Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Artificial Intelligence: Compliance risks & benefits

An e-Book publication sponsored by Socure

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

Socure

Socure is the leader in Day Zero digital identity verification technology. Its predictive analytics platform applies artificial intelligence and machine-learning techniques with trusted online/offline data intelligence from email, phone, address, IP, device, velocity and the broader internet to verify identities in real-time. Socure powers financial inclusion—approving as much as 40% more millennial and other thin-file consumers. It also reduces fraud for online new account openings by up to 95% with false positives of better than 1:1, and cuts manual review rates by as much as 90%. Socure was founded in 2012 by Johnny Ayers and is led by CEO Tom Thimot. The company is based in NYC, with offices in San Diego, San Jose, and Chennai, India.

Inside this e-Book

AI tools carry risks, benefits for securities industry

A study of AI use in the securities industry found many challenges, but "significant benefits" as well, reports **Aaron Nicodemus**.

A Financial Industry Regulatory Authority (FINRA) white paper released recently found that large broker-dealer firms have successfully implemented Artificial Intelligence (AI) tools in areas including communications with customers, investment processes, and operational functions.

The report, which included input from broker-dealer firms, academics, technology vendors, and service providers, concluded that, when regulated properly, firms can use AI tools to increase efficiency, increase productivity, improve risk management, enhance customer relationships, and increase revenue opportunities. The report was the result of a two-year study of AI use among broker-dealers.

Many firms have already applied AI tools to compliance and risk management functions, the report found.

AI-based credit-scoring systems "have faced criticism for being opaque and potentially biased and discriminatory. These models not only analyze traditional credit-evaluation criteria, such as current financial standing and historical credit history, but may also identify other demographic factors as deterministic criteria, which could lead to unfair and discriminatory credit scoring based on biases present in the underlying historical data."

FINRA report

AI tools were crucial in both expanding the reach of surveillance and monitoring tools to include new communication pathways like video chats, images, and more, while at the same time reducing "false positive" alerts, allowing compliance professionals to focus their attention on the remaining alerts. Firms were also successfully implementing AI tools for know your customer (KYC) and financial crime monitoring.

Similarly, Artificial Intelligence tools could prove effective in regulatory management, allowing firms to digitize the traditionally manual process of regulatory review and compliance.

"Some industry participants noted that automated regulatory intelligence management programs have the potential to increase overall compliance, while reducing both costs and time spent implementing regulatory change," according to the white paper.

With pressure from regulators and the market to improve cyber-security practices, firms are examining how Artificial Intelligence tools can "assist overwhelmed cybersecurity staff to predict potential attacks, detect threats in real-time, and respond to them faster and at lower costs," noted the report.

One area where FINRA expressed concern about the use of Artificial Intelligence tools was in credit risk management. The tools can be used to speed up assessments of the creditworthiness of their counterparties, but some AI-based credit-scoring systems "have faced criticism for being opaque and potentially biased and discriminatory. These models not only analyze traditional credit-evaluation criteria, such as current financial standing and historical credit history, but may also identify other demographic factors as deterministic criteria, which could lead to unfair and discriminatory credit scoring based on biases present in the underlying historical data."

For communicating with customers, artificial intelligence is all about efficiency. Virtual assistants are ubiquitous at large broker-dealers, providing the first response to customer inquiries by providing answers to some and routing others. E-mail inquiries are also handled using AI-enabled digital tools. More cutting-edge AI tools are being tested to provide targeted marketing to customers and potential customers. The AI tools "analyze their customers' investing behaviors, Website and mobile app footprints, and past inquiries, and in turn, to proactively provide customized content to them."

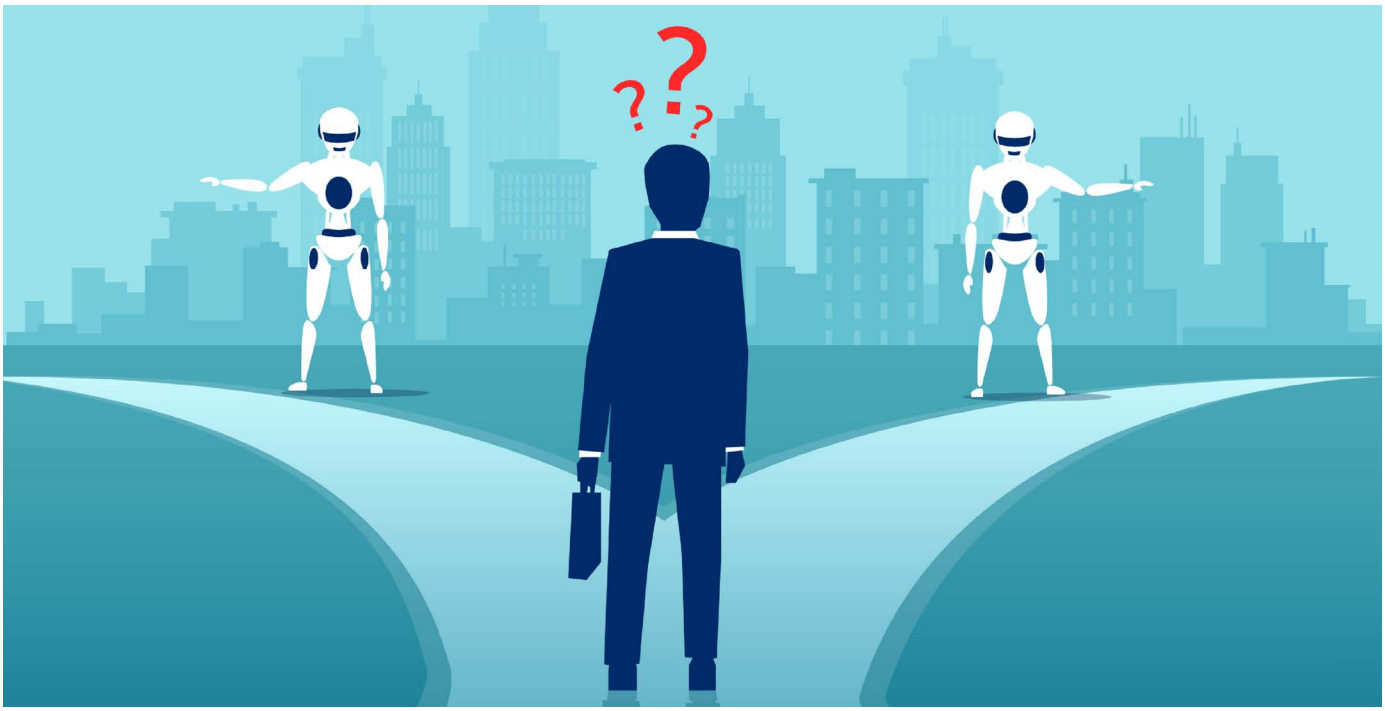
The idea of using Artificial Intelligence to monitor trades and customer behavior is more common in brokerage account management, according to the FINRA report's findings.

"Industry participants indicated that registered representatives use this information to augment their existing knowledge and expertise when making suggestions to their customers," the report ascertained, adding that organizations can also use this information to create customized research on investment opportunities for their customers.

In portfolio management and trading, AI tools can help broker-dealers predict price movements and maximize trading speed and price performance. But the report also noted that using AI to make automated trades comes with pitfalls, particularly when the market is experiencing unpredictable swings.

Unmonitored Artificial Intelligence trading transactions "may create a situation where the AI model no longer produces reliable predictions, and this could trigger undesired trading behavior resulting in negative consequences," the report said.

The FINRA report also noted that organizations are using Artificial Intelligence tools to automate paper-based processing and to extract targeted information from digitized documents. ■



Six things to know about recent ICO AI guidance

Recent guidance from the Information Commissioner's Office offers tips on disclosing how AI decisions are made, writes **Neil Hodge**.

The U.K. Information Commissioner's Office released guidance to help organizations explain how AI is used in decision making and how the technology uses personal data to form judgments.

The 122-page publication, called "Explaining decisions made with AI" and written in conjunction with The Alan Turing Institute, the United Kingdom's national center for AI, hopes to ensure organizations can be transparent about how AI-generated decisions are made, as well as ensure clear accountability about who can be held responsible for them so that affected individuals can ask for an explanation.

The guidance consists of three parts:

» **Part 1** on "The basics of explaining AI" is aimed at organizations' designated data protection officers (DPOs) and compliance teams and defines the key concepts.

» **Part 2** on "Explaining AI in practice," which helps organizations with the practicalities of explaining these decisions and providing explanations to individuals, is aimed at technical teams, though the ICO says DPOs and compliance teams will also find it useful.

» **Part 3** on "What explaining AI means for your organization" is primarily aimed at senior management and goes into the various roles, policies, procedures, and documentation that you can put in place to ensure your organization is set up to provide meaningful explanations to affected individuals. However, compliance functions will also find it useful.

Below are six key takeaways from the guidance:

1. Data protection law is technology neutral. It does not directly reference AI or any associated technologies such as machine learning. However, the General Data Protection Regulation (and the U.K.'s 2018 Data Protection Act) does have a significant focus on large-scale automated processing of personal data, and several provisions specifically refer to the use of profiling and automated decision-making. This means data protection law applies to the use of AI to provide a prediction or recommendation about someone.

For example, the GDPR has specific requirements around the provision of information about, and an explanation of, an AI-assisted decision where:

» It is made by a process without any human involvement; and
» It produces legal or similarly significant effects on an individual (something affecting an individual's legal status/rights, or that has equivalent impact on an individual's circumstances, behavior, or opportunities, such as a decision about welfare or a loan).

2. The guidance says that any explanation about how AI is used in decision-making needs to address the processes used in making decisions and how outcomes are reached as a result. The ICO has also identified six main types of explanation:

» Explanation regarding the rationale behind the decision;
» Explanation regarding who is responsible for making the decision;
» Explanation regarding what data has been used to make the decision and how;
» Explanation to ensure the decision was made fairly;
» Explanation to provide reassurance the AI system is performing safely; and
» Explanation to ensure the AI system is being monitored for its impact on individuals and society.

3. To ensure the decisions you make using AI are explainable, the guidance says organizations should follow four principles: Be transparent, be accountable, consider the context you are operating in; and reflect on the impact of your AI system on the individuals affected, as well as wider society.

4. To help design and deploy appropriately explainable AI systems, the ICO guidance outlines six tasks organizations should carry out to meet with customer and regulatory expectations about how personal data is gathered, processed, and used in decision-making. They are:

» Select priority explanations by considering the domain, use case, and impact on the individual;
» Collect and pre-process your data in an explanation-aware manner;
» Build your system to ensure you are able to extract relevant information for a range of explanation types;
» Translate the rationale of your system's results into useable and easily understandable reasons;
» Prepare implementers to deploy your AI system; and
» Consider how to build and present your explanation.

5. At the core of the guidance is the need for organizations to ensure transparency about how decisions are made and accountability about who is responsible for them—including the product manager, implementer, AI development team, compliance function, DPO, and senior management.

The ICO suggests compliance teams (including the DPO) and senior management should expect assurances from the product manager that the system the firm is using provides an appropriate level of explanation to decision recipients. Further, compliance and senior management should ensure they have a "high level" understanding of the systems and types of explanations these AI systems should and do produce.

Additionally, according to the ICO, there may be occasions when the DPO and/or compliance functions need to interact directly with decision recipients—for example, if a complaint has been made. In these cases, compliance teams will need a more detailed understanding of how a decision has been reached, and they will need to be trained on how to convey this information appropriately to affected individuals.

6. Compliance functions will need to be aware that their organizations' AI system may be subject to external audit—perhaps even by the ICO—to assess whether it is complying with data protection law.

During such an audit, organizations will need to produce all documentation they have prepared, as well as the testing they have undertaken, to ensure the AI system is able to provide the different types of explanation required that could be suitably understood by those overseeing the system and monitoring it; regulators; and those affected by the decisions (decision recipients). ■

Socure

A Next-Generation Approach to KYC:

3 Essentials for Safe, Seamless Digital Onboarding

Introduction

Introduced in 2001 as part of the U.S. Patriot Act, Know Your Customer (KYC) compliance is essential for conducting digital business today. These guidelines were established to address the risks of financial crime and to help financial institutions (FIs) fight identity fraud and money laundering activities.

With the introduction of the more recent Title III, FIs must also deliver on two requirements to comply with stricter KYC: the Customer Identification Program (CIP) and Customer Due Diligence (CDD). These regulations allow FIs to accurately verify the identities of their applicants, make sure they're real, confirm they're not on any prohibited lists, and effectively assess their risk factors to mitigate money laundering, terrorism financing, and other financial fraud risks.

Although crucial to the success and safety of customer onboarding, implementing and maintaining a successful KYC program can sometimes create an overwhelming administrative burden. Additionally, navigating manual verification methods is costly and prone to inaccuracy, creating greater risk of customer turnover and lost revenue.

The good news? With the right KYC solution, businesses (including FIs) can overcome these challenges and provide a safe, seamless onboarding experience that mitigates risk while enabling top-line revenue growth.

This paper will explain the three essential elements required for a successful KYC solution that enables a next-generation approach to onboarding, growth and compliance.

3 KYC Essentials for Safe, Seamless Digital Onboarding

The ideal KYC solution will ensure that businesses and FIs get identity verification right every time and will provide feedback that allows the institution to proceed knowing that the applicant doesn't present a risk and is someone with whom they are able to conduct business.

The Ideal KYC solution should include:

1. Advanced analytics-driven identity verification
2. Intelligent, automated global watchlist screening
3. Continual watchlist monitoring

Requirement 1: Advanced Analytics-Driven Identity Verification

As the top requirement for the ideal KYC solution, businesses should be autonomously examining data using sophisticated techniques and tools, typically beyond those of traditional business intelligence (BI), to discover insights, make predictions and generate recommendations on how they are coming to a resolution on the identity.

BUSINESS *ISSUE*

Identity Verification ***MUST*** Be Fast and Accurate

Why is this so important?

The ultimate goal of KYC compliance is to verify identities quickly and accurately, allowing businesses to gain high auto-approval rates and minimize manual reviews.

The ideal solution should include advanced analytics techniques including data mining, machine learning, pattern matching, forecasting, cluster analysis and more to ensure high match rates and fast response within seconds.

Using advanced analytics enables institutions to experience and benefit from accurate, automated identity verification with over 90% auto-approval rates.

In contrast, solutions that only apply simple, binary-based matching with little to no intelligence will produce lower-than-desired auto-acceptance rates in the 60-70% range.

This is why implementing advanced analytics for identity matching is key. Incorporating a broad range of advanced analytics techniques increases accuracy, maximizes auto-acceptance rates, alleviates customer friction and improves the onboarding experience.

DIVERSE DATA COVERAGE AND PROPRIETARY SEARCH ANALYTICS EQUATE TO A BEST-IN-CLASS SOLUTION

We are well past a time when credit and KBA checks alone are enough to keep bad actors at bay. Achieving the best identity verification outcomes from a KYC solution requires large and diverse data sources with billions of records. Such a database holistically reflects the population, including mainstream and underbanked or thin-file consumers.

When evaluating KYC solutions, businesses will want to look for the following data sources:

1. Ingested data feeds
   - Credit bureaus
   - Telecom records
   - Utility records
   - Verified identities
   - Social Security records for deceased individuals
   - Marketing records that include addresses and phone numbers
   - Student data
   - Military data
   - NIST 800-63 Authoritative Sources
2. Techniques to standardize, validate, correct, deduplicate, and resolve multiple entities
3. Continuous data updates to maintain quality and avoid degradation

ADVANCED DATA ANALYSIS AND RESOLUTION

With a breadth of data sources, businesses require a KYC solution that applies advanced analytics techniques to intelligently analyze the data and deliver accurate results. The solution must go well beyond a simple binary, text-based matching approach, which is inadequate to manage analysis on the billions of records or to yield accurate results.

Basic, rules-based KYC solutions have been available for years. They walk through the multiple characteristics of a person's profile, weigh them and deduce if any number of them signal risk. However, bad actors have a number of ways to circumvent these simple techniques.

BUSINESS *VALUE*

Intelligent Data Analysis Delivers **90%+** Auto-Approval Rates

In contrast, a solution with intelligent analytics techniques like machine learning algorithms can provide the foundation for the best path forward to accurately ensure a provided identity is real.

Why advanced analytics?

In terms of innovation and applying AI to big data, advanced analytics and machine learning can often be misunderstood. When considering their merits in identity verification solutions, it's important to understand some of the specific capabilities they should provide.

Scale

First, there's serious scalability. Rules-based systems are not capable of analyzing the dynamic data needed to recognize the nuanced and emerging patterns of identity and synthetic fraud. However, a KYC solution that uses advanced analytics can automate this effort at scale to clean and normalize the data while providing rigorous quality assurance scrutiny.

Correlation

Then, there's the value of data correlation that advanced analytics provides with the ability to combine data sources into the idea of an "identity cluster." This provides greater detail with a longer history on an identity and allows the solution to accurately determine whether the identity, as a whole, represents a real individual.

For example, checking against a single source like a Social Security number provides limited identity matches. However, when searching that identity's data records further, across sources, a KYC solution can use fuzzy approximation to uncover name derivatives, misspellings, variations in identifier form, and phonetic variations to find identities and paint a broader and more accurate picture.

Resolution

A KYC solution that is capable of drilling down not only on individual attributes but also the relationships between them, can better "learn" and understand the data in the repositories. The ideal solution should then dynamically apply risk weightings to the attributes to come to a resolution on the validity of the identity. This intelligent risk analysis approach provides the business with an accurate assessment on whether that identity is valid.

The importance of advanced analytics in the ideal KYC solution cannot be understated. It provides organizations with greater precision in detecting authentic identities and deflecting identity fraud attempts—automatically. The gains that FIs and other organizations will experience with 90%+ auto-approval rates will turn the KYC process from a check-box compliance solution into a growth-focused, revenue-generating endeavor.

Requirement 2: Intelligent, Automated Global Watchlist Screening

The risk of inadvertently doing business with criminals and enabling money laundering has led many organizations to experience the sting of lost revenue and regulatory fines—not to mention the long-term impact it has on an organization's brand reputation.

As part of the U.S. Patriot Act's Customer Due Diligence (CDD) Rule, requirements for anti-money laundering were placed on FIs to mitigate this risk by conducting ongoing due diligence to understand the nature and purpose of customer relationships to develop a customer risk profile.

Adopting a KYC watchlist screening program also allows organizations to address similar requirements from various regulating bodies, such as the FDIC Bank Secrecy Act and Anti-Money Laundering Act and FinCEN KYC requirements, as well as reduces the risk of OFAC enforcement actions.

In reality, putting this requirement into action has FIs conducting screening of customers against a long and growing set of watchlists. Think tedious, manual review against a company's customer accounts and daily transactions. For a typical bank conducting these KYC watchlist screenings, 75%-85% of the daily alerts that they must manage and remediate are false positives.

In contrast, the ideal KYC solution will use automation to accelerate the screening process and reduce false positives.

BUSINESS *ISSUE*

Legacy Watchlist Screening Solutions Are Manual & Prone to False Positives

BUSINESS *VALUE*

Increases Screening Accurancy and Efficiency to Confidently Assess Risk

WATCHLIST SCREENING RECOMMENDATIONS

With expanding watchlists combined with transaction and customer growth, organizations need a KYC solution with global watchlist matching technology that scales to automatically address the search requirements and eliminates the challenges of manual reviews and false positives.[1]

When evaluating KYC solutions, look for the following watchlist screening capabilities:

- Broad integration with worldwide watchlists, including the 1,100+ sanctions and enforcement lists, 6,000 politically exposed persons (PEP) lists, and adverse media screening lists
- Advanced search capabilities that make it easy to filter search queries and drill into data sources, countries, and other criteria
- Smart matching technology with techniques such as equivalent and phonetic name matching and options for exact or fuzzy name and date of birth matches

Requirement 3: Continual Watchlist Monitoring

To effectively prevent money laundering and financial crime, there are many worldwide KYC-focused regulations that require watchlist screening, and, generally, they require the process to be ongoing.

Specifically, the CDD Rule requires FIs to "conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."

Putting this rule into practice has created challenges for organizations like FIs, and the pragmatic results of truly knowing the current risk profile of an FIs customer base have, largely, been ineffective.

Conducting annual—or even quarterly—audits on an organization's customer accounts against current watchlists is not only a laborious effort, it's immediately stale and out of date the moment the audit is done. This manual approach means businesses can only reasonably check against a portion of watchlists and involves more complexity when attempting to answer the question, "Do my customers currently present a risk?"

CONTINUAL WATCHLIST MONITORING RECOMMENDATIONS

Instead of manual customer base audits for risk, businesses should seek a KYC solution that will continually audit the organization's customer base against the current and broad set of worldwide watchlists.

BUSINESS *ISSUE*

Maintaining an Accurate Status on Customer Risk Is Time Consuming and Ineffective

A KYC solution that proactively and consistently monitors watchlists against an organization's current accounts and customer list will provide the most accurate measure of their customers' present risk profile. This approach empowers institutions to immediately act on any new customer risks so that they can mitigate any potential financial loss or damage to the corporate brand.

BUSINESS *VALUE*

Continual Watchlist Monitoring Effectively Provides a Current Assessment of Customer Risk

[1]The Global Treasurer. False positives: a growing headache. October 2015.

Building on the watchlist screening requirements, businesses should look for the following continual watchlist monitoring capabilities when evaluating KYC solutions:

- Allows FI to import current customer accounts into a "customer monitoring list" to create a complete customer base to monitor
- Following an initial screen, adds identity to FI's "customer monitoring list" to automatically maintain a current list of customers
- Consistently query global watchlists daily, at minimum, and sends alerts to designated personnel when a customer's status changes

Socure's Next-Generation Approach to KYC

Socure's mission is to be the single source of trusted identity for every business-to-consumer transaction, eliminating identity fraud while fueling growth. Socure's holistic solution for identity management encompasses intelligent KYC, real-time identity fraud risk scores, proactive watchlist monitoring, and analytics-based document verification that enables organizations to streamline identity management accurately and effectively.

Socure's ID+ KYC uses advanced analytics coupled with broad data sources to deliver the highest identity match accuracy with over 90% auto-approval rates, and detailed risk and reason codes for every identity element to provide businesses with actionable intelligence.

With ID+ Global Watchlist Screening, Socure enables organizations to automate the screening process by searching identities against a wide range of sanctions and enforcement lists. Applying smart matching technology, organizations will gain more accurate results that improve customer experience and eliminate the operational overhead. When combined with Socure's proactive watchlist monitoring, businesses can also continuously and accurately answer the question, "Do my customers currently present a risk?"

Conclusion

If there's one thing organizations can count on, it's that perpetrators will continue to advance their identity fraud techniques for financial gain. To mitigate this risk, businesses who conduct digital transactions need a KYC solution that provides a strong foundation of advanced analytics to identify and thwart these attempts accurately and efficiently.

In the pursuit of the ideal KYC solution, organizations should use the three requirements outlined in this paper to vet, select, and ensure their new identity verification solution can effectively position their business for success—now, and for years to come.

Learn More

Boost your top-line revenue growth and increase auto-acceptance rates with Socure's Intelligent KYC solution. To learn more, contact us at **sales@socure.com** and **schedule your demo** today.

Socure

How Highmark Health uses AI to root out fraud

Highmark Health's CCO shares how AI saved the firm hundreds of millions of dollars in finding fraud. **Jaclyn Jaeger** explores.

Tens of billions of healthcare dollars are lost to fraud, waste, and abuse each year. For compliance officers and internal auditors in the healthcare space, examining a sea of data to spot red flags is a labor-intensive process, prone to human error, not to mention a very reactive process—parsing through fraudulent medical claims after they've been paid. Among forward-thinking healthcare organizations, however, Artificial Intelligence (AI) is changing all that—and with some very lucrative results.

Fellow chief compliance officers and chief audit executives need look no further than Highmark Health as a prime example. A national health and wellness group, Highmark Health uniquely serves the dual role of being both a healthcare provider and a healthcare payor, with a consolidated

"One of the goals I set out for the team is, how do we start to do things bigger, better, and faster? And how can we put that into the work that we do every day? How do we utilize our staff to the highest potential?"

Melissa Anderson, EVP, chief auditor and compliance officer, Highmark Health

revenue of $18 billion as of year-end 2019. With 35,000 employees across the United States, Highmark Health's network of affiliates and subsidiaries collectively provides everything from healthcare to dental care, healthcare insurance, reinsurance, and technology-based solutions for the healthcare space.

Since at least 2012, Highmark Health has realized hundreds of millions of dollars in savings through using highly sophisticated data analytic tools to improve efficiencies and to help detect fraud, waste, and abuse in all its forms. "One of the goals I set out for the team is, how do we start to do things bigger, better, and faster? And how can we put that into the work that we do every day? How do we utilize our staff to the highest potential?" says Melissa Anderson, executive vice president, chief auditor and compliance officer at Highmark Health.

The idea was that by taking some of the more tactical work that staff members were doing and, instead, having algorithm and systems to process data, staff is effectively freed up to think more strategically. "So, it was really about how to do more with less, but yet gain more precision as part of the process. It was a win-win," Anderson says of Highmark Health's decision to begin leveraging Artificial Intelligence.

One significant benefit afforded by AI capabilities is being able to detect indicators of fraudulent activity much sooner than in the past—such as spotting trends and unusual activity in claims closer to the time they're paid, or even before they're paid, with the goal being to stop would-be criminals before money goes out the door as opposed to after the fact. AI also allows for continual analysis of healthcare claim patterns that may be indicative of red flags, such as high-claim utilization in a given day or provider billings that greatly exceed normal billing patterns generated by comparable providers.

"For us, it's about how do we find these issues before they become large issues and try to mitigate them as quickly as possible?" says Kurt Spear, vice president of Highmark's Financial Investigations and Provider Review (FIPR) unit, which is tasked with detecting and investigating all alleged cases of healthcare fraud, waste, and abuse in all lines of its business that impact the organization financially. Fraud referrals can come from both internal and external sources—members, employees, and providers, for example.

Aside from wanting to detect fraudulent activity more quickly, Spear says another thing Highmark Health wanted, and has gained, through using AI software is "reasoning" capabilities—in other words, machine-learning software that takes the data and knowledge of forensic investigators and other human analysts and embeds that knowledge into the AI capabilities, essentially turning them into mathematical algorithms processed by computers. And, unlike people, the memory and processing capabilities afforded by AI is nearly limitless.

From an operational standpoint, Highmark has what it calls the company's "Payment Integrity" program, under which it deployed 28 unique initiatives to help ensure claims' payment accuracy, 15 of which are embedded within the FIPR unit and specific to fraud, waste, and abuse initiatives. Healthcare claims go through rigorous reviews, using a combination of automated AI algorithms and a manual assessment process. "It really helps us to have a targeted audited approach, so that we're looking at all the right places based on the output that we can get much quicker," Anderson says.

Both Anderson and Spear stress that AI complements human analysis and is not a replacement for it. "It's a combination of people, process, and technology that enable us to put a program together that is very effective," Anderson says.

The FIPR unit, for example, utilizes an internal team that includes registered nurses, investigators, accountants, former law enforcement agents, clinical coders, and programmers, complemented by an array of vendors, to complete its objectives.

As part of its work, the team performs audits to identify unusual claims, coding reviews, and investigations that assess the appropriateness of provider payments. "It takes a lot of different individuals and entities across the enterprise, as well as outside the enterprise, to have a solid an-

ti-fraud program," Spear says.

Savings realized

By using AI, Highmark Health has been able to realize hundreds of millions of dollars in savings—$850 million in the last five years alone, to be exact—associated with the prevention of waste, fraud, and abuse. According to data provided by Highmark, the company has realized savings of $120 million in 2015; $148 million in 2016; $183 million in 2017; $145 million in 2018; and $260 million in 2019, which included prevented losses, recovered money, and policy savings.

Anderson and Spear don't intend for Highmark Health's efforts to remain in a vacuum. In fact, its information-sharing approach has earned it national accolades. In 2019, the National Health Care Anti-Fraud Association honored Highmark's FIPR department with the "Special Investigation Resource and Intelligence System Investigation of the Year" award.

The award resulted from an investigation involving a specialty pharmacy that was supplying excessive amounts of hemophilia-factor medications to patients. To drive up its reimbursement, the pharmacy and individuals set up a sham employer group that "employed" the recruited hemophiliacs.

Within the first several months, the sham employer group (or pharmacy) submitted claims seeking reimbursement for millions of dollars, with $4.5 million in claims in just the first several weeks.

Ultimately, the scheme was shut down. Spear explains the award to Highmark resulted from information it shared with peers across the United States to help stop similar schemes from happening to them.

Anderson says learning from others in the industry is very important. "Don't reinvent the wheel," she says. "Learn from experts in the industry. Don't be afraid to reach out to them. That's how we've learned a lot about the programs that we have put into place."

Spear explains that it's also important to not be afraid of change and to embrace it. Fraud schemes today are a lot more complex and more organized than they've ever been in the past, which really forces the hand of healthcare organizations to be as adaptable as the organized criminals themselves.

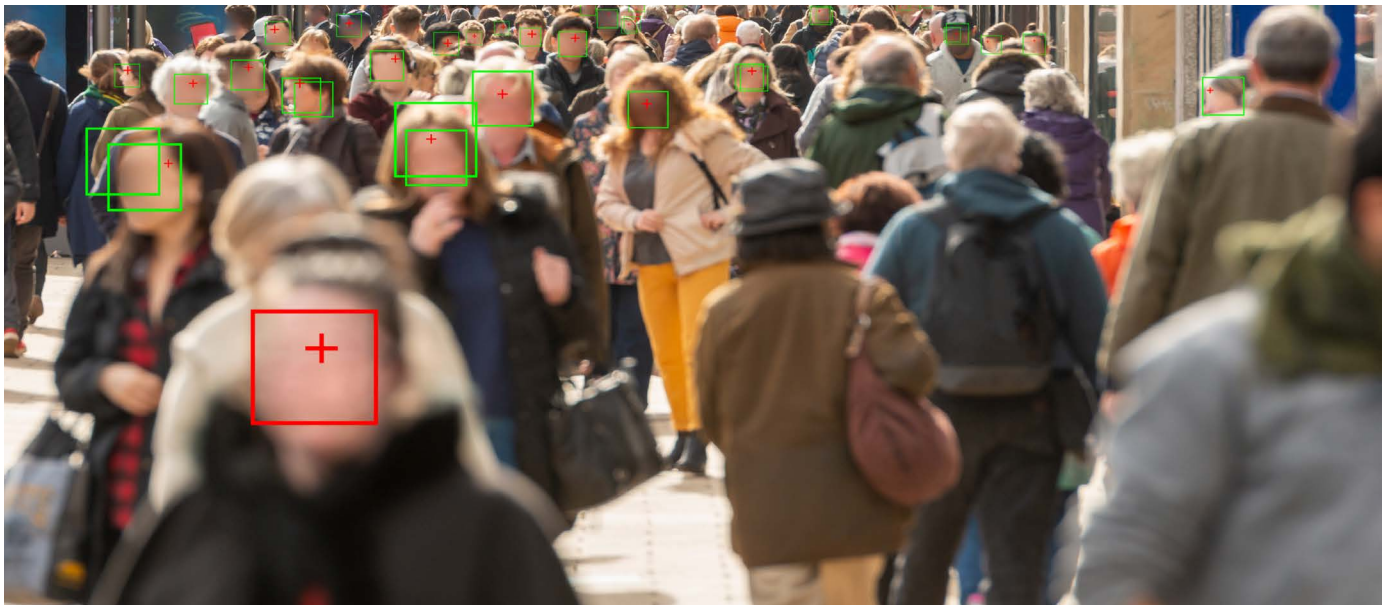
The increase and proliferation of fraud activity during the pandemic is a timely example and makes using AI to identify fraud, waste, and abuse more important than ever before. "We are enhancing our AI software to be able to hone-in on suspect behavior specific to COVID-19 schemes," Spear says.

Suspect behaviors may include impossible day scenarios whereby providers bill more telehealth services than could have been rendered in a 24-hour period and large volumes of coronavirus tests for the same patient, for example. "At this time, it's still too early to report on results from these efforts," he says. ■

Types of fraud investigations

- **Provider fraud** (billing for services not provided, billing for a more costly service than one performed, billing each stage of procedure as if it was separate, billing for a provider's services outside of the provider's practice, issuing kickbacks, billing for non-covered services or making a false diagnosis, setting up phony clinics to generate false claims)
- **Subscriber fraud** (allowing someone else to use your insurance card or your spouse's card, using an insurance card that has been canceled, placing ineligible dependents on your plan, asking the provider to falsify a report to receive a non-covered procedure, asking a provider to waive a copayment, forging receipts from a provider to get reimbursement from the insurer)
- **Pharmacy fraud** (using multiple pharmacies to get more drugs, using different prescribing providers, submitting false prescriptions, altering pharmacy receipts)
- Employee fraud (misrepresenting information on an enrollment application, placing ineligible dependents on your plan, accessing employee data or PHI without authorization)
- **Group fraud** (ghost employees or non-existent employees, subscribers that aren't employees, part-time employees, ineligible dependents)

Source: Highmark



Facial recognition technology comes under attack

More are denouncing facial recognition technology, as its implications for abuse and racism surface. **Aaron Nicodemus** has more.

Facial recognition technology, under assault for alleged biases and misuse by law enforcement, could be facing a moment of reckoning.

IBM announced in June it has discontinued research and sale of its general facial recognition tools, telling Congress it believes the technology should not be used "for mass surveillance, racial profiling, violations of basic human rights and freedoms."

"IBM no longer offers general purpose IBM facial recognition or analysis software," wrote CEO Arvind Krishna in a letter posted on the firm's website. "We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies." Krishna wrote all Artificial Intelligence (AI) should be tested for bias, "particularity when used in law enforcement, and that such bias testing is audited and reported."

In the place of facial recognition technology, IBM recommends national policy "should encourage and advance uses of technology that bring greater transparency and accountability to policing, such as body cameras and modern data analytics techniques."

It will be interesting to see if other large players in the facial recognition space—Apple, Facebook, and Google, although there are dozens more—will follow IBM's lead and cast the technology aside.

More likely, IBM's announcement may cause tech companies—which have been struggling to find the right corporate tone in response to Black Lives Matter rallies—to completely rethink the way facial recognition technology works and how it should be used.

In early June, Amazon announced a one-year ban on police use of Rekognition, its facial recognition software. "We've advocated that governments should put in place stronger

"We've advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology, and in recent days, Congress appears ready to take on this challenge ... We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested."

Amazon blog post

regulations to govern the ethical use of facial recognition technology, and in recent days, Congress appears ready to take on this challenge," Amazon said in a blog post. "We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested."

A day later, Microsoft announced that it also won't sell facial recognition software to police until a federal law is passed.

IBM, Amazon, and Microsoft's moves come as facial recognition tech has come under fire for racial biases that have been found to be baked into its algorithms.

One study by the National Institute of Standards and Technology found 139 facial recognition algorithms studied misidentified African American and Asian faces at a rate 10 to 100 times greater than Caucasian faces. A 2018 study on facial recognition software by researchers Joy Buolamwini and Timnit Gebru revealed the extent to which many such systems (including IBM's) were biased. "This work and the pair's subsequent studies led to mainstream criticism of these algorithms and ongoing attempts to rectify bias," according to a story in The Verge.

Privacy concerns are tantamount as well. Fears of the Chinese government's wide-ranging use of the technology to monitor its citizens has been highlighted by publications including The Atlantic. But western governments and police have been using facial recognition to find suspects and monitor citizens, using technology that is almost completely unregulated.

And there has been blowback. Clearview AI, a company whose business model is selling access to law enforcement agencies for its facial recognition database of over 3 billion images scraped from social media, has been issued numerous cease and desist orders and is at the center of a number of privacy lawsuits. Facebook in January announced it would pay $550 million to settle a class-action lawsuit over its unlawful use of facial recognition technology.

So criticism of facial recognition technology is not new. What is new is the impetus for IBM's decision, which has to be viewed through the lens of the moment. It is a corporate reaction to the Black Lives Matter movement that has been re-energized following the death of African American man George Floyd at the hands of police in Minneapolis.

What may follow is a complete rethinking of how facial recognition technology should be used by law enforcement. Recently, the Black Lives Matter movement and protestors marching throughout the country have demanded that police be "defunded." That doesn't necessarily mean that police departments should be disbanded, but rather reorganized and streamlined. The argument goes that responsibilities that have for years defaulted as police matters would be more appropriately handled by other governmental and community organizations better positioned to handle them without bias or violence.

Why are police in charge of traffic enforcement and parking regulations? Why are officers assigned to public schools? Why are they paid to provide security at construction sites and large private events? Why are police departments tasked with enforcing public health rules during the coronavirus pandemic?

If it is true that facial recognition technology is being misused by a police system built on racial profiling and targeted brutality, then perhaps the technology itself should also be overhauled. If racial biases are baked into facial recognition algorithms, then the algorithms need to be discarded and rebuilt from scratch as something completely new.

It's easier to discard algorithms than it is to eviscerate police department budgets and lay off police officers in the name of reforming a rotten system. Perhaps new guidelines and guardrails placed on facial recognition technology—to make the technology more accurate and less biased—could be applied to the much more difficult task of reforming the police.

Said another way, if government establishes regulations for the proper use of facial recognition software to squeeze out bias and racial profiling, could it not use those same principles to reform the country's police departments? The two reform efforts may not be as different as they first appear. ■

What regulators want to know about KYC technology

Hear from experts on how to begin the process of onboarding KYC technology to regulators. **Aaron Nicodemus** reports.

So, your organization has decided to embark on an update of its legacy Know Your Customer (KYC) system. You've completed your internal diligence and collected the various internal signoffs and approvals. But now it's time to present your new KYC technology solution to your regulator.

No regulator will "approve" or endorse a vendor solution—instead it will review the new system to ensure it is commensurate with the risk profile of the institution and that it complies with regulatory requirements as well as the institution's internal policies and procedures.

Using Artificial Intelligence (AI) and robotic process automation, the new technology can often achieve higher auto-approvals and reduce false positives compared to a legacy system. In addition, KYC technology can mine billions of publicly available data points to provide a complete applicant profile and use facial recognition software to compare an applicant's submitted mobile phone selfie to an identification photo.

Financial institutions have been among the most eager first adopters of ever-evolving KYC technology, applying tools to improve their ability to screen and verify loan applicants. But new tech can serve other industries: Casinos and online gaming platforms can use KYC tech to screen customers who might appear on sanctions or other watchlists, while online marketplaces and social networks use it to weed out fraudulent vendors and scam artists. Really, any business seeking to verify the identity of a customer might find some value in applying KYC tech to screen low-risk applications so its investigations team can focus its attention on the smaller, high-risk slice of the pie.

Begin at the beginning

According to Jason Somrak, chief of product for AML & Advanced Analytics at Oracle Financial Crime and Compliance Management, the process of onboarding your KYC tech with regulators will take between 18 months and two years. The division works with banks to use advanced tech to fight financial crime and modernize risk and compliance operations.

"People won't be penalized for trying new things," he says. "But I think regulators will expect that firms won't throw everything away and start fresh." There will be a transition, where regulators will want to see that the new KYC technology provides better results than the firm's legacy system.

"Regulators want to see your work; they want to see the long division and know that the bank understands how the system technology works—why it flags or alerts, why/how are the decisions being made," says Kimberly Hebb, who spent 20 years as a commissioned bank examiner with the Office of the Comptroller of the Currency (OCC) and is now chief risk officer of BillGO, a bill payment provider. "Many FinTech companies think that their technology is special and needs to be in a 'black box' system and don't want to discuss their processes."

Regulators want to hear from the financial institution that is planning to utilize new KYC technology—not the vendor, she says. They also want to understand the impetus driving the move to a new KYC solution. Is the proposal to use new KYC technology part of a planned strategy for growth or a reaction to a deficiency, violation, or past pattern or practice?

Whichever KYC program your institution uses, it "should be commensurate with the risk profile of that institution," Hebb notes. "It's not that regulators don't appreciate the need; there is still the expectation that the bank knows its customer base and provides internal controls." They also want to know that the new tool has been customized for the financial institution in question, that the results are being actively monitored, and that the processes are being updated as needed.

Regulators 'leaning in'

With KYC tech becoming a focus of many industries, several regulators, including the OCC and the Commodities Futures Trading Commission (CFTC), are having to adapt regulations.

"We are seeing regulators lean in, even though they're not recommending particular tools or vendors. We are seeing a very strong adaptation of complicated analytics," says Johnny Ayers, co-founder and senior vice president of Socure, a FinTech company that provides digital identity verification and KYC solutions through AI, advanced logic, and machine learning.

"Regulators have gotten more comfortable with new KYC technologies, including machine learning (ML) and robotic automation (RA), but they require clear understanding of the model used. While stratifying data may be an easier model to verify, the large number of alerts can only be tackled effectively using ML and RA techniques," adds Piotr Jastrzebski, director of technology product management for the Financial Crimes Control group at Wolters Kluwer, a risk management and regulatory compliance consultant to U.S. banks and credit unions.

In 2017, the OCC established its Office of Innovation, which was tasked with helping financial institutions large and small to sample FinTech solutions. The agency's support of "responsible innovation" attempts to balance innovation with prudent risk management.

The agency formed partnerships between financial institutions and FinTech vendors through an Innovation Pilot Program "to support the testing of innovative products, services, and processes that could significantly benefit consumers, businesses, and communities, including those that promote financial inclusion," OCC Chief Innovation Officer Beth Knickerbocker said in testimony before a House committee in 2019.

Similarly, LabCFTC helps "promote responsible FinTech innovation to improve the quality, resiliency, and competitiveness of our markets" as well as accelerating "CFTC engagement with FinTech and RegTech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently." The Consumer Financial Protection Bureau also has an innovation program that attempts to "promote innovation, competition, and consumer access within financial services."

Regulators in other countries have similarly embraced KYC technology. In 2019, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) announced it would allow for the use of digital documents to authenticate an individual's identity. This new policy allows individuals being vetted to supply their financial institution to scan their "government-issued photo identification document using the camera on their mobile phone or electronic device." The individual would then be required to take their own photo with their device and submit it to the institution.

But in order to verify the selfie and the photo on the identification match, the bank or credit union must have the technology to "apply facial recognition technology to compare the features of that 'selfie' to the photo on the authentic government-issued photo identification document," FINTRAC noted in its 2019 directive on identifying individuals and corporations.

"The tech demonstrated it was feasible," said Zac Cohen, chief operating officer of Vancouver, Canada-based Trulioo, a FinTech vendor that "delivers trust, privacy, and safety online through scalable and holistic identity verification." KYC tech vendors were able to prove to regulators the technology was accurate and produced verifiable results, he says.

European regulators seeking to sign off on KYC technology at companies that must comply with the General Data Protection Regulation have sought to understand the "context" of its decision making—that is, how an AI tool arrives at its decisions, without focusing on the individual decisions themselves.

Factors such as the urgency of the decision, its impact, and significance might outweigh a data subject's wish to know more about the process, suggesting a "one size fits all" approach to explaining AI-generated results is unworkable, according to U.K. data regulator the Information Commissioner's Office. ■

Socure

Intelligent KYC and Watchlist Screening with Monitoring

Regulatory compliance driven by more data, advanced logic and actionable insights

Accept More Customers Without Friction

With unparalleled data coverage and proprietary search analytics, Socure ID+ KYC and Global Watchlist Screening with Monitoring guarantees unmatched auto-acceptance rates for mainstream and underbanked consumers, as well as continuous compliance monitoring in real-time. Delivered via a single RESTful, modular API, you benefit from faster implementation.

90%+
Auto-Approval Rates

65%+
Reduction in Manual Reviews

Contact **sales@socure.com** to learn more about these services and how Socure can transform your business.

Benefits

- Enroll more new customers with higher auto-acceptance rates while delivering the frictionless onboarding experience that today's consumers expect.
- Make sense of billions of consumer records and complex datasets using proprietary identity resolution analytics.
- Gain greater insight and actionable intelligence with simple yet detailed reason codes.
- Mitigate risk with continuous compliance monitoring in real time.
- Boost your top-line revenue growth and digitally revolutionize KYC compliance and watchlist monitoring for the future.