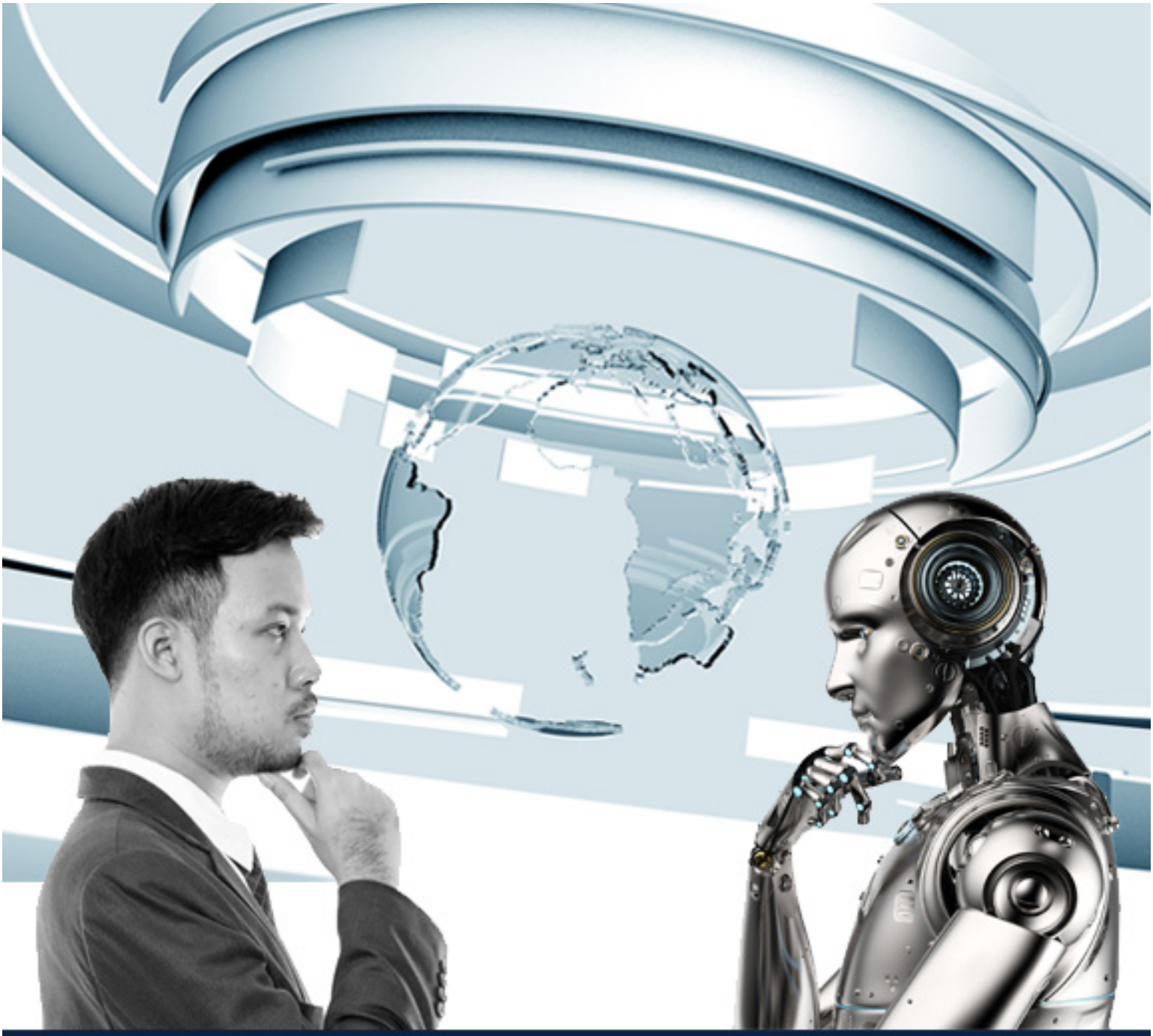


Artificial Intelligence & Human Analysis: A Collaborative Relationship

Prepared by: KRELLER GROUP **November 19, 2019**

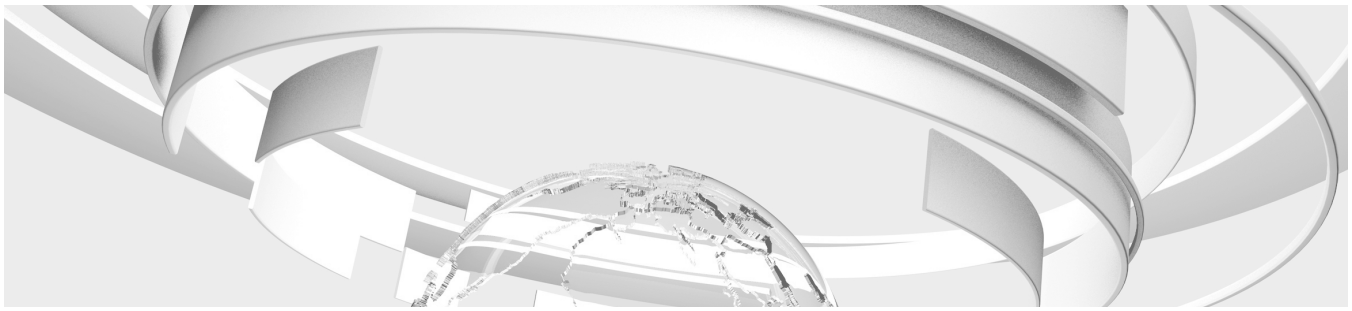


TABLE OF CONTENTS

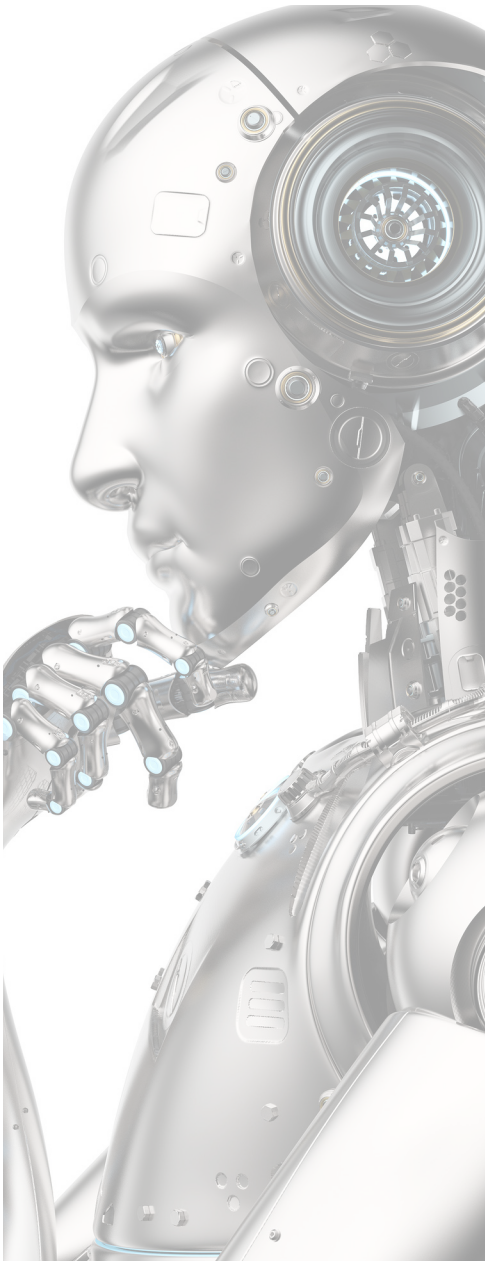
Kreller Group
817 Main Street | Suite 700
Cincinnati, OH 45202
1.800.444.6361
www.kreller.com

SECTION 1
Executive Summary

Like most technological developments, both the promise and the threat of AI routinely verge on the hyperbolic. This white paper examines the possible applications of existing AI and machine learning technologies for due diligence investigations in the realm of corporate anti-money laundering and anti-corruption compliance, many of which can be derived from AI's current usage within the financial technology (fintech) sector. AI and machine learning's greatest contribution to anti-money laundering (AML) and know your customer (KYC) efforts in the financial industry is its ability to process vast quantities of data quickly and extract specific anomalous transactions indicative of potential fraud.

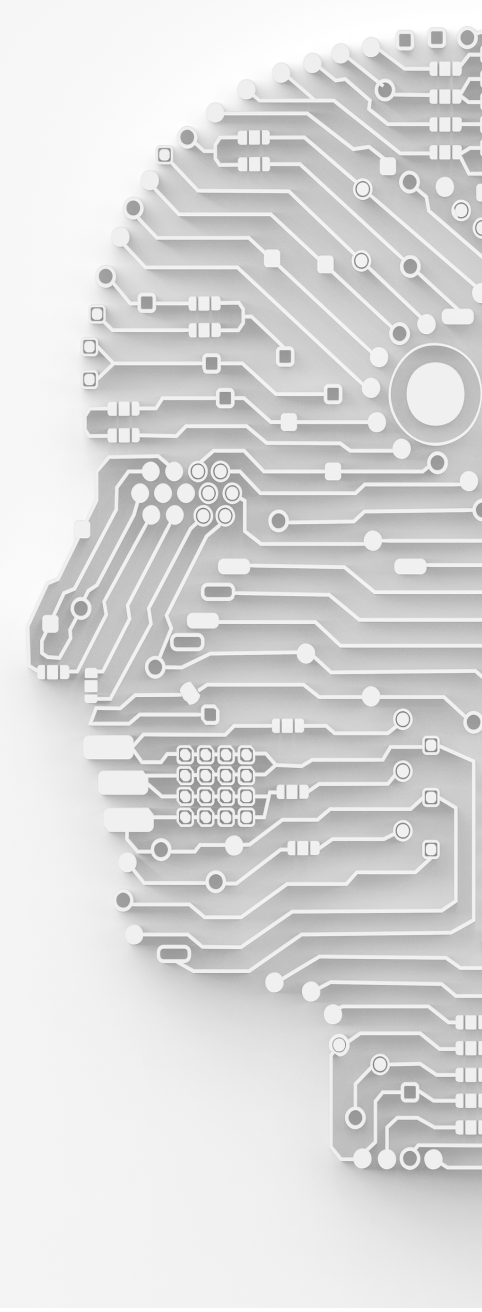
The paper then explores some of the major limitations of machine learning, including the problem of false positives, the amplification of human bias through poorly constructed and under-tested algorithms, and issues related to the ethical use of AI. Crucially, we explore the ways in which machine learning, even in its more sophisticated permutations (unsupervised machine learning and deep learning/neural networks), still struggles to make actionable decisions in the face of novel situations. AI's relative weakness when operating in circumstances it has not trained for creates a significant downside when applying machine learning to corporate due diligence.

Human intelligence (known in investigative circles as HUMINT) continues to be an irreplaceable element of a strong corporate due diligence program. Investigators and analysts have access to tools which can be used to overcome many of AI's issues with false positives. More importantly, human intelligence is far more adaptable to novel situations, making it better suited for handling unique geo-political contexts and analyzing trans-national actors who use innovative methods to circumvent international anti-corruption laws. The paper closes by envisioning a hybrid model of corporate due diligence which leverages both the strengths of machine learning and the best features of human intelligence, to provide an efficient and cost-effective range of solutions for corporate compliance.



SECTION 2
The Promise of AI for Compliance: Lessons from the Financial Sector

Nearly a year ago the U.S. Federal Reserve, FDIC, Financial Crimes Enforcement Agency (FinCEN), National Credit Union Administration, and the Office of the Comptroller of the Currency released a joint statement to encourage financial institutions to explore innovative approaches in order to meet compliance requirements[1] with regard to anti-money laundering (AML) and the Bank Secrecy Act (BSA).

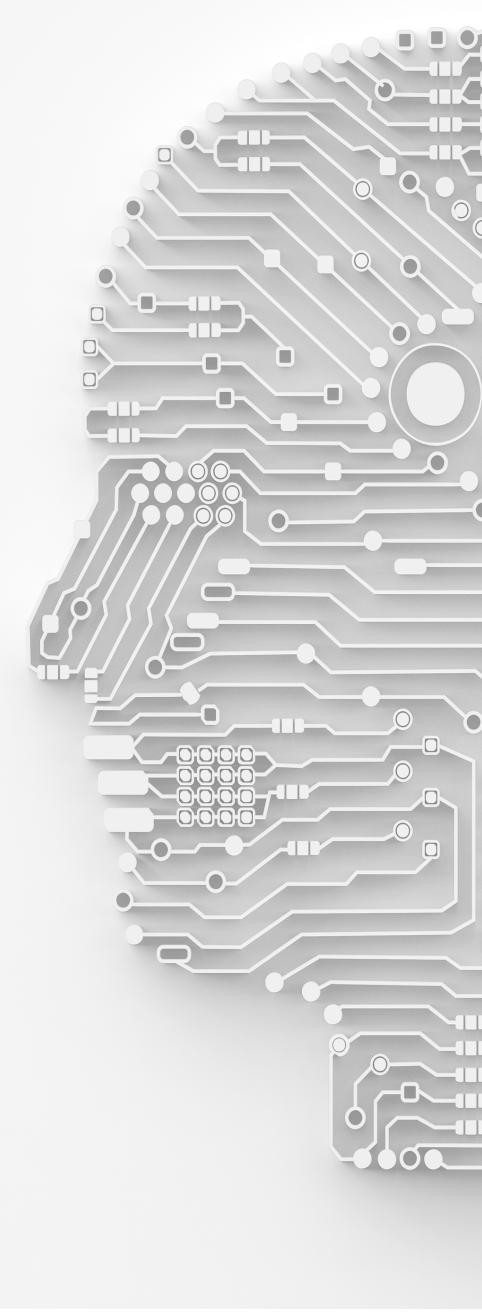


In order to foster a sense of experimentation, the agencies sought to provide a degree of latitude to banks in implementing various pilot programs, stating they would not criticize unsuccessful pilot programs or take supervisory action against banks merely because pilot programs exposed flaws in their current BSA/AML compliance protocols. The agencies also stated they would not saddle innovating banks with additional regulatory requirements. The collection of agencies specifically reference artificial intelligence as a primary example of the sort of innovation they are seeking to encourage in the financial industry's KYC and compliance programs. In remarks given at the 2019 Securities Industry and Financial Markets Association (SIFMA) Anti-Money Laundering & Financial Crimes Conference, FinCEN Director Kenneth Blanco again stressed the importance of developing AI and machine learning (ML) based approaches to anti-money laundering and counter-financing of terrorism.[2]

As Bonnie Buchanan, PhD, FRSA noted in her report[3] Artificial intelligence in Finance, produced in April 2019 with support from The Alan Turing Institute, recent years have seen a wave of innovation in applying AI capabilities within the financial industry. Buchanan, who follows Jerry Kaplan's definition of intelligence (artificial or otherwise) as "the ability to make appropriate generalizations in a timely fashion based on limited data,[4]" contends that artificial intelligence and its subfields, machine learning (ML) and deep learning (DL), are uniquely suited to the information-processing requirements of the financial services industry.

According to Buchanan, AI is currently used in a wide range of applications including algorithmic trading, portfolio optimization, robo-advising, market analysis, and fraud detection. In particular, the field of machine learning (ML), which is defined as an "approach to AI able to take the data and algorithms and apply it to new scenarios and patterns without being programmed directly," and its subfield, deep learning (DL), have proven immensely beneficial in financial fraud prevention and detection. You have probably encountered one of ML's most successful financial applications, perhaps when your credit card was frozen in a patisserie in the 5th arrondissement, after you neglected to notify the bank of your upcoming trip to Paris. Banks and credit card issuers are able to train AI through machine learning to classify purchases as potentially fraudulent based on historical transaction data; thanks to ML, your croissant is labeled as an anomaly and the transaction can be blocked in real time.

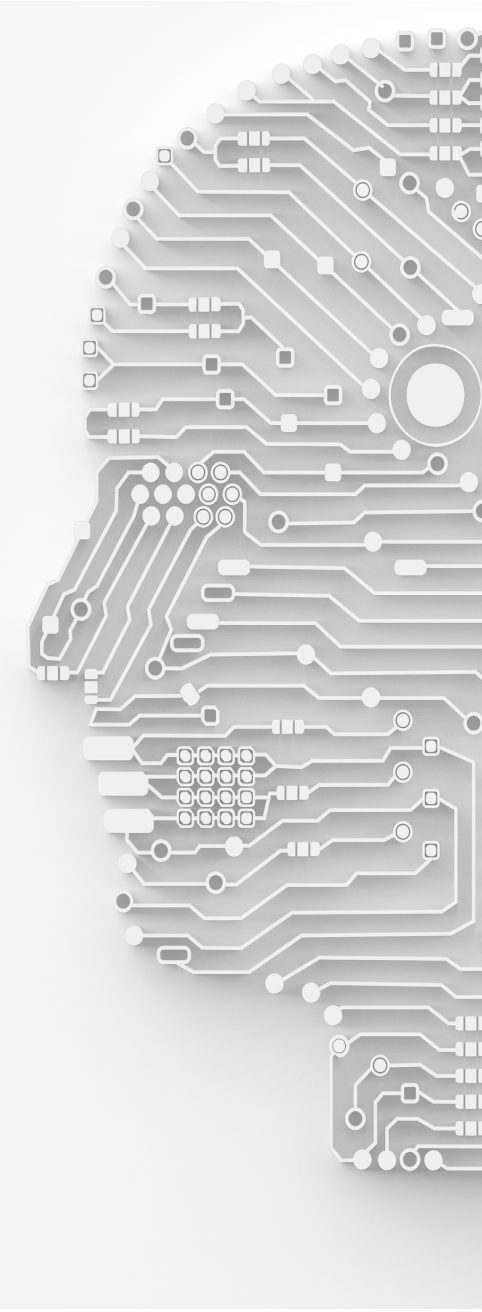
Over the course of numerous transactions, a machine learning application is able to recalibrate its analysis of your transaction history, with enough purchases your penchant for French pastries might cease to be flagged as suspicious, as the application has effectively learned your consumer habits. The rate at which an application is able to learn a customer's spending behavior and adapt accordingly has a significant impact on credit card issuers. While false positives are a necessary consequence of a fraud-prediction system, accurate prediction tools minimize the number of legitimate transactions which are declined, thereby protecting an issuer's reputation with its customer base.



AI Terms – Cheat Sheet

Artificial neural network (ANN)	An algorithm that attempts to mimic the human brain, with layers of connected "neurons" sending information to each other.
Black box algorithms	When an algorithm's decision-making process or output can't be easily explained by the computer or the researcher behind it.
Computer vision	The field of A.I. concerned with teaching machines how to interpret the visual world
Deep learning	ANNs that have multiple layers of connected neurons. This makes the process deep compared to earlier, more shallow networks.
Generative adversarial networks	Also called GANs, these are two neural networks that are trained on the same data set of photos, videos or sounds. Then, one creates similar content while the other tries to determine whether the new example is part of the original data set, forcing the first to improve its efforts. This approach can create realistic media, including artworks.
Machine learning	Systems that learn from data sets to perform and improve upon a specific task. It's the current area of A.I. experiencing the biggest research boom.
Natural language processing (NLP)	The discipline within A.I. that deals with written and spoken language.
Supervised learning	A technique that teaches a machine-learning algorithm to solve a specific task using data that has been carefully labeled by a human. Everyday examples include most weather prediction and spam detection.
Unsupervised learning	An approach that gives A.I. unlabeled data and has to make sense of it without any instruction.

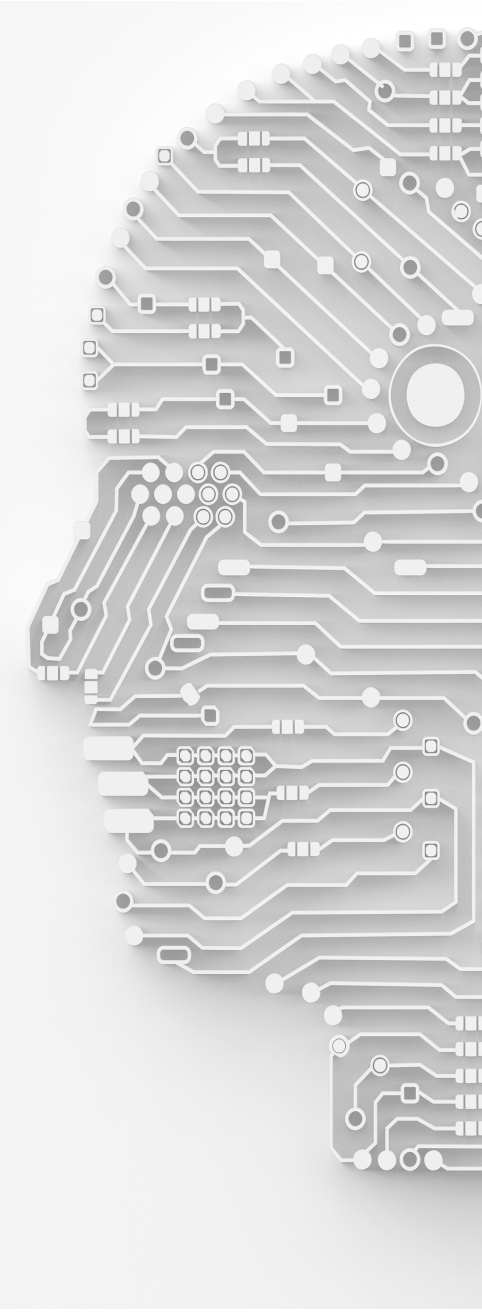
(Jackie Snow, The New York Times, October 18, 2018)[5]



Another reason machine learning applications have flourished in the financial compliance sector is their ability to process, sort, and analyze massive amounts of data in search of unusual transaction patterns suggestive of various financial crimes including money laundering, embezzlement, and payments fraud, a form of fraud in which a bad actor masquerades as a legitimate supplier in order to redirect payments which would otherwise be made to the supplier. As a September 5, 2019 Forbes article indicated, payment fraud has become increasingly complicated and thus less detectible by rule-based predictive tools alone.

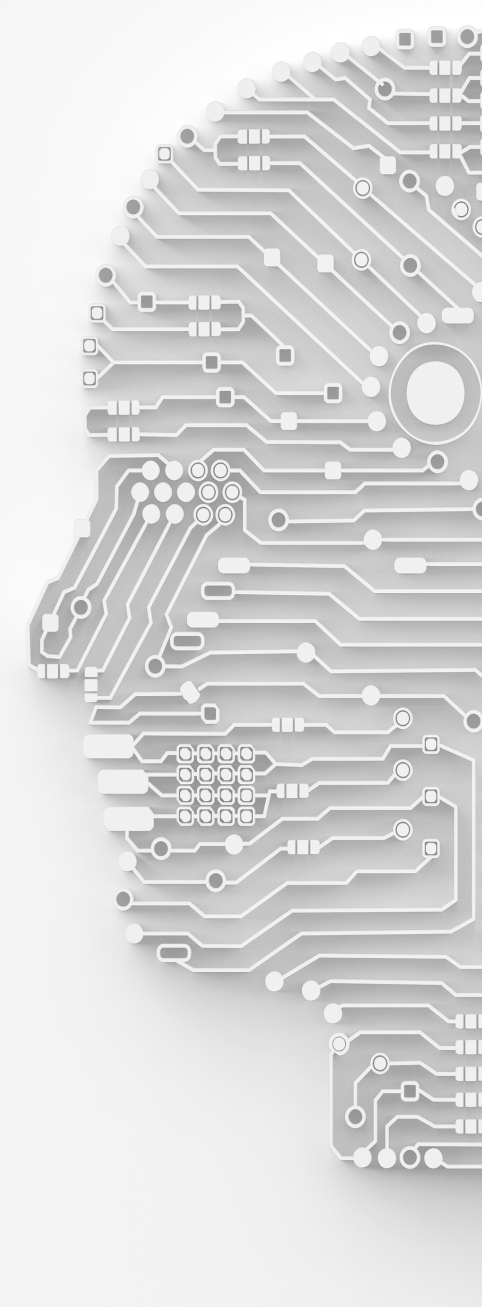
AI applications, particularly those that blend elements of supervised and unsupervised machine learning, are able to adapt to changing fraud patterns, making AI significantly more effective against redirection schemes than standard predictive models.[6] The ability to sift through vast quantities of data in order to detect patterns has also proven beneficial to forensic accountants. CPA and Certified Fraud Examiner Gary Krausz of Gursey Schneider LLP and John Colthart of MindBridge AI discussed their own experience collaborating in a December 14, 2018 blog post for ACFE Insights.

Reportedly, Gursey Schneider LLP enlisted MindBridge to implement an AI solution on behalf of a client who discovered fraud which was perpetrated by their in-house CPA. The AI program allowed Krausz' audit team to evaluate over three years of activity (totaling about 6.2 million individual transactions), a volume which far "exceeded the capabilities of Microsoft Excel or traditional CAAT tools." While an audit team would normally approach such a data set by "relying on hunches and instinct to pick an account and start digging," the AI tool was able to analyze the myriad transactions and quickly zero in on suspicious items, allowing the forensic accounting team to work more effectively and efficiently.[7]



Just as AI's facility with vast quantities of data and speed in preforming routinized tasks have proven useful in detecting and preventing credit card fraud and payments fraud, it has also been employed to identify patterns with regard to money laundering activities and utilized as part of banks' know-your-customer (KYC) protocols. In fact, as Dr. Bonnie Buchanan notes, AML was one of AI's earliest realms of application, having been adopted by FinCEN in 1993. In its first two years of operation, the FinCEN Artificial Intelligence System (FAIS) was able to flag "400 potential money laundering incidents, worth approximately $1 billion."[8] According to Niall Twomey, CTO of Fenergo, as the AI subfield of natural language processing (NLP) advances, an increasing number of applications are in development which are able to scan client onboarding documents in a number of languages and assess the documents for signs of AML risk within the onboarding process.[9]

As reported by the Wall Street Journal[10] and Retail Banker International,[11] Fair Isaac Corp. (FICO) has recently released two AI solutions designed to facilitate KYC and onboarding protocols without requiring in-person identity verification. The first of these uses facial analysis to match an applicant's selfie with an ID photo. The second is able to verify an individual's "digital identity" through assessing behavioral biometric data such as keystroke speed and mobile device use.



SECTION 3
Lost in Translation: Shortcomings of AI for Compliance

As seen in the previous section, AI is especially well-suited to compliance within the financial industry as it is able to extract noteworthy information from millions of individual transactions, while also being able to adjust to changing patterns within the data. As noted in a March 14, 2018 Reuters article, these AML monitoring systems used within the banking industry typically analyze transaction data using detection rules which are focused on specific suspicious behaviors, such as rapid shuffling of money across accounts, abnormally large cash deposits, and oddly-structured transactions.[12] While AI has enhanced these detection systems, there are still several major drawbacks from applying an action-based model to complex money laundering systems.

As the abovementioned Reuters article discusses, this logic behind the current action-based detection model "has proven flawed and inefficient at identifying financial crime, resulting in record-breaking regulatory fines for financial institutions that fail to detect terrorists, drug cartels, and sanctioned state actors exploiting the U.S. financial system." One reason for this, is the high rate of false positives produced by such methods; according to Reuters only 2% of the alerts trigged by financial transaction monitoring systems actually results in a suspicious activity report (SAR). The false alerts ultimately "cost the financial industry billions of dollars in wasted investigation time." Meanwhile, sophisticated bad actors, who have discovered ways to conduct transactions such that the detection systems are not triggered, leave banks vulnerable to regulatory action for failing to detect and prevent illicit financial activity.[13]

While action-based detection models divert investigative resources into scrutinizing false positives, they also fail to detect complex and advanced laundering schemes developed by transnational criminal organizations (TCOs). Different types of criminal organizations will naturally favor different methods of money laundering depending on the type of TCO, the source of the illicit money, and the access to various means by which to convert the dirty money into legitimate accounts.

While action-centric AML detection systems examine transactions to look for tell-tale signs of laundering, law enforcement and regulatory agencies approach AML by focusing on operational and organizational factors within each TCO, resulting in an actor-centric investigative approach. An actor-centric focus often yields a different set of red flags than one centered specifically on individual anomalous transactions. As Reuters points out, even the most high end AI applications, which usually rely on unsupervised machine learning (UML), are typically "developed by technical specialists" without the necessary background in financial law enforcement or awareness of the "transnational security issues, public policy, and the regulatory climate" needed to remain abreast of emerging money laundering trends and risks.[14]

Reuters cites Hezbollah as an example of an extremely sophisticated and far-reaching crime syndicate with a very effective trade-based money laundering operation. Hezbollah's money laundering system is made possible by "an elaborate global distributions network" which allows the organization to move counterfeit goods and obscure the proceeds of human and narcotics trafficking. Such a transnational distribution network allows Hezbollah and other TCOs to move funds in ways which "superficially appear entirely legitimate" and thus are not regularly flagged by action-based AML detection systems.[15]

While incorporating actor-based investigations and analysis into KYC protocols can mitigate regulatory risks for banks, actor-based analysis is also a vital part of standard corporate due-diligence procedures. This is especially true of businesses with international operations and those with ties to highly regulated and/or high risk industries. One such cautionary tale occurred in 2017 when a high-end boutique specializing in home décor, located in the posh Miami suburb of Coral Gables, was found to be linked to an international gold smuggling scheme benefiting Peruvian narcotics dealers.

The boutique shares an address with MVP Imports LLC and both entities are owned by South Florida businessman Jeffrey Himmel, who previously made his fortune reviving aging brands such as Breck shampoo and Ovaltine. MVP Imports was named —but not charged— in a criminal indictment against NTR Metals, a Doral-based gold trader alleged to be "at the center of the largest money-laundering case involving precious metals in U.S. history.[16]"

On March 16, 2018 NTR's parent company, Elemetal LLC, pleaded guilty to violating the Banking Secrecy Act (BSA) by failing to maintain adequate AML protocols, as required for precious metals dealers. According to the U.S. Attorney's Office for the Southern District of Florida, NFT's AML negligence was so thoroughgoing that they unquestioningly accepted gold from suppliers in Latin America, despite publicly available information indicating that these suppliers were dealing in criminally-derived gold[17].

According to extensive[18] in-depth reporting by the Miami Herald, Elemetal pleaded guilty following the convictions of three of its traders for their involvement in the money laundering and smuggling scheme, wherein $3.6 billion in gold was purchased from criminal organizations in Latin America. Reportedly, gold was purchased from unauthorized mines operating deep within the Peruvian rainforest and run by local drug cartels.

These mines and others like them are known to cause profound environmental damage both from deforestation and from heavy metals including mercury which are used in extraction. The mercury pollutes the waterways, contaminates local fish stock and poisons exposed miners, many of whom are indigenous peoples.[19] Much of the information regarding the illicit source of the gold was publicly available prior to NTR's purchases. Reportedly, in one instance Elemetal's compliance officer unsuccessfully warned NTR's gold dealers not to conduct business with an individual known as "Peter Ferrari" due to his suspected activity as a narcotics trafficker in Peru.[20]

As the money laundering scheme progressed, NTR began to feel pressure from the Peruvian authorities, and by late 2013, the company began smuggling gold out of Peru and into other nearby countries, so that they could export the gold to the United States without drawing as much suspicion. Reportedly, NTR enlisted Himmel and MVP Imports as "a fig leaf" so that NTR could obscure its role as the gold's ultimate purchaser on U.S. Customs records. Himmel contends that he was unaware of MVP Imports' role in the scheme, stating through his attorneys: "I didn't see the sharks swimming under the surface but, apparently, they were there… A lifetime in business without a blemish, obviously I feel betrayed. I'm kicking myself for allowing myself to be deceived.[21]"

An actor-based investigation is precisely the right tool to provide businesses with insight as to the potential risks lurking under the surface of a partnership or deal. A knowledge of the intersection between the narcotics and gold trades in Latin America, coupled with due diligence regarding NTR's reported sources and activities would have likely proved just as effective as a transaction-based AML system —not to mention far less expensive in a one-off scenario— for uncovering the inherent risk in a partnership with NTR.

Rule-based fraud detection models, such as those used within the financial industry, even those which utilize machine-learning, also exhibit another major weakness, namely the relative inability to handle wholly novel events. In some instances this blind spot within AI can have tragic effects, as seen with instances of traffic fatalities caused by self-driving cars. A May 24, 2018 preliminary report issued by the U.S. National Transportation Safety Board (NTSB) following a fatal crash involving a driverless Uber vehicle in Tempe, Arizona, described a situation in which a pedestrian in dark clothing was walking a bicycle across a poorly lit street in an area which was not designated as a crosswalk prior to being fatally hit by the self-driving vehicle, which was approaching at an angle perpendicular to the pedestrian's path.

The car's system report indicated that the vehicle registered the pedestrian approximately six seconds prior to the collision, while traveling at 43 mph, but was unable to definitively classify the pedestrian (who was registered first as an unknown object, then as a vehicle, and then as a bicycle) or to predict the pedestrian's travel path. Due to its delay in identifying the pedestrian, the self-driving car did not deploy its automatic breaking mechanism until approximately 1.3 seconds prior to impact. The vehicle's operator, who stated that she had been monitoring the car's self-driving interface, took control of the steering wheel less than a second before the collision.[22]

According to a November 5, 2019 article from Wired, new documents released by the NTSB regarding the Tempe collision indicated that the self-driving car involved in the crash had not been programmed to recognize humans crossing outside of crosswalks, making it unable to classify the unknown hazard in the road, leading to a critical delay in the vehicle's decision to employ the brake.

Compounding the fatal mistake, the Uber vehicle's inability to classify the entity in the road prompted an "action suppression" mechanism, delaying the car's automatic braking mechanism for an additional second.[23]

The NTSB report is helpful for illustrating the ways in which AI "thinks" about things differently than a person might. Uber's self-driving vehicle was not trained to recognize jaywalkers as human pedestrians and was thus unable to determine the proper course of action when confronted with such a commonplace situation. As seen in this example, AI's range of responses when challenged by a novel experience or data set can be limited, counterproductive, and in this instance even tragic.

Such counterintuitive AI behavior is also responsible for a phenomenon which has come to be known as the "flash crash," in which stock prices rapidly plummet and then quickly rebound. As Matt Levine, a former investment banker for Goldman Sachs, explains in a January 3, 2019 op-ed for Bloomberg, flash crashes are typically caused by AI operating according to preprogrammed algorithmic rules, or orders, known as a schedule of demand. However, such orders can differ significantly from typical "real-world" human behavior. Levine gives the following example:

> *Lots of people who own, say, Tesla Inc. stock would sell it if the price doubled; lots of people who don't own it would buy it if the price dropped by 50 percent; very few of those people have bothered to alert their brokers to those desires. There's just no need, you know? If the price drops by 50 percent, then you can put in your buy order; if it doubles, then you can sell it; you don't have to think about it now… But if a lot of people want to sell all at once — or if one person wants to sell a lot all at once — then there will be a small, technical problem. The schedule of demand in the computer system will be sketchy and limited, reflecting not the actual demand for the thing in the world but just the orders that people bothered to put into the computer system based on the current price.*

The scattershot nature of the pre-programed schedule of demand as compared to actual human trading behavior, coupled with other more complicated algorithmic factors, results in the sudden sell-offs seen in a flash crash scenario. As Levine points out, instead of this being a case of black-box algorithms behaving in ways which are mysterious to people, it is actually a case of "humans being inscrutable to the algorithms." Machine learning may find ways to capture elements of human behavior efficiently, i.e. buying and selling certain stocks at certain prices, or navigating a vehicle around the streets of Tempe. But, as Levine puts it, "that efficiency comes at the cost of not capturing their views completely."

The algorithm does not fully capture real market behavior; the car doesn't automatically brake for the unidentified hazard in the road.[24] In short, AI has difficulty making human-analogous decisions in surprising or unscripted situations on which it has not trained. Even AI systems that operate through unsupervised machine learning or deep learning, must learn through trial and error. These errors can have real and profound human costs.

AI's weakness when it comes to novel situations has clear implications for its application in the sphere of general corporate compliance. As seen with the Hezbollah example, sanctioned organizations can be complex, well-organized, and well-funded enough to find novel ways of incorporating dirty money into the system. They are also able to take advantage of sympathetic or corrupt government organizations, financial institutions, and opaque corporate registries. Effective protection of your brand's reputation requires a comprehensive due diligence program which can account for novel circumstances. Bad actors become successful by taking advantage of and adapting to systemic loopholes; the best way to prevent regulatory issues such as AML, OFAC, and FCPA violations is to counter bad actors with an equally adaptive approach to risk assessments and investigations.

Perhaps the issue that has raised the most skepticism toward the widespread adoption of AI technologies is the concern that AI will serve as a tool to reinforce and even amplify existing forms of social bias.

While we might assume that structural inequity is primarily a problem found in under-scrutinized and poorly written applications, the issue may be more thorny and tenacious than proponents of AI might have originally hoped. For example, according to an October 9, 2018 Reuters report, Amazon disabled an AI-based recruitment tool, after finding that the program was biased against women. The program, which began development in 2014, was meant to aid in Amazon's search for top-tier job applicants, and was designed to rate resumes via a five-star system. A year into development, Amazon realized that its AI tool for processing applications was rating resumes in a way which unfairly favored male candidates.

The machine-learning element of the system had been trained on previously submitted resumes; due to the overrepresentation of men in the tech sector in the decade prior to the software's development, most of the resumes the AI trained on were submitted by men. This resulted in the AI downgrading the resumes of candidates from all-woman's colleges as well as resumes which included the descriptor "women's" (i.e. "women's chess club captain"). Even more granularly, the AI was found to favor resumes which featured language more commonly found on resumes submitted by men, i.e. terms such as "executed" and "captured."

While Amazon initially corrected for these mistakes, the tech behemoth ultimately scrapped the project as there was no way of determining with a sufficient degree of certainty that other elements of bias did not exist in the system.[25] As Rachel Goodman, a staff attorney for the American Civil Liberties Union pointed out, while Amazon acted properly in abandoning its AI recruitment program after if found it was unable to adequately address the issue, other such tools are proliferating across hundreds of other companies, putting these entities at risk of Title VII violations.[26] As the Harvard Business Review further explains, such programs can also undermine a corporation's stated diversity initiatives.[27]

Just as there has been increased interest in AI-driven recruitment tools which function by examining the data presented in a resume and predicting the applicant's likelihood of success at a given job, there has been a similar rise in the prevalence of AI-driven risk assessment tools. These risk assessment tools—which are becoming commonplace in various judicial systems throughout the country, often as part of sentencing guidelines—have been found to have similar issues regarding encoded elements of bias.

A study published by ProPublica on May 23, 2016, examined the risk assessment scores of over 7,000 individuals arrested between 2013 and 2014 in Broward County, Florida. According to ProPublica, Broward County uses a risk assessment tool known as Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), developed by the private company Northpointe. Researchers than compared the risk assessments provided by COMPAS against the rates of re-offense for the following two years in order to determine the predictive accuracy of the COMPAS algorithm.

Summary of *ProPublica's* findings regarding Machine Bias Broward County's Risk Assessment Tool

	White	African American
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

(Julia Angwin, et al. "Machine Bias," *ProPublica*)

The tool was found to be "remarkably unreliable" in its predictions regarding violent offenses: "Only 20 percent of the people predicted to commit violent crimes actually went on to do so." Further, researchers found that the algorithm would systematically label black defendants as higher-risk and white defendants as lower-risk: "Black defendants were still 77 percent more likely to be pegged as at higher risk of committing a future violent crime and 45 percent more likely to be predicted to commit a future crime of any kind," even when controlling for criminal history, rate of recidivism, age, and gender.[28]

In both the COMPAS risk assessment example and the various recruitment tool examples, one major source of criticism is the general lack of transparency in proprietary machine learning systems. In the case of COMPAS, defendants may have difficulty contesting the results of the risk assessment because, while the defendant's attorney may have access to the COMPAS report, the mechanisms by which data regarding the defendant is converted into a score, are not typically revealed.[29]

Meanwhile the ACLU has announced that it has filed a lawsuit contesting the constitutionality of the Computer Fraud and Abuse Act (CFAA) which criminalizes unauthorized uses of websites, including attempts by "academics, researchers, and journalists from testing for discrimination on the internet" such as auditing proprietary hiring software and AI applications.[30] As one ACLU attorney writes, while the companies who have designed hiring algorithms contend that their applications are free from bias, since these software programs and their underlying logic are proprietary, third-party audits are necessary to determine compliance with Equal Employment Opportunity Commission (EEOC) standards.[31]

Issues of access regarding AI mechanisms are at the heart of a new complaint filed by the Electronic Privacy Information Center (EPIC) with the Federal Trade Commission against the company, HireVue, Inc., a Utah-based technology company which "markets and conducts pre-hire assessments using facial recognition technology, biometric data, and artificial intelligence."

According to EPIC's November 6, 2019 complaint, HireVue's job candidate assessment software, which is used by over 700 corporate customers, including Hilton, Ikea, Oracle, Dow Jones, Koch Industries, AB InBev, Penguin Random House, and Anheuser-Busch, violated the guidelines established by the Organization for Economic Cooperation and Development (OECD) and the Federal Trade Commission for the ethical use of artificial intelligence.

Reportedly, HireVue uses proprietary AI software to conduct video interviews and evaluate potential hires via game play. HireVue's website stated that it collects "tens of thousands of data points" including "intonation," "inflection," and "emotions" in order to assess a candidate's aptitude for a position. HireVue's CTO stated that 10%-30% of the candidate's score is derived from an analysis of facial expressions, while the remainder is derived from the language used by the candidate. EPIC contended that HireVue's practices violate the FTC in two ways: First, the HireVue website states that the company does not use facial recognition technology; however, the facial data that HireVue collects meets the FTC's definition of facial recognition technology. Second, EPIC argues that because HireVue's algorithms are secret and proprietary and because the candidate is never given access to their score or to the algorithms underlying the scoring process, the candidate is unable to know or consent to the ways in which their personal data is being used. EPIC further notes that HireVue has not ensured that its assessments are accurate, reliable, or free of discrimination.[32] The Federal Trade Commission's ruling with regard to this complaint will serve as a useful benchmark in evaluating the acceptable uses of AI as part of the hiring process.

The FTC's response to EPIC's complaint against HireVue will also prove relevant in corporate compliance circles as due diligence often entails pre-employment screenings.

Depending on their content, some pre-employment screenings and background checks fall under the purview of the Fair Credit Reporting Act (FCRA). As such, many pre-employment investigations require that prospective employees provide written consent after being informed of the scope of the screening. Should the FTC find that HireVue violates disclosure and consent standards it may have implications for the ways in which similar algorithm-driven technologies can be used as part of pre-employment background checks.

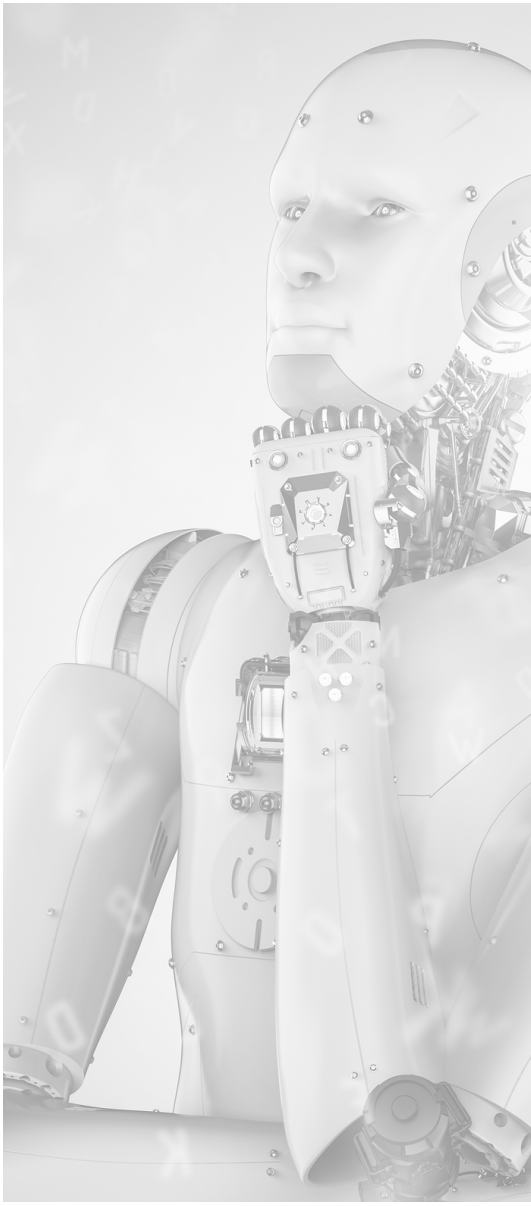
Further, background checks must also follow guidelines set out by the Equal Employment Opportunity Commission (EEOC) and cannot be used to discriminate based on race, religion, sex, etc. Cases such as EPIC's FTC complaint against HireVue may prove to be sources of precedent regarding bias in algorithmic and machine learning applications.

KEY POINTS

- Transaction-centric AI applications, such as those used within fintech, often result in false positives, leading investigators to focus on cases which are ultimately not deemed to be high risk.
- AI applications sift through large amounts of data to locate suspicious actions or transactions. However, regulatory and law enforcement agencies are more focused on bad actors and the illicit organizations to which they belong. Thus regulatory and law enforcement agencies may spot areas of risk or violations that might not be caught by AI.
- Relatedly, transaction-based machine learning analysis may miss important information which can be gleaned from the context of a given business transaction or partnership – i.e. socio-political cues.
- There may be potential regulatory ramifications of relying on black-box algorithms to provide assessments, especially in pre-employment due diligence.
- Machine learning has difficulty processing novel forms of data and seeking outside-the-box solutions

SECTION 4
Putting Things in Context: The Continued Role of Human Intelligence

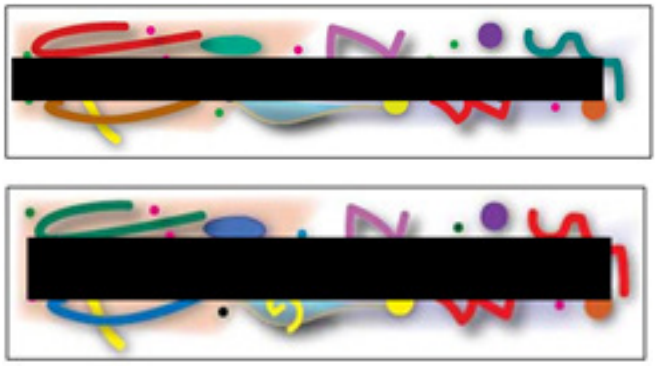
As discussed in the previous section, one major drawback of machine learning based approaches to anti-corruption investigations is that these applications tend to focus on actions and transactions rather than on actors. While one of AI's strengths is its ability to analyze large quantities of data from a limited number of sources, human analysis is able to access a much wider variety of sources and thus additional information. Such information is often required to minimize the number of false positives in compliance reports. In due diligence, false positives often take the form of name match records. While an AI application could be used to consult sanctions lists databases for the names of prospective partner companies and their officers, such searches would result in numerous name match and similar name match entities.



Additional information sources are often required to deconflict such name matches so that a compliance officer can ensure that a business partnership or transaction can proceed with a minimal risk of violating the Foreign Corrupt Practices Act (FCPA), sanctions maintained by the Office of Foreign Assets Control (OFAC), or other regulatory statutes. Human analysts are able to research a wide variety of publicly available sources such as business registries, birth registries, land records, and media sources in order to find the identifiers needed to eliminate (or verify) many name match records.

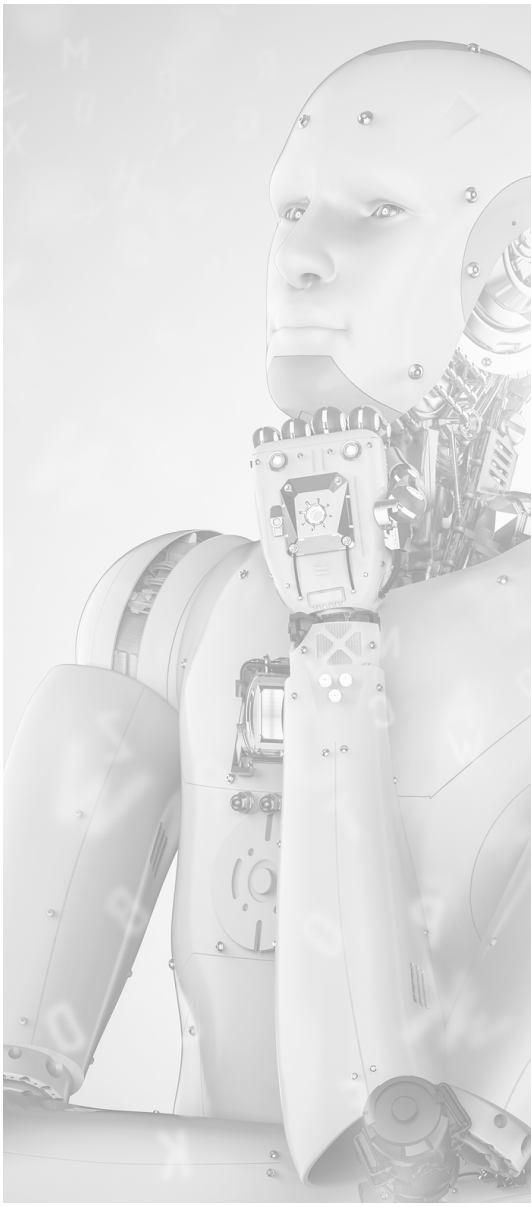
Beyond denied party and sanctions lists research, due diligence investigations can develop in directions that may not have been foreseen at the outset of research. Often lines of inquiry develop organically through the course of an investigation, based on the client's needs, the nature of the business risk, or the type of information located. Robust anti-corruption compliance requires a degree of flexibility with regard to research methodology in order to get full account of the risk present in a business relationship.

For example, Kreller recently conducted an investigation on behalf of a client who wanted to find information regarding a website offering investment advice. The website did not appear to be the official website of a named company and domain registration information had been privatized so that the identity of the registrant could not be immediately determined. As the investigation progressed, evidence arose suggesting that the investment website was created by an individual who was also affiliated with the website for a media company specializing in prank phone call tapes. Given the surprising nature of the apparent link between the investment site and the media company, one goal of the investigation became finding additional evidence to link the former site to the latter site and, ultimately, to the individual affiliated with the media group. One link came in the form of a distinctive graphic used on both webpages to offset the site's contact information, as illustrated in redacted form below:

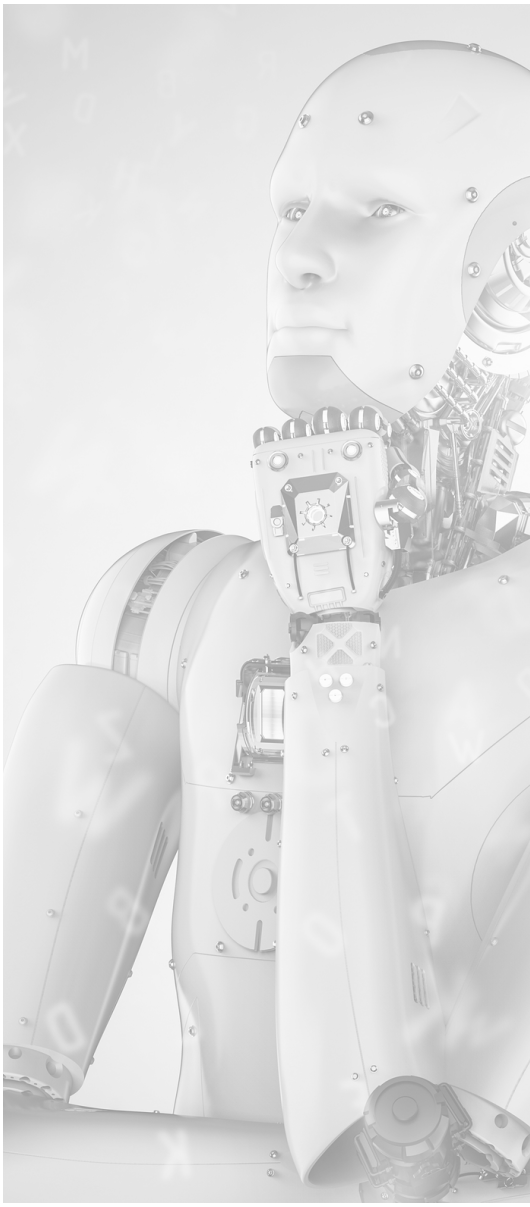


Top: Image of contact email (redacted) from the client-provided investment website
Lower: Image of contact email (redacted) from the media website discovered during the course of the investigation

This and other stylistic similarities between the two webpages bolstered our confidence that we had determined the identity of at least one individual affiliated with the client-provided website.



While many corporate due diligence investigations are fairly routine —a few legal filings, perhaps some bad press— some require creative problem solving in order to locate information which would provide the client with a complete picture of an entity's potential for risk. In one case, Kreller analysts identified a regular social venue for an individual by matching a generic patterned carpet found in several of the individual's Facebook photos with Instagram photos of a club which had hosted a deceased relative's band. In another instance, a Kreller analyst was tasked with locating the business affiliations of an Indian individual residing in the United Arab Emirates.

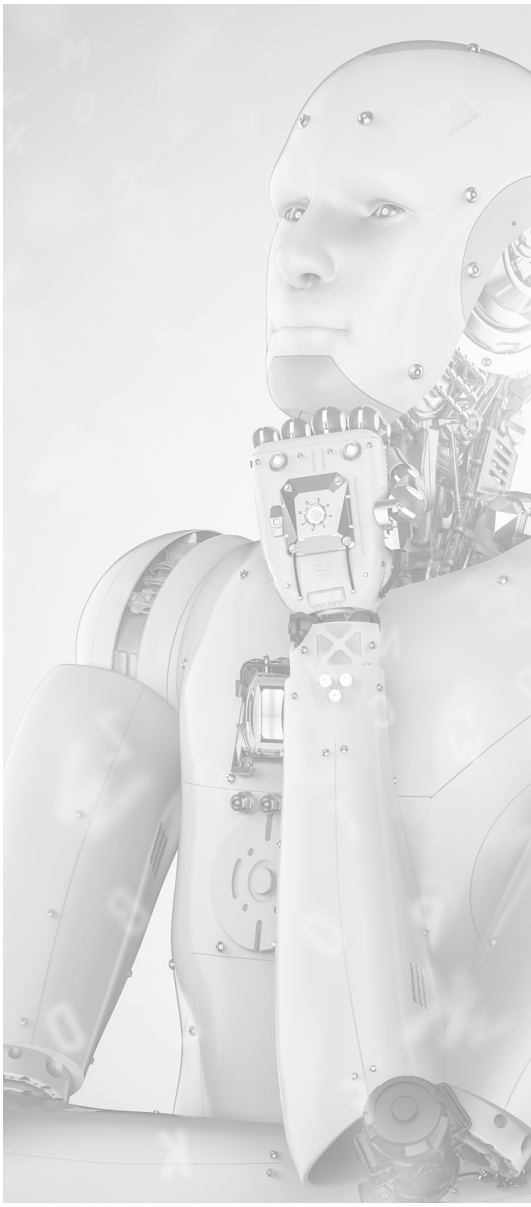


Many of the business affiliations for this individual were registered to other people from the same tiny hamlet in the Indian state of Kerala. Business affiliations research was conducted by cross referencing information from the social media pages of the cohort from Kerala with corporate registration and chamber of commerce records in the UAE. Of course, AI can be trained to recognize formatting and rhetorical similarities across websites, or to identify carpet patterns, or to cross reference the Abu Dhabi Chamber of Commerce and Industry with the Facebook pages of Indian expatriates. However, these lines of inquiry all arose from the idiosyncratic elements of each of these investigations. The unique nature of these cases reveals the blind spots of certain AI applications. Instead, due diligence investigations which present surprising twists and turns require the ability to shift between and synthesize numerous information sources. In terms of data analysis, AI is a very precise and powerful tool – the investigative equivalent of a pre-programmable precision laser cutter; in contrast a seasoned investigator is a multi-tool.

Beyond the human advantage with regard to the novelty factor, human intelligence (HUMINT) remains necessary when confronting a number of geo-political challenges within due diligence investigations. One such challenge involves the increase in international legislation involving digital privacy. For example, the General Data Protection Regulation (GDPR), which came into effect in the EU in May 2018, gives European consumers far greater control over how their personal identifying information is collected and disseminated.

The GDPR provides EU data subjects with a range of new rights including:

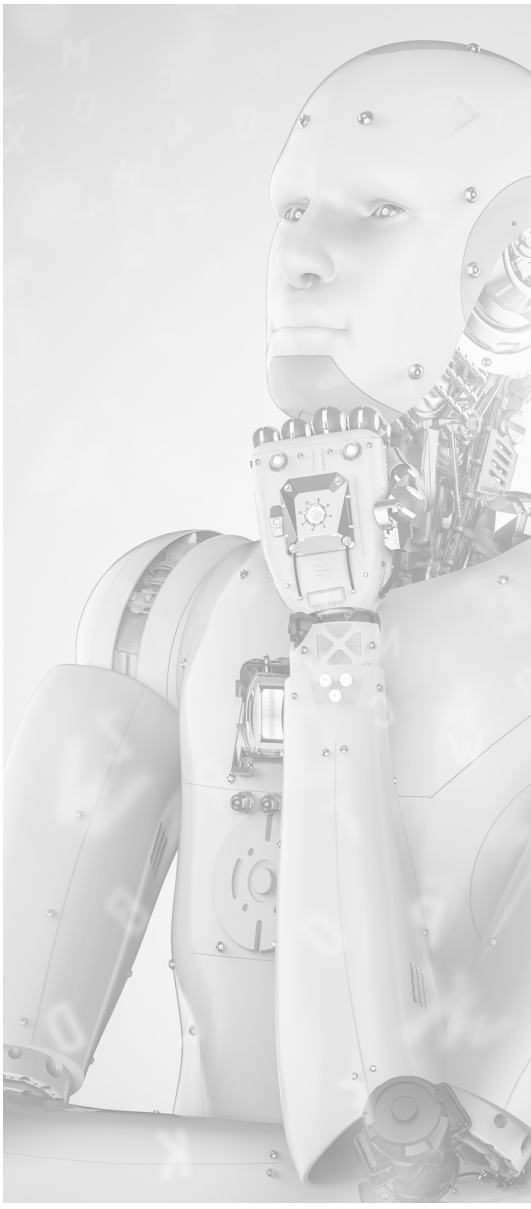
1. Stronger laws governing the conditions of consent for companies seeking to collect personal identifying information;
2. The right to access, which provides consumers with information regarding both the personal data collected by third parties and the reasons for the data collection;
3. The right to be forgotten, which allows consumers to withdraw consent for the collection and distribution of personal identifying information;
4. The right to timely notification should personal identifying information be compromised through a data breach.[33]



California has passed similar digital privacy legislation set to take effect in January 2020. The New York Times described the California Consumer Privacy Act (CCPA) as "one of the most significant regulations overseeing the data-collection practices of technology companies in the United States.[34]" As we think back to the HireVue example, relying on AI for data collection purposes may have serious ramifications under such privacy laws, as consumers are able to request information on both the information obtained and the reasons and methods used for the collection, perhaps shining light on the algorithmic data collection employed by AI.

Human-driven due diligence typically derives information from two types of sources: publicly available records and information uncovered via interpersonal communication. Investigations which utilize public records such as corporate registries, legal filings, regulatory filings, land registries, and birth registries are typically known as open-source intelligence (OSINT). One benefit of an open source investigation is its transparency; the sources of individual records are clearly stated and the scope of an open source report can be adjusted based on the nature of the consent received from the subject of the report and based on the jurisdiction in which a report is being conducted. In contrast to identifying information gathered through some forms of AI, OSINT investigations don't typically have a black box filled with proprietary methodology to protect.

In addition to limits imposed by privacy laws on information gathering, another more troubling investigative challenge arises in jurisdictions in which the internet and media are tightly controlled and censored by the government. In some jurisdictions there is a growing worry that AI and machine learning are being adopted in the service of authoritarian and anti-democratic forces, as seen in concern over "deep fakes" being employed to undermine elections[35] as well as surveillance technologies used to stifle political dissent and control minority groups in countries such as China.[36]



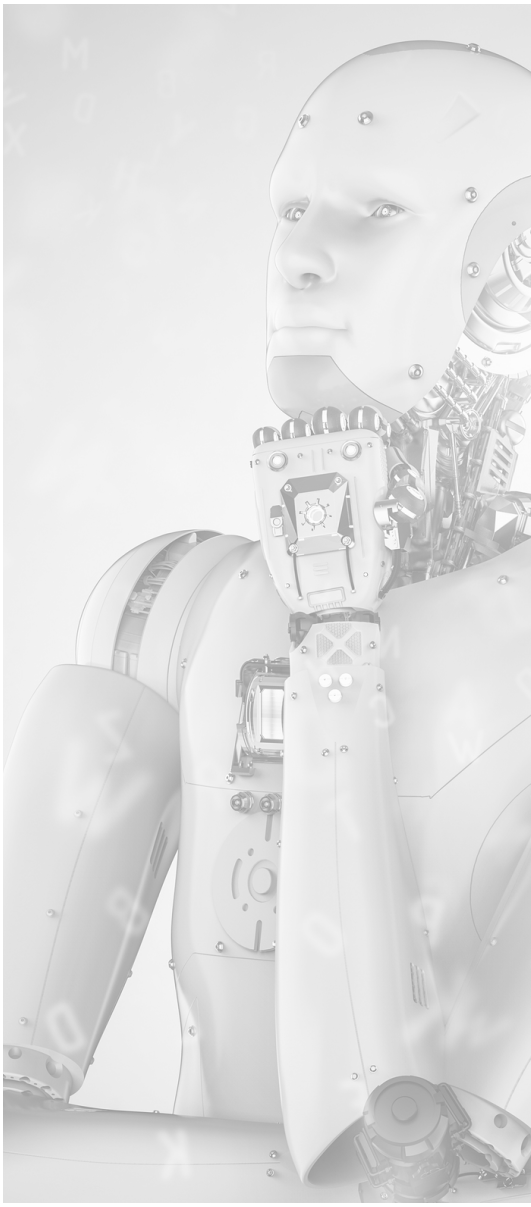
The renowned philosopher of science and prominent AI theorist Daniel Dennett reflected on some of these issues in a February 2019 essay for Wired. Dennett argues that AI is now able to create perfect forgeries of events that never transpired and that such capabilities will "render obsolete the tools of investigation we have come to take for granted in the past 150 years." He argues that while analog sources of evidence, i.e. photos taken on film and secured through a tight chain of custody may provide a temporary solution, the negative aspects of AI are here to stay. "The information age is also the disinformation age.[37]"

One tool in the arsenal for conducting due diligence research in jurisdictions known for media censorship and control, politically motivated arrests, and other forms of disinformation is the strategic use of in-person intelligence gathering by trusted local investigators. Kreller recently conducted a corporate due diligence investigation set in Uzbekistan, a country which Transparency International ranked 158th out of 180 countries for its perceived level of corruption. Transparency International notes that Uzbekistan lacks an independent media and a functionally autonomous judiciary.[38]

Media research indicated that the subject of the report, an executive within the energy sector, had at one time been arrested and detained for alleged embezzlement. However, no criminal record was located to corroborate these media reports. During the course of discreet character and reputation inquiries, conducted by Kreller's in-country investigator, several sources within the business community reported that the subject's arrest was politically motivated.

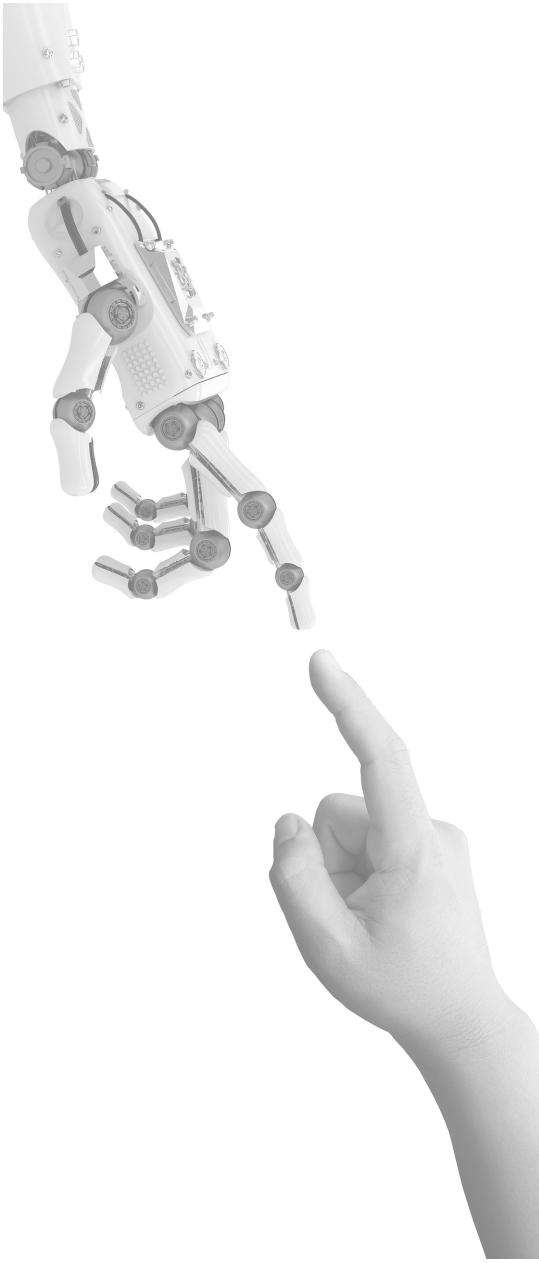
The sources also stated that the subject was one of a number of wrongfully imprisoned businessmen who was released and rehabilitated following the instatement of a new political regime. While media sources were located which indirectly indicated that the subject had been released from prison, no media reports were located specifically detailing the subject's reported exoneration. In a case such as this one, a fully machine-based approach to the investigation would have failed to uncover many of the case's critical details.

Artificial Intelligence can be used to scan news sources in search of derogatory information pertaining to an entity, but such tools are less useful when the media is subject to political censorship or control. In this Uzbekistan case human intelligence, in the form of discreet inquiries made within the industry, were necessary to achieve a sense of the context of the subject's arrest as well as details regarding the nature and timing of his release.



SECTION 5
Adding to the Anti-Corruption Toolkit: AI Coupled with Supplemental Analysis

Moving forward, what can we expect to be the role of AI in compliance? Will some permutation of IBM's Watson replace due diligence analysts and investigators?



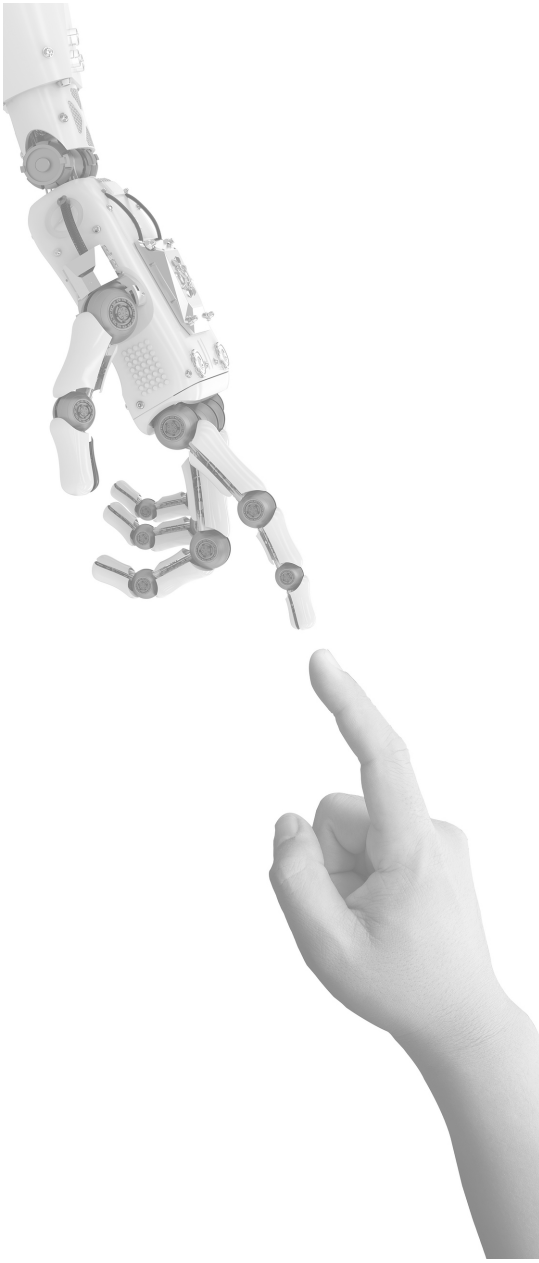
AI has a long and fruitful history in the financial sector as a tool for detecting money laundering and fraud. AI also shows promise in more general corporate compliance because it can pore through large quantities of data to analyze patterns and seek out anomalies. Additionally, AI can be a useful tool for repetitive labor-intensive activities, such as gleaning records from large sanctions lists and databases, and for constructing risk matrices. In such situations, AI can prove to be an efficient and cost effective strategy for some forms of anti-corruption compliance. However, artificial intelligence is especially limited when confronted with novel data sources or new quandaries. Conversely, creative problem solving is a hallmark of an effective fraud investigator. Human analysists are able to adjust the direction of the case based on numerous variables such as client expectations, the socio-political context of the report, and various risk factors and lines of inquiry that arise during the course of the investigation.

CPA and Certified Fraud Examiner Gary Krausz of Gursey Schneider LLP and John Colthart of MindBridge AI likened their successful use of a human/AI hybrid model to the division of labor within a bomb squad. AI identifies the signature of the device (i.e. the signature and evidence of the fraud), while the human analysts dismantled the bomb (i.e. built the forensic case from the evidence).[39] While Krausz and Colthart are describing the use of AI in conducting a forensic audit, some of the same principals can be applied to general corporate due diligence. Much of the rule-intensive and prescriptive work, i.e. sanctions lists searches, database searches, general organization and formatting, could be handled by an AI program, allowing human analysts to approach the investigative process with a more targeted focus.

For example, the AI program could discover a name match record for a politically exposed person (PEP). The human investigator could do additional research using an array of sources to eliminate or verify this record as belonging to the subject. The investigator could then conduct additional context-specific research to determine the nature of the subject's political or governmental affiliations in order to address the bribery risk this may pose to the client. Such a collaborative model would require analysts and investigators to be aware of the blind spots in the AI program and to address these weaknesses through their own strategic interventions into the investigation.

A hybrid model could provide numerous benefits to a client. First, AI allows reports to proceed more quickly and efficiently. Less labor would be needed to translate corporate registration documents, sift through databases, and comb over legal filings. This would free up investigators to target high risk aspects of a report and dig in on complex and potentially productive lines of inquiry. A collaborative model could reduce costs and turn-around times, while still allocating the resources and human capital necessary for complex investigations. Such high-quality intelligence could potentially further impact a company's bottom line by saving money which could have otherwise been lost to fraud, bad deals, regulatory infractions and fines, or brand erosion caused by bad press.

While AI is regularly billed as a panacea for various industries, it is in fact a powerful tool with a limited scope of applications. When it comes to intelligence within corporate due diligence, the old adage stands: two heads are better than one.



SECTION 6
Sources

1. **The Board of Governors of the Federal Reserve System, et al**. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing." Financial Crimes Enforcement Network. December 2018. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf
2. **Blanco, Kenneth A**. "Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the SIFMA Anti-Money Laundering & Financial Crimes Conference." Financial Crimes Enforcement Network. February 2019. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-sifma-anti-money-laundering
3. **Buchanan, Bonnie G**. "Artificial Intelligence in Finance." The Alan Turing Institute. April 2019 https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_1.pdf
4. **Kaplan, Jerry**. Artificial Intelligence: What Everyone Needs to Know (Oxford: Oxford University Press, 2016), 5.
5. **Snow, Jackie**. "An A.I. Glossary." The New York Times. October 2018. https://www.nytimes.com/2018/10/18/business/an-ai-glossary.html
6. **Columbus, Louis**. "How AI Is Protecting Against Payments Fraud." Forbes. September 2019. https://www.forbes.com/sites/louiscolumbus/2019/09/05/how-ai-is-protecting-against-payments-fraud/#4a78d0b54d29
7. **Gary Krausz and John Colhart**. "How Artificial Intelligence Uncovered Evidence of Fraud." ACFE Insights. December 2018. https://acfeinsights.squarespace.com/acfe-insights/2018/12/14/how-artificial-intelligence-uncovered-evidence-of-fraud
8. **Buchanan**. "Artificial Intelligence in Finance."
9. **Twomey, Niall**. "5 Ways AI is Impacting AML and KYC Compliance." Corporate Compliance Insights. December 2018. https://www.corporatecomplianceinsights.com/5-ways-ai-is-impacting-aml-and-kyc-compliance/
10. **Council, Jared**. "FICO Rolls Out AI Tools for Digital Authentication." WSJ Professional Resources. November 2019. https://www.wsj.com/articles/fico-rolls-out-ai-tools-for-digital-authentication-11573036201
11. **Verdict**. "FICO rolls out AI-driven authentication capabilities to combat fraud." Retail Banker International. November 2019. https://www.verdict.co.uk/retail-banker-international/news/fico-rolls-out-ai-driven-authentication-capabilities-to-combat-fraud/
12. **Fruth, Joshua**. "Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states." Reuters. March 2018. https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV

13. Ibid.
14. Ibid.
15. Ibid.
16. **Jay Weaver and Nicholas Nehamas**. "He made big bucks off Ovaltine and fancy furniture. Was he 'duped' into dealing dirty gold?" Miami Herald. January 2018. https://www.miamiherald.com/news/local/community/miami-dade/article194188324.html
17. **U.S. Attorney's Office, Southern District of Florida**. "U.S. Gold Refinery Pleads Guilty to Charge of Failure to Maintain Adequate Anti-Money Laundering Program." United States Department of Justice. March 2018. https://www.justice.gov/usao-sdfl/pr/us-gold-refinery-pleads-guilty-charge-failure-maintain-adequate-anti-money-laundering
18. **Miami Herald Investigations Team**. "How a $3.6B Gold Scheme Went Bust." Miami Herald. January 2018. https://www.miamiherald.com/news/nation-world/world/americas/article194362569.html
19. **Weaver, Jay**. "Firm behind gold-fueled, Miami-based money-laundering racket fined $15 million." Miami Herald. March 2018. https://www.miamiherald.com/news/local/article205503659.html
20. **Weaver, Jay**. "Once at center of 'sprawling' money-laundering scheme, Miami gold dealers headed to prison." Miami Herald. January 2018. https://www.miamiherald.com/news/local/article195552089.html
21. **Jay Weaver and Nicholas Nehamas**. "He made big bucks off Ovaltine and fancy furniture. Was he 'duped' into dealing dirty gold?"
22. **National Transportation Safety Board Office of Public Affairs** "Preliminary Report Released for Crash Involving Pedestrian, Uber Technologies, Inc., Test Vehicle." National Transportation Safety Board. May 2018. https://www.ntsb.gov/news/press-releases/Pages/NR20180524.aspx
23. **Aarian Marshall and Alex Davis**. "Uber's Self-Driving Car Didn't Know Pedestrians Could Jaywalk." Wired. November 2019. https://www.wired.com/story/ubers-self-driving-car-didnt-know-pedestrians-could-jaywalk/
24. **Levine, Matt**. "The Computers Are Sorry About the Flash Crashes." Bloomberg. January 2019. https://www.bloomberg.com/opinion/articles/2019-01-03/the-computers-are-sorry-about-the-flash-crashes
25. **Dastin, Jeffrey**. "Amazon scraps secret AI recruiting tool that showed bias against women." Reuters. October 2018. https://uk.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUKKCN1MK08G
26. **Goodman, Rachel**. "Why Amazon's Automated Hiring Tool Discriminated Against Women." ALCU Free Future Blog. October 2018. https://www.aclu.org/blog/womens-rights/womens-rights-workplace/why-amazons-automated-hiring-tool-discriminated-against
27. **Bogen, Miranda**. "All the Ways Hiring Algorithms Can Introduce Bias." Harvard Business Review. May 2019. https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias

28. **Angwin, Julia, et al**. “Machine Bias.” ProPublica. May 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
29. Ibid.
30. **ACLU**. “Sandvig v. Barr — Challenge to CFAA prohibition on uncovering racial discrimination online.” ACLU. May 2019. https://www.aclu.org/cases/sandvig-v-barr-challenge-cfaa-prohibition-uncovering-racial-discrimination-online?redirect=cases/sandvig-v-sessions-challenge-cfaa-prohibition-uncovering-racial-discrimination-online
31. **Goodman, Rachel**. “Why Amazon’s Automated Hiring Tool Discriminated Against Women.”
32. **Federal Trade Commission** “In the Matter of HireVue, Inc.” EPIC. November 2019. https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf
33. EU GDPR Portal. (https://eugdpr.org)/
34. **Wakabayashi, Daisuke**. “California Passes Sweeping Law to Protect Online Privacy.” The New York Times. June 2018. https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html
35. **Villasenor, John**. “Deepfakes, social media, and the 2020 election.” The Brookings Institute. June 2019. https://www.brookings.edu/blog/techtank/2019/06/03/deepfakes-social-media-and-the-2020-election/
36. **Mozur, Paul.** “One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority.” The New York Times. April 2019. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
37. **Dennett, Daniel C.** “Will AI Achieve Consciousness? Wrong Question.” Wired. February 2019. https://www.wired.com/story/will-ai-achieve-consciousness-wrong-question/
38. **Transparency International**. “Uzbekistan.” https://www.transparency.org/country/UZB
39. **Gary Krausz and John Colhart**. “How Artificial Intelligence Uncovered Evidence of Fraud.”

SECTION 7
ABOUT KRELLER GROUP

OUR COMPANY
Kreller Group is a trusted provider of worldwide compliance solutions, serving a global client base, including many Fortune 500 and Fortune 100 companies.

We have performed services in more than 180 countries and conducted over 125,000 investigations since 1988. Kreller is a licensed private investigative agency (PI License Number 201121001923) affiliated with industry associations such as ASIS International, Association of Certified Fraud Examiners, Overseas Security Advisory Council, World Association of Detectives, Council of International Investigators and the Association of Certified Anti-Money Laundering Specialists.

Kreller Online (KOL) is our revolutionary data management system with vast capabilities including multi-level customization for any company regardless of size and number of affiliations. Our highly secure web-based portal, KOL, allows users to manage third party information globally 24 hours a day, 7 days a week. KOL can administer millions of records and multiple attachments. Kreller's global operations center is located in Cincinnati Ohio.

CONTACT
For more information regarding our compliance solutions, please contact:

Scott Shaffer
Managing Director, Due Diligence
513.723.8011
sshaffer@kreller.com
www.kreller.com

AUTHOR INFORMATION
Lauren Caryer, PhD
Tel. 513.723.8914
lcaryer@kreller.com