International Comparative Legal Guides

Sanctions 2020

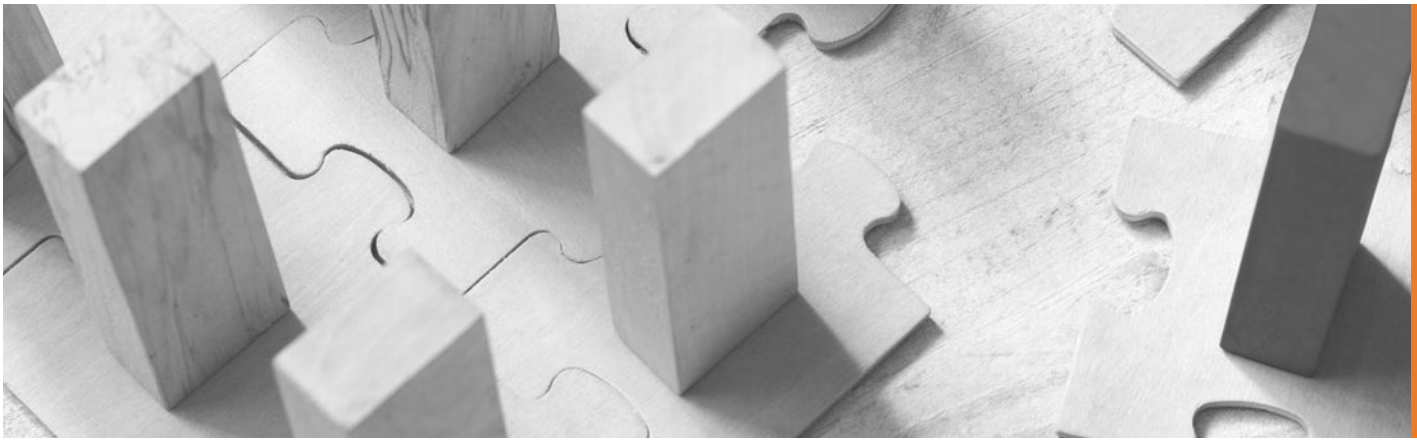
A practical cross-border insight into sanctions law

First Edition

Featuring contributions from:

Allen & Gledhill LLP
BonelliErede
Bonifassi Avocats
BSA Ahmad Bin Hezeem & Associates LLP
De Brauw Blackstone Westbroek N.V.
DELTA legal
Dentons US LLP
Djingov, Gouginski, Kyutchukov & Velichkov
DORDA Rechtsanwälte GmbH
Esenyel & Partners
Eversheds Sutherland
Hill Dickinson LLP
Homburger
JSA
JunHe Law Offices
Kluge
Lee & Ko
Linklaters LLP
Miller & Chevalier
MinterEllison
Navigant Consulting, Inc.
Nishimura & Asahi
Noerr LLP
Paul, Weiss, Rifkind, Wharton & Garrison LLP
Plesner
Proskauer Rose LLP
Stikeman Elliott LLP

ICLG.com



ISBN 978-1-83918-003-3
ISSN 2633-1365

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Publisher
Jon Martin

Senior Editors
Caroline Oakley
Rachel Williams

Sub-Editor
Amy Norton

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Sanctions 2020

First Edition

Contributing Editors:
Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Strategic Partners

Expert Chapters

Country Q&A Chapters

Technology Innovation in AML, Sanctions, and KYC/Due Diligence: Reality *vs.* Aspirations


Patrick J. McArdle


Adam Klauder


Louis DeStefano

Navigant Consulting, Inc.

Introduction

Continuous improvement is paramount to ensuring the effectiveness of any financial crime compliance programme. Financial institutions are always in search of solutions that will improve the effectiveness of their programmes while minimising the operational costs of maintaining them. In the U.S. alone, anti-money laundering (AML) compliance costs financial institutions an estimated $23.5 billion per year.[1] European banks are close behind, with $20 billion spent annually.[2] In addition, fines for sanctions-related violations have swelled in the past decade, with over $13 billion levied against financial institutions by U.S. agencies, regulators, and law enforcement from 2012 to 2015.[3] When considering innovation in financial crime compliance in the midst of this type of compliance and enforcement climate, the current discussion often focuses on three areas of technology: artificial intelligence (AI); robotic process automation (RPA); and blockchain. Buoyed by regulator statements that encourage further exploration of these technologies, financial institutions, software companies, fintechs, and consulting firms are moving at a feverish pace to apply these innovative new technologies in the areas of AML, sanctions, and Know Your Customer (KYC)/Due Diligence.[4]

Despite the attention that these technologies have received, none have developed to the point of replacing traditional forms of compliance. In adopting these technologies, financial institutions must first evaluate their current uses, challenges to implementation/use, risk coverage, and aspirations for the future.

Artificial Intelligence

AI, along with the related machine learning, cognitive computing, and deep learning technology solutions, involves the development of computer programs to perform financial crime compliance tasks that would, in the past, have required human intelligence. AI can be used to identify complex and potentially suspicious patterns in large unstructured datasets in a manner that is cost-effective, efficient, and accurate. AI programs are not static and with further development, many compliance practitioners believe that AI can learn to detect AML risks faster than humans and with significantly lower false positive or false negative rates. Some projections even suggest that applying AI to AML could save the banking industry up to $1 trillion by 2030.[5]

Current State

1. Use of AI in AML Compliance

Currently, AI applications for AML compliance primarily involve post-transaction monitoring. Financial institutions review vast quantities of transaction monitoring alerts daily to identify a small percentage of potentially suspicious transactions. This process can be inefficient and unproductive. Advances in AI present the potential to reduce "false positive" alerts and provide investigators with cases that have a higher rate of potentially suspicious activity. Advocates of AI claim that this can be accomplished in several ways:

a. Intelligent Segmentation
Financial institutions with traditional transaction monitoring systems usually sort their customers by factors such as industry, size, and business type, and employ scenario typologies that have historically worked for customers that are engaged in those business segments.[6] The use of predefined measurements can, however, limit the diversity of categorisation and unintentionally link industries with dissimilar behavioural scenarios, which often produces unproductive alerts in a transaction monitoring programme. By using "intelligent segmentation", financial institutions can create new, more relevant segments based on factors such as transaction activity and customer behaviour. This provides investigative teams with a more precise picture of the risk presented by an entity or a set of transactions.

b. Anomaly Detection
Anomaly detection (or outlier detection) is the identification of unusual items, events, or observations that have the appearance of potentially suspicious activity because they vary substantially from most of the available data.[7] In theory, anomaly detection can trigger investigations outside of preset, traditional detection scenario algorithms as the detection occurs at a specific entity or account level. This enables investigators to identify potentially suspicious activity that may have occurred outside of tuned detection scenario thresholds.

c. Alert Risk Scoring
Some financial institutions are leveraging AI to risk score alerts. The alerts are grouped at the customer level and evaluated based on the overall potential risk of the triggered activity grouping. The alerts are then escalated or "hibernated". Hibernation is a process where the review of a collection of alerts is delayed until it reaches a preset risk score.[8] Hibernation users claim that it differs from alert suppression or auto-closure, as it provides a comprehensive view of compliance risk and allows for better investigation escalations.[9]

2. Use of AI in Sanctions Compliance

As discussed earlier, sanctions violations can be extremely costly for financial institutions, from a financial as well as a reputational standpoint. As a result, institutions are looking to these emerging new technologies to address potential improvements or current deficiencies in their sanctions violation detection programmes. In particular, due to AI's ability to learn from historical behaviours, firms are examining the possibility of using AI to adjudicate first-level sanctions alerts. Humans can train a proposed AI model through supervised learning to process new alerts that utilise previously reviewed sanctions alerts. Subject matter experts can then test the model's performance by evaluating its performance on new alerts. The model can be further optimised based on their findings, until it can ultimately execute the first-level review of sanctions alerts in quicker succession and with fewer errors than a human investigator. The subject matter experts are typically involved in every part of this process, which empowers them to elaborate on and rationalise their tuned AI model to regulators.[10]

3. Use of AI in KYC/Due Diligence

a. Updating of Customer Risk Rating
With its ability to learn the behavioural patterns of specific entities and detect changes in conduct, AI presents financial institutions with the opportunity to automatically update their client risk ratings. Allowing the AI to learn from a specific client's behaviour helps reduce the possibility that an entity's risk will be incorrectly assessed due to an assignment of unsuitable static criteria.

b. Ultimate Beneficial Ownership Information
AI is capable of processing and deciphering large volumes of data, which allows it to quickly and efficiently examine onboarding documents, including the necessary information on beneficial owners that is required to meet regulatory requirements. Because AI makes it possible to manoeuvre complex collections of data into an organised format, KYC personnel are better able to draw accurate conclusions when conducting KYC reviews.[11]

The Reality and Current Potential Challenges of AI Implementation/Use

a. Age of the Technology
Although AI is by no means a new technology, its use in the financial crime world is still in the early stages. Despite the various applications listed above, many are still in the proof-of-concept stage. Even those that have advanced beyond this initial stage still face the issue of being immature processes. Although the field is not yet mature, financial institutions are incorporating AI solutions where possible to address financial crime compliance concerns in AML, sanctions, and KYC, which regulators have encouraged. Major institutions, aware that the AI technology is still developing, have not begun replacing conventional detection scenario-based systems with predominantly AI technology-based systems for transaction monitoring, sanctions screening, or customer due diligence.

b. Regulatory Acceptance
Despite conveying their support for financial institutions and other private sector participants to explore innovative uses of technology to identify and mitigate instances of illicit financial activity, as well as their implicit approval (or lack of objection) to certain institutions using AI in a limited and targeted capacity in their financial crime compliance programmes, regulators have yet to become fully comfortable with AI's use as a primary technology that replaces well-established systems and methodologies. Importantly, U.S. regulators have tried to encourage experimentation by signalling that they will not "automatically assume that the banks' existing processes are deficient" if AI or other new technologies identify suspicious activity that would not or could not have been discovered due to limitations in the institution's current compliance programme.[12]

c. Data
Most banks continue to struggle when it comes to ensuring data quality. As innovative financial crime compliance technology becomes more readily available and adopted within the industry, transaction and customer data has the potential to expand exponentially. For AI to produce results that can be relied upon, banks will need to augment the technology with high-quality data.[13] If institutions are not able to ensure the quality of the data, the results AI produces will be questionable and subject to greater regulatory scrutiny.

d. Staff
The desire to use AI appears to have outpaced the growth in available staffing resources. Demand for personnel with AI expertise is surging within the industry, creating a shortage in available specialists.[14] This demand often leads to bidding wars between firms, which drives up the cost to hire such staff. Indeed, some reports estimate that the total cost of a new hire is more than $200,000.[15]

e. Cost
Despite the long-term savings that are projected for institutions that use AI for financial crime compliance, there is a high cost of initial implementation. In addition to staffing costs, financial institutions that choose to implement AI will incur the costs of implementing the new technology while also maintaining their current compliance technology expenditures during the proof-of-concept phase. Although using innovative technologies has the potential to realise significant savings for institutions, financial crime compliance is not a profit driver for financial institutions and it can be difficult to secure funding for what may be considered an unproven technology.

Aspirations

Despite the challenges, many see AI as the future of AML and sanctions compliance. In addition to the growth and further development of the applications listed above, AI presents the potential to make additional revolutionary changes to the industry. Some in the industry see it as a wholesale replacement of the current detection scenario, the algorithm-based transaction monitoring system, while others believe that AI will eventually enable financial institutions to adjudicate cases and file suspicious activity reports (SARs). Some companies have already made advances in this area.[16]

Robotic Process Automation

Robotic Process Automation (RPA) is a software automation solution that completes repetitive tasks while running unattended. Designed to be flexible and scalable, RPA can be deployed widely within a controlled infrastructure. By performing repeatable tasks in rapid succession, RPA can increase speed, minimise common human errors, and decrease costs.

Current State

1. Use of RPA in AML Compliance

Specific to AML compliance, RPA can be used effectively in performing the negative news and public domain searches that are required for transaction-monitoring reviews of entities and transactional behaviour. By having task-driven "bots" conduct the necessary, but tedious, research, investigators can instead focus on using their training to properly evaluate AML risk in their reviews. This increases productivity and reduces overall staffing costs, as

highly skilled investigators do not have to spend time performing rudimentary research tasks. An analysis by Accenture in 2016 estimates that the use of one bot can replace three to five offshore human resources at one-third of the cost.[17]

2. Use of RPA in Sanctions Compliance

To help mitigate sanctions risk, financial institutions can use RPA to automate some of the more repetitive and manual aspects of the sanctions-screening process. Specifically, RPA can be used to extract and screen names from onboarding, trade finance, or other documents that have been submitted by clients and parties to a transaction.[18] This allows institutions to increase efficiency, reduce the potential for human error in manual data entry, and focus the attention of investigators on addressing potential issues in the sanctions-screening results.

3. Use of RPA in KYC/Due Diligence

a. Onboarding Document Management
   Completing and reviewing onboarding documents and data can be a cumbersome and inefficient process for bank staff. RPA can be used to sort and standardise the documentation of a KYC profile, which provides reviewers with easy access to relevant onboarding information and decreases review times due to the consistency of files throughout an institution.
b. Standardised Research Protocol in Onboarding or Periodic Reviews
   Financial institutions can also use RPA when performing an onboarding or periodic due diligence review. As with transaction monitoring, RPA can conduct negative news and public domain searches for reviewers, which allows reviewers to focus on evaluating a client's risk, as opposed to performing time-consuming research.

The Reality and Current Potential Challenges of RPA Implementation/Use

Similar to AI, RPA is not without its challenges. Some of the most commonly used search engines are resistant to the use of bots, which poses a significant challenge for an institution attempting to use a bot to execute tasks, like public domain searches. Although there are workarounds for this problem, they often have search limitations, such as the number of searches a user can perform at any one time. Currently, less popular search engines are more compatible with bots. In order to achieve greater efficiencies using bots, institutions could be required to change to a lesser-used search engine, which seems impractical at the current time, given the popularity of more widely used but non/less-bot-compatible search engines.

Additionally, because RPA search capabilities are in their infancy, they have had limited evaluation and acceptance by industry and regulators. As such, a design flaw or inaccurate assumption could open an institution up to regulatory and reputational risk if it tries to implement an RPA solution prematurely.

Aspirations

In the future, financial institutions will want RPA to cut costs, improve processing time, and decrease the potential for human error in their AML and sanctions compliance programmes. Further, automating the investigative process and eliminating menial tasks for high-cost investigators will allow financial institutions to place more focus on detecting illicit or sanctioned activity. Financial institutions are also exploring whether RPA can be used to increase the speed of suspicious activity reporting. This has already begun, as companies are using bots that can auto-populate required fields and begin narratives that contain an outline of the investigative information in the SAR e-filing system.[19]

Blockchain

Blockchain is a type of distributed ledger technology that forms a secure cryptographical ledger of transactions.[20] Most blockchains are open public systems that provide shared information access, which makes the technology enticing to institutions that seek to gather more information about parties that are involved in a potentially suspicious transaction or set of transactions.

Current State

1. Use of Blockchain in AML Compliance

Blockchain is most often linked to cryptocurrencies because it is the public ledger on which these transactions are recorded. As a result, understanding how blockchains work is essential for monitoring cryptocurrency for AML risk. One of the most popular aspects of cryptocurrencies (or, most concerning aspects, if you are a compliance professional) is the ability of blockchains to facilitate completely or partially anonymous cryptocurrency transactions. As cryptocurrencies have become more mainstream and regulated, however, exchanges are racing to develop best practices in detecting potentially suspicious activity to become compliant with AML and sanctions regulations. Companies such as CipherTrace offer an ecosystem that attempts to remove some of the anonymity of a cryptocurrency transaction.[21] Additionally, recently created blockchain-based registries, such as the J.P. Morgan Interbank Information Network (IIN) and KYC-Chain offer participating AML personnel the opportunity to quickly and securely access the KYC information of parties.

2. Use of Blockchain in Sanctions Compliance

Firms are currently developing the new technology to store and update sanctions watchlists on blockchains. There is little public information available on this potential development at this time.

3. Use of Blockchain in KYC/Due Diligence

Financial institutions are currently moving toward arrangements whereby they will share customer KYC information from correspondent banks and large corporations through blockchain technology KYC registries. Although these registries will not contain every customer's information, they will speed up the onboarding and review process of correspondent banks and corporations that participate in the correspondent banking system.

a. J.P. Morgan Interbank Information Network
   J.P. Morgan's IIN is an online KYC registry that is open to other financial institutions. Using blockchain, IIN reduces the time that correspondent banks currently spend responding to compliance and other data enquiries that delay payments. Launched as a pilot in 2017, IIN expanded to 273 participating banks as of August 7, 2019.[22] According to J.P. Morgan, the initial use case for IIN was around sanctions screening.[23]
b. KYC-Chain
   KYC-Chain is a platform that utilises a distributed, central ledger between participating financial institutions and corporations for the verification and exchange of reliable KYC information of entities and individuals. KYC-Chain utilises blockchain technology that pools and authenticates KYC information to form a consensus between KYC-Chain participants on the identity of customers, which provides a more accurate and compliant KYC onboarding process for all participants. Centralising KYC information in a single ledger also allows KYC-Chain to provide adverse news, sanctions, and Politically Exposed Persons screening of the dataset in real time, reducing participants' in-house customer-screening costs and increasing their comfort with their compliance of AML and sanctions requirements as dictated by their local regulators.[24]

Current Challenges to Implementation/Use of Blockchain

1. Lack of Information to Share in Cryptocurrencies

Although the ability to share information securely is one of the primary benefits of using blockchain technology, its most widely known application (cryptocurrencies) is often used precisely because of its lack of transparency. As noted, many cryptocurrencies are either completely or partially anonymous, which creates problems for financial crime compliance departments that need to gather and review as much information as possible about a potential transaction in order to properly assess AML risk. While the transaction information on the actual blockchain is secure and verifiable, the presence of accurate and verifiable KYC information attached to individual users is questionable. Despite recent regulatory guidance for cryptocurrency exchanges, KYC information has room for improvement.

2. Participation

While blockchain offers the opportunity to quickly and securely access KYC information, the information available is limited. A transacting entity must be present in the same registry that an AML investigator also has access to, or that investigator will not have the necessary information to conduct a proper investigation of the entity. As financial institution registry participation increases, more data will be available, providing for more informed investigations and faster production without the need for a request for information.

Aspirations

Even though it is in its early stages of use, blockchain is seen by many as a technology that will become more prevalent in the overall financial crime detection and compliance space. While the immediate focus in this area appears to be perfecting the approach to crypto-transaction monitoring, many see trade finance compliance as an area of potential growth for blockchain technology. As more financial institutions and corporations join online registries, transaction parties will have greater access to information that is needed to appropriately screen and assess trade finance deals.

Conclusion

Financial institutions are constantly exploring innovative solutions to detect financial crime while also cutting the expenses associated with their AML, sanctions, and KYC/Due Diligence compliance programmes. This desire for innovation inevitably leads to discussions about new technologies with promising applicability, such as AI, RPA, and blockchain. These technologies have demonstrated the potential to both improve the quality of financial crime investigations while at the same time reducing their costs. Despite the potential that these technologies show, reality does not always match aspiration. These technologies are still developing and must overcome major challenges to reach their full potential. Every financial institution must take its own sophisticated risk-based approach when weighing whether to adopt one or all of these technologies. The decisions institutions make may determine whether these technologies revolutionise the industry or are just a minor disruption.

Endnotes

1. Brian Monroe, "Financial Crime Wave – U.S. Compliance Costs Surpass $25 Billion, EU, U.K. AML Fines and More", Association of Certified Financial Crime Specialists, October 13, 2018, https://www.acfcs.org/financial-crime-wave-u-s-compliance-costs-surpass-25-billion-eu-u-k-aml-fines-and-more/.
2. Pawel Kuskowski, "The Step that Would Save European Banks Twenty Billion Dollars", *Forbes*, September 10, 2018, https://www.forbes.com/sites/pawelkuskowski/2018/09/10/the-step-that-would-save-european-banks-twenty-billion-dollars/#64ba3383398b.
3. Yalman Onaran, "Stung by Big Fines, Big Banks Beef Up Money-Laundering Controls", *Bloomberg*, April 4, 2019, https://www.bloomberg.com/news/articles/2019-04-04/global-banks-beef-up-money-laundering-controls-as-fines-sting.
4. Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, Board of Governors of the Federal Reserve System, December 3, 2018, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf; Christopher Woolard, "The Future of Regulation: AI for Consumer Good", Financial Conduct Authority, July 16, 2019, https://www.fca.org.uk/news/speeches/future-regulation-ai-consumer-good; KC Cheung, "Monetary Authority of Singapore (MAS) Reinforces AI Ecosystem", Algorithm-X Lab, January 16, 2019, https://algorithmxlab.com/blog/monetary-authority-of-singapore-mas-reinforces-ai-ecosystem-2/.
5. Financier Worldwide, "Strengthening AML protection through AI", July 2018, https://www.financierworldwide.com/strengthening-aml-protection-through-ai#.XWNWtOhKiM8.
6. Ellen Zimiles and Tim Mueller, "How AI Is Transforming the Fight Against Money Laundering", World Economic Forum, January 17, 2018, https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/.
7. Vegard Flovik, "How to use machine learning for anomaly detection and condition monitoring", Towards Data Science, December 31, 2018, https://towardsdatascience.com/how-to-use-machine-learning-for-anomaly-detection-and-condition-monitoring-6742f82900d7.
8. Wallace Chow *et al.*, "What is the next-generation AML?", SAS, https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/next-generation-aml-110644.pdf.
9. Beth Herron and Robert Goldfinger, "Artificial Intelligence and Machine Learning: What do we know?", ACAMS Today, September 18, 2018, https://www.acamstoday.org/artificial-intelligence-and-machine-learning-what-do-we-know/.
10. Zimiles and Mueller, World Economic Forum.
11. Niall Twomey, "5 Ways AI is Impacting AML and KYC Compliance", Corporate Compliance Insights, December 19, 2018, https://www.corporatecomplianceinsights.com/5-ways-ai-is-impacting-aml-and-kyc-compliance/.
12. Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, Board of Governors of the Federal Reserve System, December 3, 2018, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.
13. JiaYin Low, "Is AI really, really stupid?", On the Limitations of AI, Information-Age, February 21, 2019, https://www.information-age.com/limitations-of-ai-123479433/.
14. Ayehu, "Overcoming the AI Talent Shortage", January 25, 2019, https://ayehu.com/overcoming-ai-talent-shortage/.
15. Insights Team, "Overcoming AI's Challenge in Hiring: Avoid Human Bias", *Forbes*, November 29, 2018, https://www.forbes.com/sites/insights-intelai/2018/11/29/overcoming-ais-challenge-in-hiring-avoid-human-bias/#1d60f5ec73bf.
16. NICE Actimize, "Transforming Transaction Monitoring & Reporting of Suspicious Activity", August 29, 2019, https://www.niceactimize.com/anti-money-laundering/suspicious-activity-monitoring.
17. Samantha Regan *et al.*, "Evolving AML Journey", Accenture Consulting, September 2016, https://www.accenture.com/_acnmedia/pdf-61/accenture-operational-transformation-anti-money-laundering-robotic-process-automation.pdf.
18. Bruce Klein, "Could RPA Help or Hinder your Manual Process?", *Forbes*, January 7, 2019, https://www.forbes.com/

sites/forbesnycouncil/2019/01/07/could-rpa-help-or-hinder-your-manual-process/#575b2c0f1c36.
19. Insights Team, *Forbes*.
20. Alma Angotti and Anne Marie Minogue, "Risks and Rewards: Blockchain, Cryptocurrency and Vulnerability to Money Laundering, Terrorist Financing, and Tax Evasion", Thomson Reuters Westlaw, November 26, 2018, https://www.navigant.com/-/media/www/site/insights/gic/2018/thomson-reuters_wlj_bll2414_angottiminogue.pdf.
21. CipherTrace, Compliance Monitoring – CipherTrace, August 29, 2019, https://ciphertrace.com/compliance-monitoring/.
22. J.P. Morgan, "Largest Number of Banks to Join Live Application of Blockchain Technology", August 7, 2019, https://www.jpmorgan.com/global/treasury-services/IIN.
23. Laura Noonan, "JPMorgan to Widen Use of Blockchain System", *Financial Times*, April 21, 2019, https://www.ft.com/content/87ae3010-61ec-11e9-b285-3acd5d43599e.
24. KYC-Chain, "KYC-Chain – KYC & AML Compliance Banking Solution", August 29, 2019, https://kyc-chain.com/.

Patrick J. McArdle is a Managing Director in Navigant's Global Investigations and Compliance practice. He has 20 years of experience in regulatory compliance, consulting and law enforcement. Mr. McArdle specialises in Bank Secrecy Act ("BSA") and anti-money laundering ("AML") compliance, fraud prevention and forensic accounting investigations.

Navigant Consulting, Inc.
685 Third Avenue
14th Floor
New York, NY 10017
USA

Tel: +1 646 227 4841
Email: patrick.mcardle@navigant.com
URL: www.navigant.com

Adam Klauder is a Senior Director in Navigant's Global Investigations and Compliance practice. He is a seasoned compliance executive, attorney, and senior leader with an extensive background in developing overall compliance strategy, directing and coordinating sensitive and high-profile global investigations, and providing strategic guidance on the build-out of corporate compliance functions. Mr. Klauder advises clients in the defence, healthcare, financial services, transportation and logistics, energy and infrastructure, and telecommunications sectors, and is a subject matter expert in compliance matters involving economic sanctions, export controls, anti-corruption, data privacy and other cross-border regulatory regimes. Prior to joining Navigant, Mr. Klauder was a senior global compliance executive at HSBC, serving as Global Head of Sanctions Investigations and Global Investigations Advisor.

Navigant Consulting, Inc.
1200 19th Street, NW
Suite 700
Washington, D.C. 20036
USA

Tel: +1 202 481 8371
Email: adam.klauder@navigant.com
URL: www.navigant.com

Louis DeStefano is an Associate Director in the New York office of Navigant's Global Investigations and Compliance practice. Louis has extensive Anti-Money Laundering ("AML") experience involving large-scale transaction monitoring investigations, and has conducted reviews of AML and Bank Secrecy Act ("BSA") programmes at financial institutions and money service businesses as well as participated in the risk assessment of these programmes. Louis specialises in the evaluation of the investigations process conducted via post transaction monitoring. He conducted reviews of international correspondent banks, domestic retail banks, and large money service businesses. He has extensive experience in the conduct of alert/case adjudication and SAR drafting. Louis is also experienced in training personnel in the related AML subject matter. He is also responsible for the examination of related policies and procedures, ensuring their compliance with applicable laws, regulations, and industry best practices.

Navigant Consulting, Inc.
685 Third Avenue
14th Floor
New York, NY 10017
USA

Tel: +1 646 227 4801
Email: louis.destefano@navigant.com
URL: www.navigant.com

Navigant Consulting, Inc. (NYSE: NCI) is a specialised, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results.

www.navigant.com

NAVIGANT

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group