customer onboarding times that may leave some prospects frustrated and looking for another bank. However, lackadaisical attitudes toward KYC put the entire financial system at risk.

Artificial intelligence can forge a path through the KYC jungle. Its multilingual name matching, entity resolution and relationship-discovering capabilities can rapidly identify people, companies, and organizations — and map connections among them. From legal documents to customer emails, AI applications can scour unstructured and structured data in a broad array of languages; create reports; generate detailed relationship visualizations; and tell you how confident it feels in the matches it has made. In doing so, AI slashes KYC costs and times; reduces the chance of fines; and cuts customer onboarding times.

AI helps FIs better understand reporting mandates

Forget improving compliance. Are you having trouble just parsing ever-evolving AML and KYC mandates? Can't figure out which new rules apply to *you*? AI can help. Applications can be programmed to recognize the terms and topics relevant to your firm's AML activities. They can then analyze reams of regulatory updates, and report what matters to your compliance officers.

Hasten fraud detection

Fraud is a complex crime with a direct impact on FIs' bottom line. Financial institutions need every technological resource available to fight it.

AI excels at pattern recognition, a capability that is particularly valuable in fraud detection.

In fact, unsupervised machine learning (a type of machine learning in which algorithms analyze unlabeled datasets, discovering patterns without human intervention) can identify fraud patterns human analysts would not have found on their own.

Still, too few FIs use AI in their fraud-detection efforts. Like AML and KYC processes, most current fraud detection relies on rule-based systems to flag suspicious activity. Fraudsters, like money launderers, learn transaction rules, and ways to avoid them.

AI is a better choice. Machine learning algorithms can analyze petabytes of information in hours, more quickly and accurately detecting fraud patterns.

Increase business through improved customer relationships

In many financial institutions, customer data is either stored in data lakes or scattered across siloed warehouses. To improve customer acquisition and retention efforts, financial institutions need a single, holistic view of each customer. The same AI capabilities used to match names and resolve entities for AML, KYC, and anti-fraud efforts can give FIs a business-critical view of who's who.

Consider the following scenario. State Bank has a plethora of customers named Mary Smith and Harry Smith. Using name matching and identity resolution software, State Bank determines which Mary Smith is married to which Harry Smith. They see that this couple's home is a rental. Examining credit card transactions and account transfers, the bank learns that Mary, who used to spend significant sums at high-end shoe and electronics stores, has lately been putting more and more money into her savings account. Harry, meanwhile, has been shopping at home improvement stores, and has paid a retainer to a lawyer specializing in real estate.

The bank may infer from this information that the couple is buying a house. The bank contacts Harry and Mary with information about mortgages, including special programs available to first-time home buyers. The Smiths decide to work with the bank, solidifying their relationship with the institution for the next 30 years.

Financial institutions operate in a complex, competitive industry. But existing AI capabilities can help FIs more efficiently and cost-effectively comply with regulatory mandates, halt money laundering, fight fraud, and improve business.

Machine learning algorithms can analyze petabytes of information in hours, more quickly and accurately detecting fraud patterns.

Endnotes

1. United Nations Office on Drugs and Crime, "Money Laundering," 2022. https://www.unodc.org/unodc/en/money-laundering/overview.html

2. U.S. Department of the Treasury, Office of Foreign Assets Control - Sanctions Programs and Information. https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information

3. U.S. Department of the Treasury, "2019 Enforcement Actions," 2019. https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information

4. Laumann, Alina "The History of Anti-Money Laundering – Events, Regulations, and Adaptations in the United States," 2019. https://www.kroll.com/en/insights/publications/compliance-risk/history-anti-money-laundering-united-states

5. Hassoumi, Nabli "What the EU 6th AMLD means for your compliance programme," May 7, 2021. https://www.refinitiv.com/perspectives/regulation-risk-compliance/what-the-eu-6amld-means-for-your-compliance-programme/

6. Chen, James "Money Laundering: What it is and How to Prevent It," 2022. https://www.investopedia.com/terms/m/moneylaundering.asp

7. The 117th Congress, 2022. https://www.congress.gov/bill/117th-congress/house-bill/5525?s=1&r=78

8. "LexisNexis® True Cost of Fraud™ Study: Financial Services & Lending." 2022. https://risk.lexisnexis.com/about-us/press-room/press-release/20220106-annual-true-cost-of-fraud-study

9. The World Economic Forum "Forging New Pathways: The Next Evolution of Innovation in Financial Services." 2020. https://www3.weforum.org/docs/WEF_Forging_New_Pathways_2020.pdf

10. "Refinitiv Global Risk and Compliance Report." 2021. https://www.refinitiv.com/en/resources/special-report/global-risk-and-compliance-report

11. ibid

12. "LexisNexis® Risk Solutions 2022 True Cost of Financial Crime Compliance Study: U.S. and Canada Edition." 2022. https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada

13. ibid

14. "From source to surveillance: the hidden risk in AML monitoring system optimization" 2010. https://www.pwc.com/us/en/anti-money-laundering/publications/assets/aml-monitoring-system-risks.pdf

15. Chartis Research Staff, "Risk Tech100(R) 2018," 2018. https://www.chartis-research.com/financial-risk-and-evaluation/credit-risk/risk-tech100r-2018-1190

16. ibid

Babel Street. Unlock the most insights that matter.

Babel Street is the trusted technology partner for the world's most advanced identity intelligence and risk operations. The Babel Street Insights platform delivers advanced AI and data analytics solutions to close the Risk-Confidence Gap.

Babel Street provides unmatched, analysis-ready data regardless of language, proactive risk identification, 360-degree insights, high-speed automation, and seamless integration into existing systems. We empower government and commercial organizations to transform high-stakes identity and risk operations into a strategic advantage.

Learn more at babelstreet.com

BABELSTREET

© 2023 Babel Street Rosette, Ltd. "Rosette" is a registered trademark of Babel Street Rosette, Ltd. All Rights Reserved.