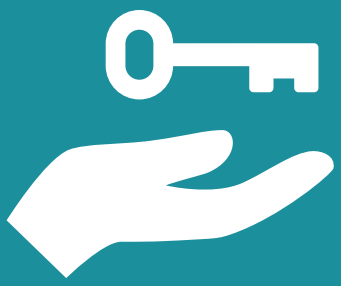
QuantaVerse



How Data Science Can Reduce AML 'Fifth Pillar' Risk

New Technologies Including Artificial Intelligence (AI), Machine Learning And Big Data Enable Banks And Financial Institutions To Surpass KYC Regulatory Requirements

FINANCIAL INSTITUTIONS HAVE LONG RECOGNIZED THE IMPORTANCE OF KNOW YOUR CUSTOMER (KYC) REGULATIONS AND REQUIREMENTS,

yet over time, many institutions came to view KYC as a check-the-box compliance function rather than as a robust risk management tool. This mindset was driven by manpower and systems expenses.

The KYC mindset began to change on April 3, 2016, the day the Panama Papers were released. More than 11 million documents described in excruciating detail how wealthy individuals and some high-ranking public officials used a Panamanian law firm to establish shell corporations for illegal purposes, including the commission of fraud, tax evasion, and avoidance of internationally imposed sanctions.

One month later, and in the midst a global firestorm that ensnared former British Prime Minister David Cameron, the Financial Crimes Enforcement Network (FinCEN) published a Final Rule [1] designed to formalize new and existing customer due diligence (CDD) requirements.

The Final Rule codified four anti-money laundering (AML) provisions or "pillars" found in Section 352 of the USA Patriot Act. FinCEN also added a fifth pillar, requiring covered institutions to:

- Identify and verify the identity of the beneficial or true owner(s) of the account by determining who directly or indirectly owns 25 percent or more of the equity interests of the legal entity customer; or

- Determine which individuals control, manage, or direct a legal entity customer, including an executive officer or senior manager, or any other individual who regularly performs similar functions.

In addition, financial institutions must verify that customer information is based on "reasonable and practicable risk-based" procedures. Covered financial institutions must comply with the fifth pillar rule by May 11, 2018 (the "Applicability Date").

DROWNING IN COMPLIANCE CHALLENGES

The last thing most financial institutions want to tackle is another compliance mandate. Since the enactment of Dodd-Frank in 2010, nearly 23,000 pages of Dodd-Frank-related rules have been published, according to the law firm Davis, Polk and Wardwell. Dodd-Frank compliance has been further complicated by a patchwork of multiple regulations and reporting requirements promulgated by regulators across multiple jurisdictions.

Set against this backdrop, fifth pillar requirements raise additional compliance challenges. For one, current efforts to prevent financial crimes (money laundering, terrorist financing, and fraud) by customers have been costly and ineffective. Many financial executives see no clear roadmap for overcoming known institutional KYC or KYCC weaknesses, which include:

- Incomplete information on the ultimate beneficiary owner/customer when conducting transactions on behalf of a correspondent bank or institutional client;
- Rules-based transaction review systems that look at risk through the "rear view mirror;"
- Reliance on human investigators with varying levels of skills and training;
- Limited research and investigative tools;
- Siloed information that prevents a holistic view of the client or transaction, and;
- Restrictions on sharing information regarding financial bad actors with peer group competitors other than through formal 314(b) methods.

Faced with inadequate approaches to KYC, one way financial institutions have responded is by "de-risking." Internally, this has meant hacking off entire divisions or lines of business. This has resulted in financial institutions terminating or restricting business relationships with longstanding clients and correspondent banks.

APPLYING DATA SCIENCE TO ENSURE GOOD BANKING RELATIONSHIPS

At its core, data science involves using automated methods to analyze massive amounts of structured or unstructured data, and then extracting knowledge from the filtered results. Data science typically comprises artificial intelligence (AI), machine learning, behavioral science, and Bayesian statistics to create analytical algorithms to model patterns of behavior.

When undertaken in a comprehensive way, data science can help financial institutions to reduce AML risk -- this includes addressing fifth pillar obligations without undertaking the expensive manual process of asking clients highly intrusive questions or blindly trusting the answers that are provided on forms and applications.

Data science and AI strategies useful to supporting KYC requirements include, but are not limited to:

- Link Analysis: Evaluates relationships or connections between various types of objects (nodes), including people, organizations, and transactions. Link analysis today is widely used in search engine optimization as well as in investigations, intelligence, security analysis, and market and medical research.
- Transactional Analysis: Through a risk-based approach, data science evaluates a pre-determined amount of transactional data and identifies suspicious activity related to the KYC subject. Data science techniques then "learn" what activity is expected and alerts the KYC team to anomalies before traditional transactional monitoring systems would detect the out of bounds transactions.
- Outside Investigative Sources: Through a data science-based examination of e-mails, phone numbers, addresses, and other customer identification program (CIP) information, anomalies can be quickly identified in customer activity through fraudulent account activity, social media monitoring, open source data, and other data points.

All of the above data science-enhanced KYC tools can allow institutions to conduct KYC and AML operations cheaper and more effectively. To illustrate this point, John X. Smith is a customer of Our Bank US and has the following CIP (Customer Identification Program) information:

- Date of birth
- Residence/address
- Social security number
- E-mail address
- Mobile phone number
- Occupation
- Twitter username/handle
- Smith's account is expected to be used for bill payment and a few ATM withdrawals of about two to five per month

With a data science-powered solution, compliance leaders would see that his address is being used by five other customers in different parts of the state and Smith's date of birth and social security number are also being used by at least five other bank customers. The data science solution would also reveal that Smith's e-mail and Twitter username/handle are being detected in chat rooms and social media posts related to drug use and trafficking. The data science solution would also reveal after an analysis of 90 days of transactional activity that Smith and 10 other customers are transferring money between accounts and are involved in structuring related transactions through consecutive ATM withdrawals and deposits.

The above hypothetical KYC example depicts how a data science-solution, such as the technology offered by QuantaVerse, could instantly perform requisite KYC on the customer, alleviating costly staff reviews of data. A data science solution would also be able to quickly flag customers as high risk, which would enhance institutions' ability to enhance the enterprise risk assessments.

PAINTING CLIENT PORTRAITS THROUGH FIFTH PILLAR NODES

The traditional method of verifying the beneficial or true owners of an account routinely fails to identify connections between customers and their underlying motives. That's why data scientists start from a macro perspective. They pose basic questions about beneficial ownership and seek to escalate their understanding of the connections between account ownership (who), account set up (what), and account purpose (why). For example:

- Who registered the company?
- Who owns the company?
- Who are the employees?
- Who is on the payroll?
- Who manages the company?
- Who is on the board of directors?
- How is the company registered?
- What IP address is being used for banking and where is the IP related (registered)?
- Is the IP being used in any other parts of the bank for other customers?
- Where is the company registered?
- What law firm registered the company/serves as the registrant?
- Does the company have active addresses that correspond to its business activities?

To obtain this basic level of information, open source data, government or commercially produced data, 314 (b) responses, SWIFT (Society for Worldwide Interbank Financial Telecommunication) messages, and other available sources are used. Data science enhances the above data points through transactional data, link analysis, and machine learning to uncover clear patterns, and anomalies to those patterns, regarding a company's business operations including but not limited to:

- With what organizations or individuals does the entity transact business?
- What financial relationships does the entity have with suppliers or vendors?
- What transactions are happening with customers?
- Which bank accounts are being used?
- What is the frequency of money transactions with each entity?
- What are the general sizes of transactions with various entities?

By automatically polling messages associated with transactions, more data is fed into the analysis. For example, payments identified as "payroll" provide insight into other business patterns and may serve to identify new nodes. Data analysis can determine if the entity is practicing a legitimate and consistent pattern of making payroll. It can check payroll transactions against employee rosters. It will also find disparities in patterns whether in amount paid, frequency, or bank account number.

These data science techniques enable financial institutions to go well beyond bank data and client self-reporting to inform KYC determinations. Through the use of algorithms and by tapping independent and external sources of information, data science-powered solutions are able to define specific risk factors for affiliated institutions or customers and predict future risk trends. This approach is capable of:

- Automatically addressing fifth pillar requirements;
- Eliminating prospective customers from consideration out-of-hand by identifying bad actors; or at least
- Providing investigators with the intelligence needed to drastically shorten the time they require to manually review and retire a case.

These methods enable financial institutions to substantially reduce AML risk and retain the revenue earned from legitimate clients they might have otherwise been forced to abandon through de-risking or expanding compliance costs.

Data science enables financial institutions to go beyond traditional KYC efforts and actually predict what customers might do. Once a client portrait emerges, it becomes possible to predict or model future customer actions, which can be used to reduce regulatory risks and costs, identify lucrative cross-selling opportunities, or create entirely new data-oriented products and services.

A MORE COMPLEX COMPLIANCE FUTURE

By using data science to delve deeper into customer transactions and relationships, financial institutions could prepare for a more regulated future. Data science is uniquely suited to address the increasing country, customer, and product-specific regulations from federal and state regulators.

Speaking at the Society for Worldwide Interbank Financial Telecommunication's April 2015 business forum, Thomas Piontek, head of regulatory services at Commerzbank AG, believes the financial services industry by 2020 will "step away from customer identity and verification and look much more at customer transactions." [2]

Delving deeper into customer transactions allow banks to analyze cash flows coming in and out of a particular client, partner, and/or country. This would enable financial institutions to better know their customers, their customers' customers, and the risk posed in each country where their customers conduct business.

QuantaVerse's data science approach enables banks and financial institutions to surpass regulatory required KYC decisions. Through tactical and strategic financial crime focused algorithms, coupled with independent and external sources of information, data science-powered solutions from QuantaVerse can define specific risk factors for affiliated institutions or customers and predict future risk trends.

ABOUT QUANTAVERSE, LLC.

QuantaVerse is the emerging leader in data science-powered risk reduction solutions, purpose-built for the banking industry. Utilizing proprietary data science algorithms including artificial intelligence (AI), machine learning and big data technologies, QuantaVerse integrates and filters internal bank data and related external data – including public Internet data, unstructured deep web data, as well as government and commercial datasets – to help the banking industry to significantly improve their compliance with AML, KYC and BSA regulations and requirements. For more information, contact QuantaVerse at (610) 465-7320 or visit www.QuantaVerse.net

To learn how QuantaVerse data science powered solutions can benefit your financial institution, contact QuantaVerse at (610) 465-7320 or visit http://www.QuantaVerse.net for more information.

1. Federal Register/ Vol. 81, No. 47 / Thursday, March 10, 2016 / Proposed Rules, Wednesday, May 11, 2016.

2. Bailey Reutzel, 'Know Your Customer's Customer' Goes Global, American Banker, April 27, 2015.