PARTNER. ADVISOR. CATALYST.

Contextual Decision Intelligence: Raising the Bar of AML Detection and Investigation

AUGUST 2020

Charles Subrt

Colin Whitmore

Complimentary access to this Aite Group report is provided by:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This Impact Report sets forth a case study that explores the imperative for new and emerging anti-money laundering (AML) technologies for the financial services industry. It reveals how tools such as dynamic segmentation, entity resolution, network link analysis, and advanced analytics deliver greater risk coverage, more efficiently and effectively disrupting crime.
- Global financial institutions face a constantly evolving and escalating threat landscape. It becomes imperative for FIs, especially in higher-risk operations, to build vibrant and agile risk mitigation frameworks. Yet a litany of demanding challenges stands in the way of their ability to design, implement, and sustain effective AML compliance programs and systems.
- In 2019, an estimated US$10 billion in fines was levied for noncompliance with AML and sanctions obligations. Many enforcement actions cite ineffective risk-based frameworks, insufficient monitoring systems and review of suspicious activity, and insufficient resources. These issues accentuate the pressure on FIs to leverage innovation and next-generation technology to enhance effective Know Your Customer (KYC)/customer due diligence (CDD) processes, surveillance systems, and alert handling practices.
- Recognizing the upside of emerging technologies, regulators around the globe are encouraging the accelerated use of innovation to lift financial crime detection.
- The imperative exists, and the time to act is now. Today's technologies offer FIs groundbreaking ways to embed intelligence, efficiency, and effectiveness into their AML compliance programs; achieve regulatory compliance; and establish vibrant risk management practices. They can unlock the potential within a large volume of data, build holistic party views and networks of relationships, and deliver elevated financial crime surveillance, detection, and investigation.
- This case study was sponsored by Quantexa, a global software and solutions company headquartered in London that provides innovative and contextual decision intelligence and monitoring solutions for the fight against financial crime.

INTRODUCTION

The appalling money laundering scandal known as the "Russian Laundromat" is a well-known tale within the AML compliance community. The depth and extent of the scheme sent shock waves across the globe. For over four years, billions of dollars illegally flowed out of Russia through many of the world's largest international FIs to numerous Russian oligarchs and other corrupt individuals. Clandestine beneficial owners used shell companies and other opaque corporate structures, and complex transactions touched offshore tax havens and other high-risk jurisdictions. It took an investigation by an association of journalists, known as the Organized Crime and Corruption Reporting Project, to expose the scheme.[1] How were these seemingly obvious signs of illicit activity missed by global FIs and their AML compliance functions and monitoring systems?

The international fight against financial crime is not a new one. Regulators around the world impose extensive obligations on FIs to prevent and detect money laundering, terrorist financing, and other crime. Every year, FIs devote massive amounts of time, money, and resources to comply. But FIs often fail to detect money laundering and illicit activity, as in the Russian Laundromat. And the task becomes increasingly challenging when it is connected to more complex and institutional operations, such as correspondent banking, capital markets, and trade finance. Traditional AML approaches and legacy rules-based monitoring are no longer enough as a high volume of false positive alerts and highly manual investigative practices thwart FIs' best efforts. In order to more effectively address existing and emerging AML risks as well as manage the cost of compliance, AML leaders need data-driven and intelligent tools that can more quickly and optimally connect the dots in the data and empower more contextual financial crime detection and investigation.

This Impact Report sets forth a case study that explores the imperative for new and emerging AML technologies for the financial services industry. It reveals how tools such as dynamic segmentation, entity resolution, network link analysis, and advanced analytics deliver greater risk coverage as well as efficiently and effectively disrupt crime.

METHODOLOGY

The case study was sponsored by Quantexa, a global software and solutions company headquartered in London that provides innovative and contextual decision intelligence and monitoring solutions for the fight against financial crime. Aite Group interviewed executives from Quantexa and Standard Chartered about Quantexa's technology and its recent deployment at Standard Chartered for the purpose of discovering insights associated with integrating next-generation AML technology.

1. Emily Benson, "What Can We Learn From the Lawbreaking 'Russian Laundromat' Scandal?," Keystone Law, May 8, 2019, accessed March 11, 2020, https://www.keystonelaw.com/keynotes/what-can-we-learn-from-the-lawbreaking-russian-laundromat-scandal.

THE AML TECHNOLOGY IMPERATIVE

Money laundering and terrorist financing are connected to numerous crimes and illicit activities—political corruption, fraud, human trafficking, cybercrime, drug trafficking, and transnational organized crime, just to name a few. Historically, both the public and private sectors have focused much of their attention and resources on the initial placement of cash into the financial system and the inherent risks in the retail and depository arms of FIs. However, that dynamic is changing considerably.

Global FIs face a constantly evolving and escalating threat landscape arising from their vast diversity of products, business lines, markets, and delivery channels. Due to their complex and international nature, correspondent banking, capital markets, and trade finance are highly vulnerable to financial crime, money laundering, and other illicit activity. As global regulators advocate for risk-based approaches to fighting financial crime, it becomes imperative for FIs, especially in higher-risk operations, to build vibrant and agile risk mitigation systems commensurate with their risk, and to allocate resources to higher-risk activities and parties.

But designing, implementing, and sustaining effective AML systems is not easy, and FIs face a litany of demanding challenges. Up until now, legacy technology has hindered FIs' ability to effectively and efficiently tackle the increasingly complicated ecosystem. However, advancements in technology are empowering FIs to better identify and appreciate their risks and thus make smarter decisions. Tools such as dynamic segmentation, entity resolution, and network link analysis can help FIs unlock the potential within data by ingesting and reconciling a large volume of data from multiple sources and building holistic party views and networks of relationships. Advanced analytics can provide new and revolutionary ways to conduct KYC/CDD processes and financial crime surveillance, detection, and investigation. The future of next-generation AML technology is now, and FIs cannot afford to wait.

Table A provides a snapshot of key challenges obstructing effective AML risk mitigation and the AML technology imperative to overcoming them.

Table A: Key AML Compliance Challenges

Key AML compliance challenges	AML technology implications
Faster and more complex payment streams, increasing digitalization of products and services, and continual innovation in financial services elevate financial crime risk. Keeping up with new products and services is a major FI concern.	Heavy dependence on manual processes and legacy rules-based technology impairs AML efficiency—wasting time on unnecessary investigations, diverting attention from higher-risk events, and potentially eroding control effectiveness. FIs need tools that deliver better and more real-time enterprise risk analysis, leading to more effective detection and more efficient investigation.
Benefiting from innovation, financial criminals are becoming smarter, better organized, and more professional than ever before. Many are exploiting the vulnerabilities inherent within correspondent banking, capital markets, and trade finance operations.	As sophisticated criminals operate across complex networks, making illicit activity hard to identify, it becomes imperative for FIs to integrate smarter and more real-time surveillance, interdiction, and data collection capabilities.

Key AML compliance challenges	AML technology implications
Global regulators are increasing expectations on FIs and pushing for greater transparency. As many recent money laundering scandals and AML compliance deficiencies relate to correspondent banking, capital markets, and trade finance, regulators are intensifying their scrutiny of these sectors.	Expanding sanctions, increasing beneficial ownership obligations, and escalating regulatory expectations accelerate the imperative for enhanced AML technology. As FIs focus more on effective outcomes and less on strict technical AML compliance, they must transition away from legacy rules-based functionality and adopt more proactive and intelligent tools tailored to their specific inherent risks.
Built on primarily rules-based logic, legacy monitoring systems limit the effectiveness and efficiency of most AML frameworks. A high volume of false positive alerts drives up costs and headcount, while questionable activities, networks, and relationships often go undetected.	Smarter AML tools can deliver more meaningful alerts, enabling FIs to concentrate resources on genuine financial crime risk, detect illicit activity, and present higher-quality intelligence to law enforcement. More meaningful output will lessen the manual burdens on current investigative processes. The challenge is reconciling all the disparate data.
Data represents the most important asset in fighting financial crime. The volume and breadth of available data are expanding. Yet data is frequently fragmented, siloed, and incomplete. Harnessing data to feed financial crime analytics and detection remains a primary pain point for FIs.	High-quality AML data is difficult to exploit, as much of it is encapsulated within unstructured formats. Extracting insights within structured and unstructured data, both internal and external, requires new technologies that can digest, reconcile, enrich, and consolidate extensive and often disparate data streams as well as create holistic views of parties and transactions.
FIs seek seamless customer experiences and augmented operational efficiencies. But extended beneficial ownership obligations, fragmented data, and heavy reliance on manual processes hinder customer onboarding and resource productivity.	Needing to find new ways to do more (i.e., enhance the rigor, speed, and quality of financial crime detection and investigation), often with a lower headcount, AML leaders recognize that new technology can bring increased capacity and productivity. Holistic customer views can deliver faster and smarter KYC/CDD decision-making, minimize customer friction, and, at the same time, elevate AML risk mitigation.
Recognizing new technology's enormous potential, global regulators are increasingly promoting innovation and advanced techniques to elevate financial crime detection.	In addition to knowing AML requirements as well as the key threats, risks, and typologies, AML leaders and their teams must cultivate expertise in the new technologies, data science, and analytics, and successfully leverage innovation. Otherwise, effective and efficient risk mitigation may be practically impossible.

Source: Aite Group

THE RUSSIAN LAUNDROMAT CASE: LESSONS LEARNED

In the Russian Laundromat scheme, an estimated US$20 billion moved out of Russia to FIs around the world between 2011 and 2014. The perpetrators were largely wealthy Russians with links to the Kremlin who diverted funds from the Russian state through fraud, political corruption, and tax evasion. Using shell companies to conceal their identities, the illicit actors created false debt among each other. Corrupt judges substantiated the debt, thus facilitating billions being transferred and "cleaned" through accounts at two banks in Moldova and Latvia, with much of the money ending up at some of the world's largest global FIs. Today, law enforcement continues to investigate, as many actors involved remain hidden and much of the laundered funds are yet to be recovered.[2]

For its involvement, one European bank has reported that it expects "significant disciplinary action," as substantial funds were funneled through its correspondent banking network. Its involvement has likely caused the bank significant reputational harm and loss of customer and shareholder confidence.[3] Other banks are experiencing similar consequences.

So, what lessons can FIs take away from this scandal? It is clear that financial criminals are deploying new and sophisticated ways to exploit the multiple access points into the financial system. And to effectively tackle sophisticated global money laundering schemes, FIs must take a more dynamic, innovative, and hyper-vigilant data-driven approach to KYC/CDD as well as financial crime detection and investigation.

2. "The Russian Laundromat Exposed," Organized Crime and Corruption Reporting Project, March 20, 2017, accessed January 3, 2020, https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

3. Luke Harding, "Deutsche Bank Faces Action Over $20bn Russian Money-Laundering Scheme," The Guardian, April 17, 2019, accessed January 3, 2020, https://www.theguardian.com/business/2019/apr/17/deutsche-bank-faces-action-over-20bn-russian-money-laundering-scheme.

THE EVER-EVOLVING REGULATORY LANDSCAPE

As organized crime furthers its attack on the entry points into the financial system, the public sector becomes increasingly concerned about the effectiveness of AML regimes across the globe. Toughening AML standards are amplifying the obligations and expectations on FIs as more vigorous and risk-based approaches to AML compliance and detection are mandated. Governments continue to use sanctions as fundamental foreign policy tools to exert pressure on dangerous persons, entities, and political regimes for perceived risks to national security and human rights.

Table B provides a snapshot of recent regulatory developments across the globe, particularly those affecting correspondent banking, capital markets, and trade finance operations.

Table B: Regulatory Developments Overview

Regulation/industry guidance	Date	Jurisdiction	Regulatory overview
Fifth AML Directive	2020	EU	Substantially enhancing the Fourth AML Directive, the Fifth AML Directive strengthens and harmonizes the EU AML regime, boosts CDD and underlying beneficial ownership requirements, and elevates the powers of EU financial intelligence units.[4]
U.S. Department of the Treasury's 2020 Strategy for Modernizing the U.S. AML Regime	2020	U.S.	The 2020 Strategy underscores the U.S. Treasury's key priorities for disrupting and preventing illicit finance activities. The U.S. Treasury clearly expects supervised entities to instill dynamic, risk-based, and targeted approaches to AML compliance; deploy innovative and intelligent approaches to financial crime detection; and generate actionable intelligence for law enforcement.
Joint Statement on Risk-Focused Bank Secrecy Act/AML Supervision	2019	U.S.	The Financial Crimes Enforcement Network (FinCEN) and other U.S. regulatory bodies issued a joint statement underscoring the importance of appropriately calibrating FI AML programs to identified risks.
The Wolfsberg Group, the Bankers Association for Finance and Trade, and the International Chamber of Commerce's Trade Finance Principles (2019 amendment)	2019	Global	The 2019 update of the Trade Finance Principles expands guidance addressing the core risk mitigation and due diligence activities expected of FIs arising out of the financing of international trade.

4. See Aite Group's report *Introducing the Fifth Anti-Money Laundering Directive: Are You Ready?*, February 2020.

Regulation/industry guidance	Date	Jurisdiction	Regulatory overview
The Wolfsberg Group's Statement on Effectiveness	2019	Global	The Statement on Effectiveness champions a supervisory approach that focuses more on effective outcomes and less on technical AML compliance. The statement accentuates that many FIs are concentrating too much on technical compliance, which may not always elevate the detection and deterrence of illicit activity.
Financial Conduct Authority's (FCA's) Understanding the Money Laundering Risks in the Capital Markets thematic review (FCA Thematic Review)	2019	U.K.	The FCA Thematic Review notes that capital markets transactions are often complex and involve multiple jurisdictions and parties, and no individual firm has a holistic view of the end-to-end transaction. The FCA Thematic Review cites the fact that certain FIs are embedding transaction monitoring systems with network analysis and contextual monitoring capabilities.
FinCEN's CDD Requirements for Financial Institutions (CDD Rule)	2018	U.S.	The CDD Rule requires legal entity beneficial ownership identification and verification. Given multifaceted and often opaque corporate structures, the new CDD requirements foist substantial customer data requirements on FIs.

Source: Aite Group

RECENT ENFORCEMENT ACTIVITY

Even as FIs invest significantly in AML compliance, many are unable to sustain effective CDD and transaction monitoring practices. Weak and inadequate AML controls continue to be identified, and the consequences for failure can be severe. FIs can suffer harsh fines, reputational damage, loss of investor and consumer confidence, and diminished market value. Repairing brand and customer trust can be, and may often be, unachievable. Significant time, money, and resources can be exhausted defending allegations, negotiating regulatory settlements, appointing independent monitors, and remediating deficiencies. Compliance officers, executive management, and board members can face civil and criminal liability.

In 2019, an estimated US$10 billion in fines was levied for noncompliance with AML and sanctions obligations, with some individual penalties exceeding US$1 billon.[5] Many enforcement actions cite common AML control deficiencies—ineffective risk-based frameworks, lack of internal sanctions controls, insufficient monitoring systems, incomplete or missing customer and transaction data, inadequate review and reporting of suspicious activity and alert backlogs, and insufficient resources devoted to alert investigations. This commonality of gaps and weaknesses

5. "AML, KYC & Sanctions Fines for Global Financial Institutions Top $36 Billion Since Financial Crisis," Fenergo, January 29, 2020, accessed March 13, 2020, https://www.fenergo.com/news/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-$36-billion-since-financial-crisis.html.

accentuates the pressure on FIs to leverage innovation and next-generation technology in enhancing effective KYC/CDD processes, surveillance systems, and alert handling practices.

Table C encapsulates recent AML enforcement activity against FIs for AML compliance deficiencies associated with correspondent banking, capital markets, and trade finance.

Table C: Recent AML Enforcement Actions

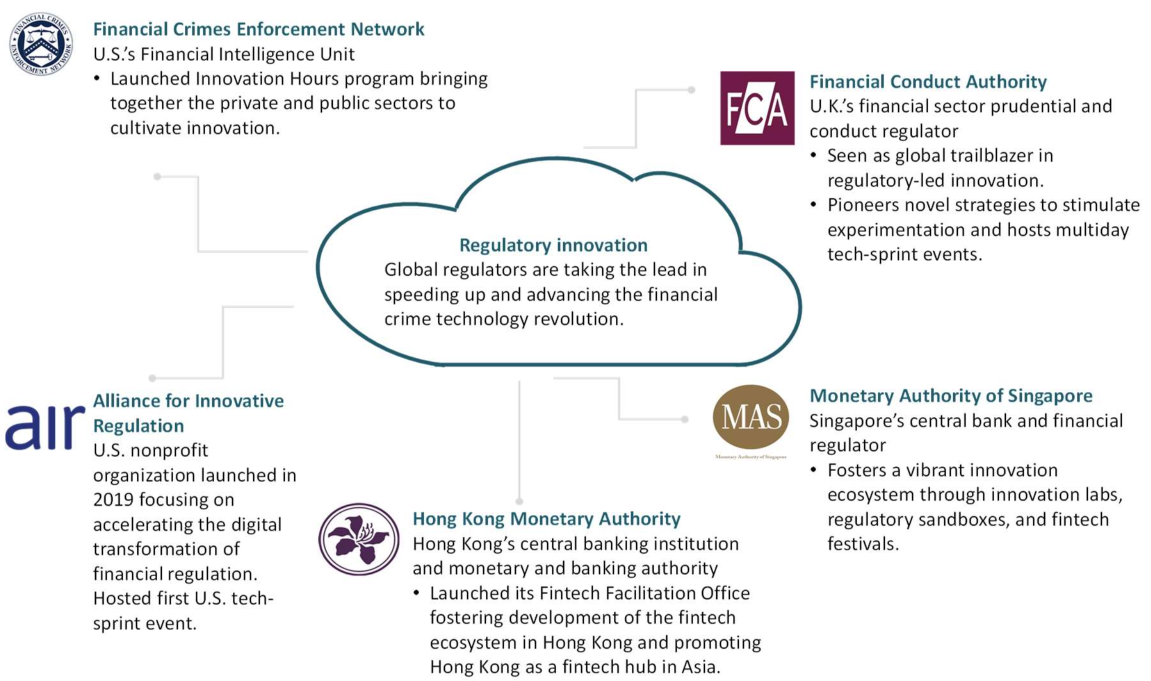
Regulators	Date	Amount	AML compliance deficiencies
Financial Industry Regulatory Authority (FINRA)	October 2019	US$15 million	Significant systemic AML deficiencies within the bank's broker-dealer operation, identifying a lack of targeted suspicious activity monitoring of penny stock transactions and inadequate review of wire transfers
New York State Department of Financial Services (NYDFS)	June 2019	US$33 million	Internal AML control weaknesses relating to foreign correspondent due diligence, transaction monitoring, and trade finance monitoring, citing failures to file reports on suspicious customer activity in a timely manner, insufficient enhanced monitoring of high-risk transactions, and a lack of appropriate AML staffing
NYDFS, New York County (Manhattan) District Attorney, U.S. Department of Justice, the Federal Reserve, Office of Foreign Assets Control	April 2019	US$1.3 billion	Failures in sanctions controls, citing thousands of transactions over a multiyear period in violation of U.S. economic sanctions, largely related to Iran
FinCEN, FINRA, and the Securities and Exchange Commission	December 2018	US$14.5 million	AML controls issues, citing ineffective oversight and monitoring of foreign currency wires and transactions in low-priced equity securities, especially those involving high-risk countries
FINRA	December 2018	US$10 million	Inadequate transaction surveillance of wire transfers and transactions in low-priced equity securities, citing ineffective monitoring systems, lack of critical data, insufficient alert investigations, and insufficient resources
NYDFS	October 2018	US$40 million	Insufficient risk-based AML and sanctions programs for the bank's correspondent banking, trade finance, and U.S. dollar clearing services for clients located in Southeast Asia, the Middle East, and Northern Africa, citing inadequate CDD, alert backlogs, and failures to identify and report suspicious transactions

Source: Aite Group

ACCELERATED REGULATORY PROMOTION FOR INNOVATION

Historically, adoption of advanced analytics in AML has been slowed by the regulatory concerns for transparency and explainability. However, recognizing the upside of emerging technologies, many regulators around the globe are advancing fintech and regtech experimentation and encouraging the accelerated use of innovation to lift financial crime detection,[6] as illustrated in Figure 1 and described further below.

Figure 1: Regulatory Innovation Around the World



Source: Aite Group

- **U.K.:** The FCA has pioneered many initiatives to stimulate innovation across the financial industry and aid investments in fintech. Its tech-sprint program fosters collaboration among technology and compliance experts across the financial services industry, spawns new learnings and ideas, and helps to discover actionable technology-driven solutions to critical challenges facing the financial industry. Many of its tactics have been emulated by other regulators around the world.

- **Singapore:** The Monetary Authority of Singapore (MAS) fosters a vibrant innovation ecosystem through its sponsorships of innovation labs, regulatory sandboxes, and fintech festivals. For example, in 2015, the MAS established the Fintech and Innovation Group to expedite technology penetration across Singapore's financial sector.

6. See Aite Group's report *Regulatory Innovation, Sandboxes, and Tech Sprints: Trends and Global Initiatives*, March 2020.

- **Hong Kong:** In 2016, the Hong Kong Monetary Authority (HKMA) established the Fintech Facilitation Office to advance Hong Kong's fintech development and promote Hong Kong as a fintech hub in Asia.

- **U.S.:** Numerous U.S. regulatory agencies are launching pilot programs and other broad initiatives to push innovation:

  - In December 2018, the U.S. Treasury Department's AML unit and U.S. federal banking regulators issued a joint statement that encouraged innovation and experimentation.
  - In May 2019, FinCEN launched an Innovation Hours program designed to bring the private and public sectors together, cultivate experimentation, and find innovative approaches and solutions to the never-ending struggle against crime, saying that "Responsible innovation can be an important part of safeguarding the U.S. financial system against new and evolving threats related to money laundering, terrorist financing and other serious financial crimes."[7]
  - In July 2019, the Alliance for Regulatory Innovation, working in partnership with the FCA, brought representatives from FIs, technology companies, and several U.S. federal regulatory agencies together in Washington, D.C. for the first-ever U.S. regulatory tech-sprint. For four days, the event explored how new technology can more efficiently and effectively combat money laundering and financial crime.

7. "FinCEN's Innovation Hours Program," FinCEN, May 24, 2019, accessed August 4, 2020, https://www.fincen.gov/resources/fincens-innovation-hours-program.

AML TECHNOLOGY: THE FUTURE IS NOW

Legacy AML systems, relying heavily on rules-based logic and basic anomaly detection, often hamper FIs' ability to design, embed, and sustain effective and efficient risk-based AML practices as well as keep pace with new and emerging threats. Because much traditional automated financial crime surveillance focuses primarily on transactional activity and less on a holistic customer view, it can be ineffective and generate a high volume of alerts. As such, AML investigators are often asked to manually sort through extensive information, regularly stored in digital files and records in multiple systems, and build the necessary context for decisioning. Often, questionable activities, networks, and relationships can go undetected.

The financial services industry has recognized that the legacy approach may not be enough. The United Nations Office on Drugs and Crime estimates that between 2% and 5% of global gross domestic product is laundered annually, which translates to between US$800 billion and US$2 trillion per year. Less than 1% of this is caught. FIs must act now and modernize their AML programs. Today's technologies can deliver groundbreaking ways to embed intelligence, efficiency, and effectiveness into their AML compliance programs; achieve regulatory compliance; and build vibrant risk management practices.[8] The following discussion expounds upon the emerging key AML technologies.

ENTITY RESOLUTION

Everything starts with the data. Most AML leaders recognize the promise of effective risk-based KYC/CDD and that financial crime detection necessitates quality data linked together and enriched from multiple sources. However, harnessing the data for effective analytics and detection is often cited as one of the top pain points for FIs.[9] FI data is frequently messy, with multiple records for a single party, name variants, address issues, typos, inaccuracies, and omissions, and it is often fragmented and siloed across disparate systems and business lines. Moreover, because most legacy AML monitoring platforms are unable to ingest and process unstructured data, current surveillance primarily analyzes data only available in structured form.

To elevate KYC/CDD and financial crime detection, FIs require sophisticated data wrangling and entity resolution tools that can cope with poor data quality issues. Entity resolution technology can connect data across internal and external data sources and generate a single holistic party (often a customer) profile or view. Entity resolution not only triangulates data across multiple internal sources but also enriches it with third-party sources.

By constructing fuller, richer, and more consistent customer views, entity resolution can enable more streamlined KYC/CDD processes, greater operational efficiencies, and more effective allocation of resources to more complex and higher-risk activities. Further, it can create the

8. See Aite Group's report *AI-Enabled Anti-Money Laundering: From Theory to Reality*, July 2020.

9. See Aite Group's report *Key Trends Driving AML Compliance Transformation in 2020 and Beyond*, November 2019.

additional contextual intelligence advantageous for smarter and faster profiling, segmentation, and decision-making.

NETWORK LINK ANALYSIS/NETWORK GENERATION

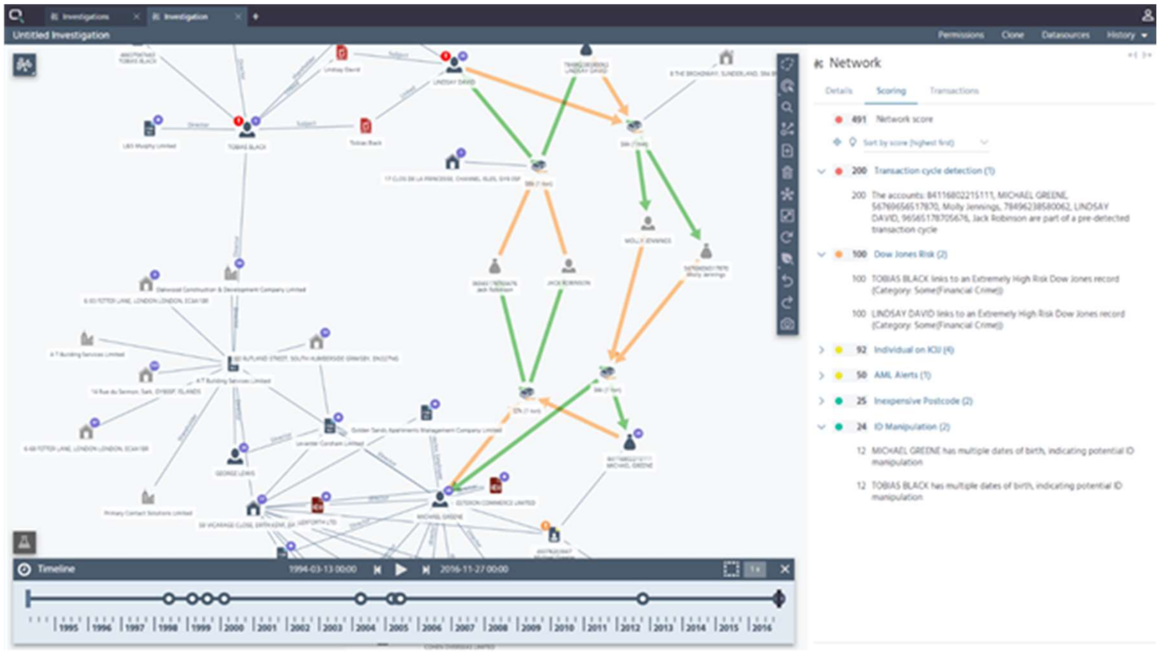
Through their ability to ingest and analyze vast amounts of data, often in real time, network link analysis/network-generation technologies can find relationships and connections—often unknown or hidden—among parties, accounts, and transactions, and graphically display them in user-friendly and easily digestible images and diagrams. Relationships can be connected through data items such as shared addresses, telephone numbers, and company associations, and payment flows and other transactions can be linked across common legal hierarchies or business groups. The ability to construct and refresh network linkages in real time or near-real time is an increasingly essential component to keeping up with the pace of financial crime.

By providing enhanced intelligence and additional context, network link analysis/network-generation tools can accomplish the following:

- They can enrich KYC/CDD practices by identifying and tracking underlying beneficial owners and their associations, and facilitate customer risk evaluations and due diligence reviews. As large corporate entities and high-net-worth individuals have complex, interconnected ownership structures, conducting KYC/CDD frequently requires extensive research and months to complete.
- They can optimize financial crime detection and investigation, especially of complex AML typologies used by the most sophisticated criminals, by graphically displaying identified networks in an interactive manner and highlighting risks for investigators. For instance, most investigators can currently spend 70% to 80% of their time gathering and creating contextual information, leaving less time for decision-making.
- As additional inputs into segmentation and analytical models, they can advance automated detection capabilities. For example, network generation tools can build segments within entity customers by identifying and clustering together underlying international beneficial ownership structures or transactions associated with counterparties in foreign high-risk jurisdictions. Moreover, by connecting inter-related ownership structures and transactions, these tools can link parties to known criminals and money launderers.

Figure 2 provides a good example of graphical link analysis.

Figure 2: Graphical Link Analysis



Source: Quantexa

DYNAMIC SEGMENTATION

Legacy AML systems typically assign customer risk scores based on information gathered at the time of onboarding, and they modify those scores only upon the triggering of certain rules-based criteria. Using new advanced analytics and machine learning data-clustering technology, dynamic segmentation can analyze customer behavior and dynamically create risk-based segments depending on that analysis. As customer financial and transactional profiles change, these segments will evolve. Dynamic segmentation techniques enable more proactive, risk-based, and customer-centric approaches to KYC/CDD, ongoing monitoring, and financial crime detection.

Dynamic segmentation becomes particularly important when monitoring correspondent banking, capital markets, and trade finance, where involved parties use complex corporate structures and instruments, and their activity can vary greatly. Dynamic segmentation considers company size, structure, and associations and transaction networks as well as the specific details associated with the related parties and transactions.

NATURAL LANGUAGE PROCESSING (NLP)

NLP technology converts unstructured data, such as text or audio, into structured data that can then be read and deployed for additional purposes. NLP can be used for automated summarization, language translation, keyword tagging, real-time adverse media and negative news analysis, and grammar analysis. For example, NLP can enable text parsing and elastic searches of unstructured data for high-risk or sanction indicators in payment transactions.

ADVANCED ANALYTICS

Advanced analytics models can help FIs maximize the value of their data and make more informed and consistent decisions faster. Through iterative optimization, advanced analytics and machine learning models can run across a large volume of data to sharpen risk recognition, hone customer monitoring, detect financial crime red flags, and minimize false positive alerts. As more data is processed, more intelligence is fed back into the models, and detection can become smarter, driving more accurate focus on true suspicious activity. The accuracy of these models can be further sharpened by integrating enhanced context in the form of resolved entities and interconnected networks. Introducing these additional inputs becomes critical in delivering better detection, increased risk coverage, and a lower volume of false positive alerts. Advanced analytics can also enhance rules and scoring algorithms within existing monitoring platforms.

Machine learning models can be deployed across various AML use cases. This becomes imperative when mitigating the elevated risks associated with correspondent banking, capital markets, and trade finance, which are more vulnerable to illicit activity due to their global and cross-border transactional nature, the volume and speed of their activity, and their use of multiple intermediaries. Transparency and a documented understanding and explainability of how the data inputs generate the alert output are still important points for regulators, however.

OTHER KEY CONSIDERATIONS

AML solutions using next-generation technologies must consider and address other essential needs of global FIs, as follows:

- **Integration and flexibility:** Next-generation platforms should be able to coexist and integrate with other technologies, systems, and data sources as well as enable third-party commercial or open-source innovations to be quickly deployed. Many FIs, already heavily invested in their current AML technology stacks, are seeking complementary functionality as opposed to replacement solutions.
- **Global data privacy and security:** With the intensifying complexity of data privacy protections governing the use of customer data, its storage, and cross-border data access and usage, solutions must support local data governance, privacy, and security obligations.
- **Scale:** Next-generation platforms should be able to resolve entities, generate networks, and run models across a large volume of records, including not only static customer and ownership information, but the full complement of transactional data.
- **Transparency and explainability:** Even as regulators actively promote innovation, they still expect the new functionality to be fully explainable and its effectiveness to be substantiated.

QUANTEXA: THE CONTEXTUAL DECISION INTELLIGENCE APPROACH

Founded in 2016, Quantexa delivers solutions into the marketplace that are transforming how its clients are using innovation to fight financial crime, especially when dealing with high-net-worth individuals and complex corporate structures, and in high-risk operations, such as correspondent banking, capital markets, and trade finance. Quantexa leverages real-time entity resolution, network generation, and advanced analytics to empower contextual decision intelligence that can drive better insight and actionable intelligence from data as well as enable faster, more informed, and more accurate detection, investigation, and decision-making. Through open architecture, its platform integrates with existing IT and data stacks, and it complements existing technologies.

At its core, Quantexa's platform resolves, enriches, and links together vast and disparate data sets and constructs more complete and holistic party profiles and networks of connections found in the data, often previously unknown or hidden. Its framework can ingest data from third-party sources as well as those generated from other internal systems and processes, such as text analytics, transaction monitoring, and risk scoring platforms. The Quantexa approach can yield greater context, meaning, and understanding of customers and other parties, and their connected relationships, behaviors, and risks. By leveraging third-party sources, Quantexa's technology can also help build underlying corporate ownership structures. Through dynamic segmentation and advanced analytics methods deployed across the enriched network, the Quantexa platform can identify outliers and anomalies and generate highly accurate and relevant alerts.

Quantexa is working with a number of large international FIs seeking solutions to better and more expeditiously tackle the elevated financial crime risks peculiar to highly complex businesses and operations. Across a variety of AML use cases, Quantexa's contextual decision intelligence approach is providing insight and intelligence, enhanced recognition of risk, and more effective and efficient detection and investigation. Table D illustrates a distinct AML use case in which a global FI is deploying the Quantexa contextual decision intelligence approach, and is further described below.

Table D: Quantexa Case Study

FI	AML use case	Project objective and outcome
Standard Chartered	Complex investigations	The objective is to optimize existing investigative systems and processes across enterprise and global financial intelligence unit (FIU) investigators. Quantexa is yielding expanded, richer, and more consumable information, enabling more effective and consistent analysis and decisions.

Source: Aite Group and Standard Chartered

CASE STUDY: STANDARD CHARTERED

As a global financial leader, Standard Chartered continually seeks new and innovative ways to combat financial crime. With over 1,500 financial crime investigators across its enterprise operations and a large global FIU that conducts complex financial investigations generated from over 1 billion transactions a year, the corporate AML executive team initiated a quest to transform its investigative tools and modernize how the investigative functions worked.

In supporting its global financial crime investigation function, Standard Chartered previously deployed an expensive yet inefficient investigation platform that required many labor-intensive processes. Investigative teams were devoting significant time to gathering data, understanding it, and trying to differentiate legitimate and potentially suspicious activity. With 45 markets and multiple lines of business, the bank is challenged by disparate data sources and highly complex businesses. The extensive volume of data and the bank's highly complex nature tested the investigative function's ability to not only find the connections among parties and transactions but also fully comprehend the true threats and risks.

Standard Chartered's AML leaders desired a more efficient solution that would leverage newer technologies as well as advanced analytics, and that would better complement its existing financial crime systems. Through a new platform, they hoped to bring together the bank's extensive data on a single platform, connect the dots within the data, and construct a more holistic global view of parties, transactions, and interrelated associations. This would deliver a deeper understanding and recognition of financial crime risks and threats and empower more informed, more accurate, and more consistent investigations and decision-making. Further, the AML leaders sought a firm that would be a true partner and that would collaborate with them on their transformation journey.

APPROACH AND DEPLOYMENT

Given the bank's deep commitment to fighting financial crime, building a business case for a new and more innovative solution and attaining the required budget were straightforward. From the six investigations solutions assessed, Standard Chartered chose the Quantexa solution for the following reasons:

- Its entity resolution and network analytics capabilities to ingest, enrich, and contextualize a vast volume of data from multiple internal (often with years of information) and external sources in real time, and intuitively display a full picture of the data and the network connections
- Its open architecture and capacity to complement Standard Chartered's existing AML systems

The full selection and procurement process took about nine months. Throughout that process, the bank's senior AML leaders did have to invest much time educating their executive management on a previously unknown solution.

The bank's first AML use case deploying Quantexa's technology focused on integrating seven years of historical bank data, consolidating it into a central enterprise view, and bringing enhanced network analysis and intelligence capabilities to its investigative functions across the global enterprise. The following illustrates the key steps taken by Quantexa and the bank over the course of 18 months:

- In order to build a specific and tailored solution, Quantexa worked closely with the bank's AML leaders and subject-matter experts as well as its IT and data science functions.
- A critical step involved getting seven years of the bank's internal data into the Quantexa application. Though this step required considerable effort and time, the Quantexa solution was then able to facilitate data aggregation and the building of connections and context within the data.
- To ensure the application and the Quantexa configuration met its specific needs, the bank worked closely with Quantexa to continually modify the application's initial design. Based on the bank's continual insight and feedback, Quantexa introduced various enhancements and new features into its solution.
- Taking an agile approach throughout the development and testing phases, the bank deployed two separate releases:
  - Deployed within the initial five months, the first release delivered minimum viable product functionality while making 18 months of the bank's historical data available for use by the investigative teams.
  - Subsequently, through several enhancements and customizations, a second release, deployed nine months later, integrated expanded technology while absorbing, enriching, and contextualizing seven years of internal bank data.
- The bank's senior AML leaders regularly discussed the Quantexa deployment with local regulators—including the FCA, the MAS, and the HKMA—to explain the bank's thinking and approach. As strong proponents of innovation in the financial crime space, the regulators, especially those in the Asia-Pacific, were supportive of this endeavor.
- With over 1,500 investigators expected on the solution, much time was devoted to training them and getting them comfortable with the new functionality.

The solution, which allows users to explore seven years of transactional data, is now used across all markets where Standard Chartered operates. Additional enhancements introducing key functionalities such as link analysis and custom dashboards are being developed and are expected to be rolled out in the near future; the new functionality is expected to deliver additional benefits on efficiency and consistency for investigators and analysts.

OUTCOMES: BENEFITS, LESSONS LEARNED, AND FUTURE PROJECTS

Although the integration of the Quantexa functionality is relatively recent and not fully implemented, the bank's AML leaders are seeing the following benefits:

- By automating and simplifying highly labor-intensive and manual processes, the bank's investigators are devoting less time to information and intelligence gathering and more time to analysis and decision-making. Now, many tasks that may previously have taken days can be done within hours.

- In the future, Quantexa's contextual output, visualization techniques, and easy-to-process dashboards are expected to enable the investigation function to become more efficient and effective in sifting through vast amounts of data; finding connections, relationships, and networks, which are often hidden, among parties and payment flows; and understanding the bigger picture.
- Having access to a more holistic view, investigators should become confident in their work producing better insights, more informed and more consistent decision-making, and more actionable intelligence for law enforcement.

Based on their experience with the Quantexa deployment, Standard Chartered's AML leaders shared some key lessons learned and best practices:

- Find a partner that is committed to a true collaboration, work closely with that partner throughout, and continuously learn from each other.
- Clearly define the requirements for the solution, prevent scope creep, and set expectations across the organization; a disconnect between what people think they will get and what they do get could sink a project quickly.
- Engage system users early in the process, educate them, and seek input often; the Quantexa functionality and visualization features were different than the replaced platform, and often something can be perceived as inferior due to a lack of familiarity.
- Tackle the data challenges, address quality issues quickly, and translate the data into a consistent format; legacy systems and historical data challenges can easily delay deployment and hinder the solution's performance.
- Continually learn from testing and user experience and feed that insight into solution building and enhancement, and into process transformation and execution.
- Regularly talk with your local regulators about strategy, approach, and execution; their support is critical, and it is essential to get their buy-in early and often in order to avoid problems later.
- Never stop exploring new technologies and functionalities for elevated and expanded risk identification and mitigation as well as detection of illicit activity; all FIs must be able to quickly react and adapt to emerging threats as they arise.

In the next two phases, Standard Chartered will integrate and leverage data from third-party sources and introduce enhanced analytics for thematic investigations of emerging enterprise trends and risks. Additionally, Standard Chartered intends to further leverage the Quantexa solution as a platform for honing fraud prevention within its trade finance operations and introducing enhanced visualization and data analytic capabilities on its correspondent banking transactions.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION: KEY TAKEAWAYS

The global economy is becoming increasingly multifaceted, and financial criminals are only getting better at staying one step ahead of the good guys. Operational challenges prevent most FIs from effectively disrupting illicit activity within their organizations. Superior AML compliance programs recognize that strong financial crime detection and deterrence is not just about achieving technical compliance with regulatory obligations but about deploying intelligent, sustainable, and efficient risk management while delivering better customer experiences.

Today's new and emerging AML technologies can deliver greater intelligence, more focused risk recognition and coverage, and more effective due diligence, detection, and investigation. Essentially, with the adoption of new technologies, improved outcomes can be achieved with less effort and cost. The imperative exists, and the time to act is now, so consider the following:

- As perhaps the first and most critical step, develop a deep understanding of key organizational financial crime risks, vulnerabilities, and threats as well as primary mitigation and detection controls. Highly complex operations within FIs, such as correspondent banking, capital markets, and trade finance, pose elevated risk of and vulnerability to illicit activity, and FIs must apply risk-based measures to effectively address those risks.
- Intelligently design all systems and processes, and constantly reassess and fine-tune them so they are working as expected and are appropriately considering, identifying, and adapting to new and emerging risks, threats, and typologies.
- Build dynamic risk profiles of customers, their activities, and their connections to other parties, and focus on higher-risk attributes such as cross-border activity, use of newly formed corporate entities or complicated corporate structures, unknown or incomplete beneficial ownership, connections to higher-risk individuals, and ties to jurisdictions and offshore tax havens.
- Leverage all available data, both internal and external, to construct a global customer risk profile; look for and identify questionable patterns, anomalies, and connections to other parties and transactions, and use that knowledge to uncover previously unknown or hidden threats.
- Beginning at onboarding and continuing throughout the full customer life cycle, apply smart and efficient risk-based KYC/CDD and detection. Without strong knowledge of the customer (and often the customer's customer), effective financial crime deterrence and surveillance can become next to impossible.
- Build strong business cases for investing in emerging AML technologies by focusing on how transformation can expand risk coverage and detection, while decreasing the volume of false positive alerts and optimizing investigation times.
- Instill strong governance, discipline, and documentation, as your auditors and regulators will expect it. Continually talk with your local regulators while you are on your transformation journey.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

AI-Enabled Anti-Money Laundering: From Theory to Reality, July 2020.

Regulatory Innovation, Sandboxes, and Tech Sprints: Trends and Global Initiatives, March 2020.

Global AML Vendors: Embracing Innovation, February 2020.

Key Trends Driving AML Compliance Transformation in 2020 and Beyond, November 2019.

Entity Resolution and Linking: Enabling Next-Generation Financial Crime Detection, April 2019.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Charles Subrt
+1.617.338.6037
csubrt@aitegroup.com

Contributing author:

Colin Whitmore
+1.617.874.1186
cwhitmore@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com