AML/KYC TRACKER

Bridging the **Security Gap** To Win Customers' Trust

TABLE OF CONTENTS

AML/KYC TRACKER

PYMNTS.com Trulioo

ACKNOWLEDGMENT

The AML/KYC Tracker was done in collaboration with Trulioo, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

Companies of all types must either invest in anti-money laundering (AML) and know your customer (KYC) specialist teams or invest in anti-fraud technology. Going without is not an option, unless firms want to risk steep regulator fines or customer flight when something inevitably goes wrong.

Companies of all types must either invest in anti-money laundering (AML) and know your customer (KYC) specialist teams or invest in anti-fraud technology. Going without is not an option, unless firms want to risk steep regulator fines or customer flight when something inevitably goes wrong.

A recent survey of 143 decision-makers from financial institutions (FI), investment firms, asset management and insurance companies in Canada and the U.S. found that many are choosing to scale up their defenses, rather than risk running afoul of regulations or failing to stop crime and paying heavily for such lapses. Surveyed companies used anywhere from no technology to four or more different tools to support their compliance efforts.

Larger companies that deployed two or three technologies tended to spend approximately 54 percent of their overall compliance investments on full-time staff, while those that deployed four technologies or more only directed about 48 percent of their spending to compliance employees, the study reported. Employee costs typically tend to rise faster in this budget area than in others, making reductions in staffing a long-term cost saver.

The survey also found that smaller companies were less likely than larger ones to report

investing in and using AML technologies, however, implying that these firms are missing out on such tools and savings. Reports from 2018 note that smaller companies, which have fewer financial resources, may struggle to come up with the funds required for such offerings. A 2019 study underscored this point, discovering that even though the AML software market is slated to grow 15.25 percent from 2019 to 2026, the technologies' high costs prevent the market from growing more quickly.

This month's AML/KYC Tracker examines the latest fraud fighting challenges and efforts to bolster security and compliance efforts.

AROUND THE AML/KYC WORLD

The State Bank of Pakistan (SBP) recently fined four Pakistani banks for violations, showing that not all FIs manage their compliance obligations well. Bank Al-Habi, Bank of Punjab, JS Bank Limited and Soneri Bank Limited were forced to pay penalties ranging from approximately $180,000 USD to $770,000 USD, and some were advised to change their AML, KYC and other procedures.

Other firms are also calling out cases of potential misconduct. Legal marijuana company Herban Industries recently brought a suit against cannabis delivery platform Eaze Technologies. The former alleges that the latter persuaded FIs and card companies to process its transactions by pretending to sell items other than cannabis. The suit claims that Eaze directed customer payments through off-shore shell companies so that marijuana purchases would appear as sales of items such as dog toys. This kind of allegation demonstrates the need for robust know your business (KYB) practices, Zac Cohen, general manager of global identification provider Trulioo, said in a recent interview with PYMNTS. He added that KYB is tricky because of its complex challenges and the above-board reasons companies may have some off-shore operations or separate entities.

Such regulations can be conquered through collaboration, however, and six Nordic FIs are partnering to do just that. The banks are working to create standardized KYC processes as well as develop a platform for collecting and managing customer data. The to-be-launched platform will provide KYC services to medium-sized and large Nordic companies.

For more on these stories and other notable AML/KYC headlines, check out the Tracker's News and Trends section (p. 11).

HOW MOBILE FINANCIAL STARTUPS CAN BRIDGE THE SECURITY GAP

Fledgling financial companies do not have established reputations that they can leverage to persuade customers to trust them with their sensitive details, presenting a challenge for startups like payments and money management app STACK, which provides services such as

budget management and spending accounts. In this month's Feature Story (p. 7), STACK's chief operating officer, Nicolas Dinh, explained how startups can forge partnerships with established payments players and deploy a variety of fraud-fighting tools to stay ahead of synthetic ID tricks and other attacks to protect customers, assuring them that even young companies can keep them safe.

DEEP DIVE: HOW FINTECHS, FIS CAN ARM UP AGAINST FRAUD

Governments need to keep residents safe from crime and terrorist activities, and countries' regulators support these efforts by issuing and enforcing rules meant to stop money laundering, tax evasion and terrorist funding. FinTechs and FIs that fail to comply have been hit hard with fines and even license revocations.

Enacting strong AML procedures can be challenging, however, as it requires companies to sort through and gather insights from vast amounts of data. This month's Deep Dive (p. 17) examines the kinds of fraud threats and regulatory obligations that financial companies face, as well as the extent to which solutions like artificial intelligence (AI)-powered software can help make compliance easier.

EXECUTIVE INSIGHT

What are some of the AML and KYC challenges that legacy banks grapple with when they expand into the digital banking space? What tools and techniques can help them stay compliant?

"The main challenge in adapting AML and KYC procedures to digital banking services is finding the right balance of compliance and convenience. Online and mobile customers expect onboarding to be quick and easy, but banks still need to meet rigorous verification standards.

Procuring, integrating, and testing new tools with an existing [technology] stack is also difficult, especially when a legacy bank has a complex organizational structure. Multiple regulations and jurisdictional requirements across borders add to the challenge.

For faster onboarding, banks can use automated API-based tools to verify identities, ID documents, and businesses and to screen against international watch lists. The entire process occurs remotely, so customers don't have to visit a branch in person.

Legacy banks can gain significant benefits from accessing a global marketplace of identity data and solutions. For each use case and region, businesses can leverage the best data partner and service for increased accuracy, all through a single verification provider.

While compliance challenges are real, digital banking represents an exciting opportunity for established firms. By partnering with the right RegTech innovators, banks can find new efficiencies and expand their offerings to a new generation of banking clients."

ZAC COHEN

general manager at Trulioo

FIVE FAST FACTS

5

$1.4M

Average annual AML compliance spending for Canadian firms with less than $10 billion USD in total assets

10,000

Number of images of Binance KYC data allegedly accessed by a cybercriminal

$770K

Amount Soneri Bank Limited was fined for AML/KYC issues and other violations

15.25%

Projected CAGR of the global AML software market from 2019 to 2026

2.6M

Number of customers whose KYC data was exposed in Jana Bank's unprotected database

Bridging the **Security Gap** To Win Customers' Trust

Fraudsters have been increasingly focused on mobile services, with one-third of all fraud attacks worldwide reportedly targeting mobile during the first half of 2018 — a 24 percent year-over-year (YoY) increase. Consumers have reason to be concerned, especially when choosing which mobile services to trust with their personal finances, and many may resultantly prefer to use apps from major financial companies with long-established reputations over those from fledgling startups.

Such caution is a high bar that app-based startups must overcome, but how can consumers be persuaded to take a chance on these new companies? Chief Operating Officer Nicolas Dinh of year-old Canadian financial startup STACK recently spoke to PYMNTS about the key forms of fraud nascent mobile financial services firms face and how companies can leverage security technologies and partnerships to gain customer trust. STACK's mobile app provides services such as budget management and spending accounts.

"Startups like STACK are at a disadvantage by default, because we lack the reputational track records of more established institutions and brands," Dinh said.

FIGHTING FRAUD VISIBLY AND INVISIBLY

Financial service providers must run a tight ship when offering mobile services, and various techniques can help keep them secure. Dinh noted that they must be especially wary of the most prevalent attacks, such as fraudsters seeking to take over existing customer accounts or onboard using synthetic IDs — falsified documents created by altering or cobbling together pieces of legitimate IDs. Firms looking to keep legitimate users secure must take many steps that may seem minor when looked at individually, but combine to offer robust protection, he said.

STACK implements various behind-the-scenes procedures, such as tokenization, identity verification and automated fraud detection, and also provides customer-facing options that give users a sense of control and transparency. These tools include instant transaction notifications as well as capabilities for suspending or freezing cards and generating and using virtual cards when making online payments for merchants with which the customers are not familiar. Virtual cards are beneficial because they can be reissued faster than plastic cards in the event of a merchant's data breach.

"More customer-facing capabilities give [users] peace of mind — [such as] having the ability at any point in time to shut down a card," Dinh said. "Consumers in general want to be empowered … this is starting to become table stakes."

Communication is also critical, and Dinh recommended providing in-app, chat-based support as well as publishing notifications to keep customers informed about matters such as maintenance outages.

PARTNERING WITH ESTABLISHED PLAYERS

Startups can also make customers feel secure by piggybacking on well-known financial companies' reputations. STACK works with major payment networks that are able to provide safeguards like zero liability protection, for example, ensuring that cardholders are not on the hook for any fraudulent charges made with their cards that the issuer or cardholders discover and report.

"To bridge the [reputation] gap initially, [a startup should] partner directly with institutions such as a regulated bank sponsor to help build that initial level of trust with consumers," Dinh advised.

This approach remains important as the company considers expanding internationally. Going global requires forming close partnerships with local bank sponsors and regulators to ensure compliance. Dinh added that global technology providers are also important as they can offer insight and support to accelerate and simplify compliance efforts in new markets.

Partnerships with players like Trulioo are helping STACK offer quicker onboarding. Applicants who present low risk for money laundering or fraud are typically processed within two minutes.

FACING FUTURE FRAUD

Synthetic IDs are a major threat in today's digital financial services space, but more advanced attacks are sure to emerge as technology evolves. Companies have deployed liveness checks and other robust measures to help verify identities and combat fraud, and they will have to continue to upgrade their defenses to stay ahead as scams like deepfakes become more prominent, Dinh predicted. Hackers can use these highly realistic, falsified videos to challenge today's liveness tests thus necessitating that companies keep working to improve their toolkits to detect and thwart this and other new types of fraud. Dinh expects to see increased investments in neural networks, sets of algorithms that mimic the human brain to detect patterns in data, for behavioral fingerprinting — assessing devices' web browsing and navigating behavior for patterns that deviate from the norm and might indicate illicit takeovers.

Fraud in mobile services is a continuously developing issue that deeply affects consumers and businesses. Startups cannot afford to fall behind

on security measures as they work to build their user bases. Robust, cutting-edge security methods — whether through collaborations with major partners, careful processing procedures or powerful technologies — are vital to young companies seeking to earn trust and establish reputations for safeguarding their customers.

UNDER THE HOOD

How do you ensure secure onboarding?

"One of the biggest concerns right now for us is the use of synthetic IDs to gain access to accounts. Synthetic IDs and fraudulent accounts … expose us to fraudulent loans and transactions. To mitigate all [of] this, … we enforce validation of all application information against credit file information that's stored with the credit bureaus as part of the onboarding process. We [also] use a combination of fraud protection technology as well as in-house fraud analytics, which may require additional verification of the application. As part of step-up verification of the customer, we prompt the applicant to submit documents like bank statements [or] utility bills … that are authenticated in an automated fashion. … As a fallback, an actual agent verifies the documentation sent [in with] the application.

You can create a STACK account within two minutes … when the risk associated with the application is low. When we do detect any increased fraud risk for an application, the process becomes more convoluted and we ask [the user to submit] additional documents … for verification. To streamline that process, we leverage … screen scraping technology and application programming interfaces (APIs) to automatically extract any documentation from the customer's legacy bank account, for example, to reduce the friction of that onboarding experience. When it comes down to it, we believe we need to strike a balance between frictionless experiences [and] exposing us to fraud and AML risks. When any additional verification is warranted, the process has to become a bit more onerous to deter fraudsters. However, our goal is to continually evaluate and assess … emerging technologies that can be incorporated into our product to improve the consumer experience."

Nicolas Dinh,

chief operating officer, STACK

NEWS & TRENDS

STRENGTHENING KYB AND KYC

HERBAN INDUSTRIES V. EAZE TECHNOLOGIES SUIT REFLECTS WIDER KYB CHALLENGES, NEEDS

Legal marijuana company Herban Industries recently sued cannabis delivery platform Eaze Technologies, accusing the latter of gaining an unfair competitive advantage by scheming to trick financial services providers into helping it. FIs are typically leery of supporting cannabis commerce because the substance is illegal on the federal level. The lawsuit states that Eaze tricked FIs and card companies into processing marijuana transactions by directing payments through several off-shore shell companies, disguising marijuana sales as sales of dog toys and face creams, among other items.

FIs looking to detect and fight this kind of fraud must have strong KYB procedures. Zac Cohen, Trulioo's general manager, recently told PYMNTS that such processes are challenging given that many operations have legitimate reasons to establish separate entities or perform some operations abroad. FIs must therefore apply strict due diligence measures to merchants' account opening applications. Measures should verify and examine applicants' client relationships, organizational structures and more to ensure that they are legitimate and satisfy regulatory requirements. Fraud monitoring technologies and public-private data sharing partnerships can help support these efforts, Cohen said.

IDEX ENDS ANONYMITY POLICY, ADOPTS KYC MEASURES FOR ALL USERS

Ethereum-based cryptocurrency exchange IDEX officially ended a policy under which users could remain anonymous while trading up to $5,000. IDEX first announced the requirements in November 2018 before enacting the policy on July 24. The exchange now has security and AML procedures that require users to create accounts

and undergo KYC, among other measures. Existing users must — as of August 23 — pass Tier 1 KYC verification to trade and undergo more robust measures to trade or withdraw more than $5,000 per day. Additional measures could include passport scans and selfies.

Some cryptocurrency advocates spoke out against IDEX's new security approach, asserting that identity verification procedures are contrary to the sector's privacy goals. CEO Alex Wearn asserted that the impending KYC requirements had "little to no impact" on user volume.

BREACHES AND NONCOMPLIANCE

RESEARCHER DISCOVERS UNPROTECTED JANA BANK KYC DATABASE

A researcher recently discovered that a Jana Bank database of 2.6 million customers' sensitive information was left unprotected from cybercriminals. Jeremiah Fowler — a senior security researcher and journalist at cybersecurity news and consulting services provider Security Discovery — reported that the database of customer emails and usernames, as well as details from driver licenses, permanent account number (PAN) cards, passports, voter IDs and more, was publicly accessible to internet users. Anyone could view and change, delete or download the stored details. Fowler immediately informed the bank of the issue, after which it secured the data.

It is not clear whether fraudsters accessed the information during the window in which it was exposed. Details such as IP addresses and storage information could reportedly be used to further penetrate the bank's network.

Jana Bank opened in Bengaluru, India, in 2015 as a small finance bank, providing basic financial services to SMBs and consumers that larger FIs may not serve. Its services focus on micro-industries such as farming, as well as standards like accounts, deposits and SMB lending.

BINANCE REPORTS POTENTIAL KYC DATA LEAK, OUTLINES RESPONSE STEPS

Cryptocurrency exchange Binance announced in a blog post last month that an anonymous individual had demanded the company pay 300 bitcoins in exchange for the individual not posting more than 10,000 photos allegedly depicting Binance KYC data. The individual was uncooperative and began providing the data to media and other public outlets. Binance stated that while the photos resembled those it uses for KYC, they lacked the digital watermarks it adds to all KYC images it processes or otherwise did not match images in the database.

Binance contracted a third-party KYC provider between December 2018 and February 2019 and the crypto exchange noted that some of photos were similar to those that the third-party handled. The former said it would respond to

the potential security issue by contacting any potential victims, advising them on privacy protection, recommending they get new identification documents and offering them lifetime VIP memberships.

STATE BANK OF PAKISTAN FINES FOUR BANKS OVER AML/KYC VIOLATIONS

The State Bank of Pakistan (SBP) recently discovered major KYC concerns, resulting in it imposing penalties on four banks. Bank Al-Habi, Bank of Punjab, JS Bank Limited and Soneri Bank Limited were cited for failure to comply with AML/KYC and other regulations.

Soneri Bank Limited was ordered to pay a fine of Rs 55.483 ($770,000 USD) for violating regulations regarding AML, asset quality, foreign exchange operations and KYC. The FI was also asked to change its AML/KYC and credit risk monitoring practices. The Bank of Punjab was fined Rs 13.072 million ($180,000 USD) for poor AML/KYC practices, foreign exchange operations and unclaimed deposits. Bank Al-Habib Limited was similarly penalized for AML/KYC and foreign exchange operation failures and ordered to update its system and processes as well as send officials to receive new training. It paid a fine of Rs 51.75 million ($714,000 USD). Lastly, JS Bank Limited paid Rs 48.221 million ($665,000 USD) for its AML/KYC violations and was urged to review its relationship accounts — customer accounts that include more services and products beyond basic checking or savings accounts.

ONLINE GAMING AND GAMBLING

ZENGAMING ADOPTS NEW CUSTOMER ONBOARDING VERIFICATION TOOL

Fraud attempts are an increasingly pressing problem in the online gaming space, pushing gaming and eSports social network and products provider Zengaming to implement an offering from customer onboarding technology provider AU10TIX. The former is utilizing the latter to help

it meet KYC requirements and support various identity verification measures, including comparing customers' selfies to the images on their IDs. AU10TIX's offering includes a software development kit (SDK) intended to help clients get higher quality readings of such images for inclusion in their records.

Ofer Friedman, AU10TIX's vice president of marketing, said that the customer onboarding verification solution combats fraud attacks frequently launched in the gaming space, such as bad actors using stolen personal data or counterfeit IDs altered with Photoshop.

AUTOMATION TOOLS AIM TO EASE COMPLIANCE WORK FOR U.K.'S GAMBLING INDUSTRY

The U.K.'s online gambling industry has been evolving its KYC and AML approaches, but it still has a long way to go. Jane Jee and Martin Pashley, CEO and chief commercial officer respectively, of due diligence search platform provider Kompli-Global noted during a recent interview that KYC regulations were largely regarded as burdensome obligations in the gaming industry in 2005. Most eGaming websites only put in the minimum effort required, such as asking their customers to confirm they were of legal age to play without verifying such details, Pashley said.

The U.K.'s regulations have grown, however, with the Gambling Commission now issuing fines for failures to fully comply with verification and security requirements. These developments are particularly important because there is a high risk of money laundering in the space. Jee and Pashley explained that many companies in the gambling industry still regard compliance as costly and time consuming, but (AI)-powered software tools can reduce the burden by providing human employees with high-quality data that reduces their workloads and improves their risk analysis accuracy. Automation can also reduce the number of AML experts that companies must hire, though Jee added that humans will always be necessary to interpret data and make decisions.

BIOMETRIC VERIFICATION

MONEYNETINT ADOPTS BIOMETRICS VERIFICATION TO BOOST KYC PROCESSES

Cross-border money transfer and exchange services provider MoneyNetint recently adopted new tools to help safeguard and verify its corporate clients. The U.K.-based company selected a document and biometric selfie verification solution from provider Onfido to improve KYC processes and reduce the threat of bad actors using fake IDs to onboard. The latter develops solutions that recognize faces and checks them against international watchlists and credit databases. MoneyNetint hopes Onfido's offering will

allow it to quickly onboard users without compromising its system. The solution also uses machine learning (ML) to help stay current as new fraud trends develop.

GOOGLE LEVERAGES FIDO2 STANDARD FOR BIOMETRIC AUTHENTICATION ON ANDROID DEVICES

Keeping customers safe from fraud beyond onboarding requires that companies ensure their login credentials cannot be compromised.

The FIDO Alliance, which focuses on promoting standards for authentication measures that go beyond passwords, is looking for ways that allow customers to prove their identities without relying on knowledge-based information — details that can easily be stolen. The organization recently released FIDO2, a new standard intended to enhance security efforts by advancing biometric authentication measures in place of password-focused ones. The offering was developed in collaboration with the World Wide Web Consortium (W3C), an international group focused on creating standards for the internet.

Google recently announced in a blog post that it had adopted and started using FIDO2, enabling Android device users to log into certain Google web services and apps using biometrics or screen lock patterns rather than passwords. This functionality is available on devices running Android 7.0 or later versions of the operating system and marks the first time Google is providing such authentication capabilities for web services.

GLOBAL SECURITY APPROACHES

PAN-AMERICAN LIFE INSURANCE GROUP IMPLEMENTS AML SOLUTION IN FOUR MARKETS, WITH MORE TO COME

Insurance and financial services provider Pan-American Life Insurance Group (PALIG) recently implemented new technology to bolster its risk

management and AML compliance efforts in the 22 countries it serves. PALIG will utilize financial services technology provider Fiserv's AML Risk Manager, which facilitates risk monitoring and activities. The solution will help PALIG comply with different territories' AML requirements, and has already been implemented in the Cayman islands, Colombia, Costa Rica and Panama, with more markets to be added soon. AML Risk Manager supports case management, detection and notification, KYC monitoring and reporting. Such solutions are becoming increasingly popular, with the global AML software market projected to rise at a compound annual growth rate (CAGR) of 15.25 percent between 2019 and 2026.

NORDIC BANKS COLLABORATE ON KYC PLATFORM TO ENHANCE DATA COMPETENCE

Six major Nordic banks are also seeking fraud-fighting measures that can work smoothly across the globe. The FIs — Danske Bank, DNB, Nordea Bank, Skandinaviska Enskilda Banken (SEB), Svenska Handelsbanken and Swedbank — recently came together to form Nordic Know Your Customer (NKYC), which will launch in 2020 and provide large and medium-sized Nordic companies with KYC services. The banks intend to offer a platform that supports gathering and managing bank customer data, and they are also developing a standard process for handling KYC details. This will simplify processes for corporate clients and help FIs improve their AML and anti-financial crime practices and information technology systems. NKYC will operate as an independent company in which all participating banks have equity holdings with Fredrik Millde acting as the interim CEO.

TRUST STAMP, VITAL4 COMBINE SERVICES INTO GLOBAL KYC/AML OFFERING FOR FIS

AI-based identity services company Trust Stamp is also taking look at multicountry KYC. It recently integrated technology from screening software-as-a-solution (SaaS) provider Vital4 into a global KYC/AML offering for FIs. The former is leveraging the latter's AI- and ML-powered data search technology and incorporating it into its KYC/AML onboarding screening solution. The combined offering will provide FI clients with ongoing due diligence processes as well as global data about FIs' potential customers, including their presences on global watch and sanctions lists, negative news stories and statuses as politically exposed persons (PEPs). PEPs act in influential public roles, thus creating greater opportunities for them to become involved in bribery, embezzlement or other corruption, making them high-risk customers.

17

DEEP DIVE

HOW FINTECHS, FIs CAN ARM UP AGAINST FRAUD

Financial services providers that slack on regulatory compliance and fail to safeguard their operations against money laundering, terrorist financing and other criminal activities may face damaged reputations and significant fines. Compliance failures are prevalent worldwide: Approximately $26 billion worth of fines were levied against banks for AML, KYC and sanctions noncompliance between 2008 and 2018. A report found that the United States imposed a full $23.52 billion —91 percent — of those penalties, while European regulators demanded $1.7 billion and the Middle East levied $9.5 million.

FinTechs could face these financial pains as regulators increasingly demand that they follow compliance rules to those which FIs must adhere. The People's Bank of China announced in March that it plans to create rules for regulating and securing the FinTech sector, for example.

FIs and FinTechs increasingly encounter new forms of fraud as they expand their digital operations, making it all the more important that they have strong risk assessment and compliance systems in place. This month's Deep Dive examines the struggles and strategies to securing the FinTech and digital banking space and how AI may be able to help.

FINANCIAL COMPANIES' SECURITY AND REGULATORY OBLIGATIONS

Financial sector players must guard against all forms of money laundering and other criminal activities, such as "smurfing." This technique allows fraudsters to get around banks'

protections and transfer large quantities of illicit funds by dividing the money into smaller deposits placed into many different customer accounts. Banks are not be required to report the deposits to the IRS if each one is below $10,000, making this kind of attack hard to detect.

The growing prevalence of cryptocurrencies is also complicating the finance sectors' security efforts. These currencies typically provide anonymity and quick international transactions, features that can facilitate money laundering and terrorist financing. Regulators are increasingly taking note of such problems, with some seeking to improve AML and anti-tax evasion efforts by prohibiting anonymous crypto transactions. Australia began regulating digital currency exchanges and requiring compliance with AML and counter terrorism financing (CTF) rules in April 2018 and France's Finance Committee raised a call to ban the trade or distribution of digital assets that enable anonymous dealings in March 2019.

FIs and FinTechs alike must stay vigilant and keep up with new risks and regulations as the threat landscape shifts. They must also ensure that they do not sweep up legitimate transactions in their fraud fighting efforts, or else they may introduce customer frictions and drain resources by investigating and filing suspicious activity reports (SARs) on false positives. A team of analysts can only handle so many potential fraud cases at a time, after all.

CAN AI SUPPORT DIGITAL BANKING'S AML EFFORTS?

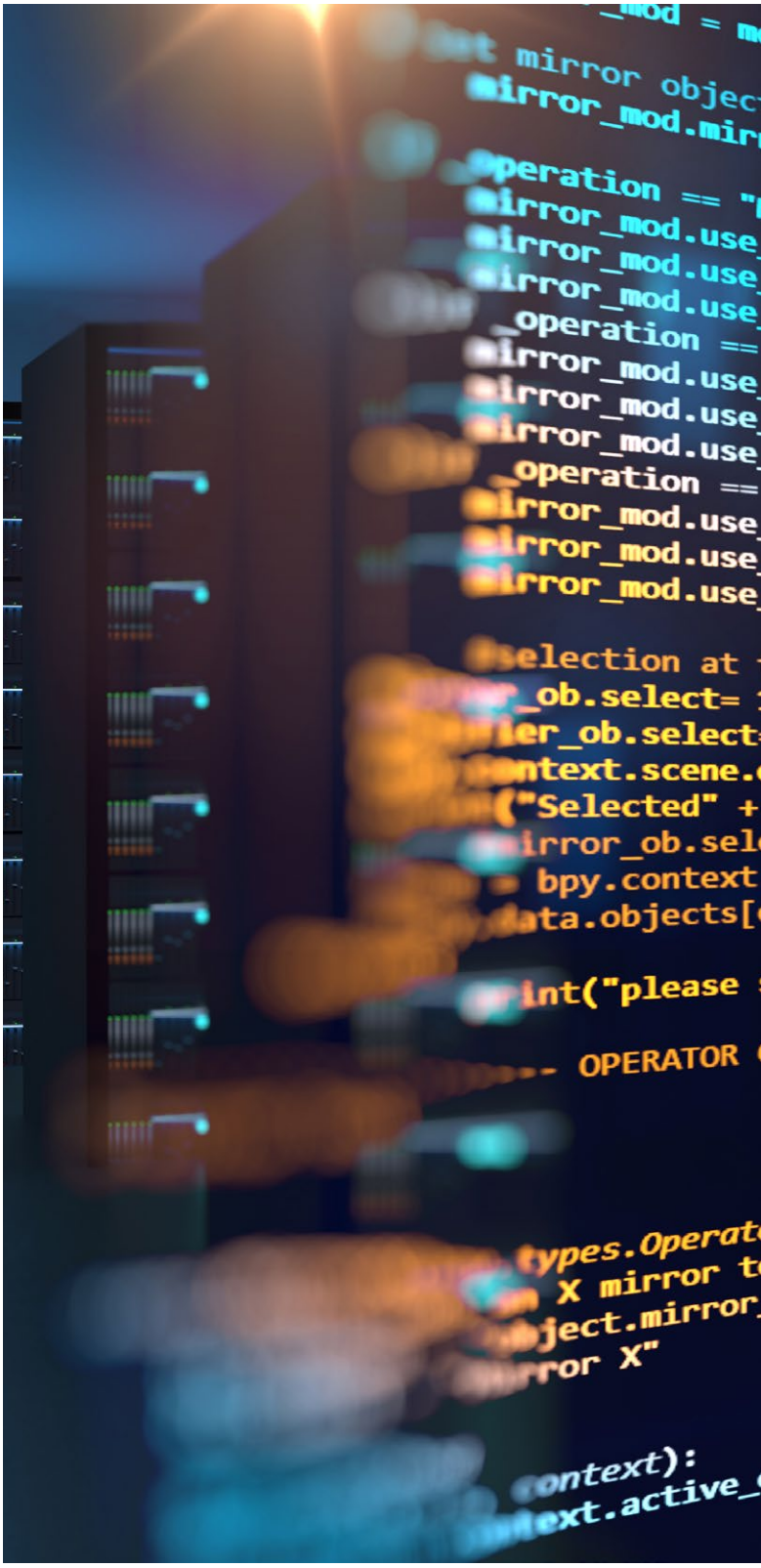
Some solution providers and observers in the space argue that many FI and FinTech AML and KYC woes stem from the struggle to acquire, sort through, fully comprehend and identify patterns in high volumes of data. Companies can experience KYC blind spots when onboarding new customers if they do not draw on the correct informational databases, which help them recognize important links the applicants may have to criminals, politicians, public figures or terrorist organizations. Those details need to be effectively analyzed, and FIs and FinTechs must continue to monitor and analyze transactional information to ensure that no issues emerge. Solution providers claim AI- and ML-based systems could aid in this by processing greater amounts of data at faster rates.

Automation tools are expected to take on the more repetitive tasks involved in AML and KYC compliance, as well as those that entail high levels of data-crunching. Leveraging automation is will likely produce fewer false positives and reduce the time it takes FIs and FinTechs to investigate red flags. ML is also capable of helping defenses stay current by adapting to emerging forms of fraud.

Effectively using AI still requires tackling some pain points, however. Some would-be adopters may question if the technology is advanced enough to make accurate, consistent

assessments. Others might find it burdensome to invest in new software and systems and change existing processes. Solution providers can alleviate such concerns by avoiding bias in AI training, establishing performance metrics for the software and assisting with gradual solution implementation, which helps avoid the disruption caused by quickly and significantly overturning existing business models. Providers should also ensure that clients understand the AI software's abilities and limitations. This allows the latter to make well-informed judgment calls based on the tools' assistances.

Money laundering, tax evasion and other types of financial fraud pose significant and evolving threats that active participants in the financial industry must contest. FinTechs looking to expand their services and customers bases, and FIs seeking to remain relevant, must find cost-effective, time-efficient ways to identify and neutralize misbehavior or risk customer defection and regulator fines. Leveraging the right technology can help these companies better support their fraud analysis teams and make the most out of their resources.



about

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Trulioo

Trulioo, an identity verification solutions provider, aims to create products that can solve online identity verification challenges in ways that are accessible to both SMBs and large enterprise customers. The company offers a single portal/API that assists businesses with their AML/KYC identity verification requirements by providing secure access to more than 5 billion identities worldwide.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at stateofAML@pymnts.com

disclaimer

The AML/KYC Tracker may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.