AML/KYC TRACKER

KEEPING CRIME OUT OF CRYPTO

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

Cryptocurrencies can be leveraged to support fast international payments, but the anonymity of such transactions also makes them appealing to cybercriminals seeking to launder money or avoid financial scrutiny. Regulators are thus pushing for greater oversight as these digital transactions grow in popularity.

Anti-money laundering (AML) and counter terrorist financing (CTF) watchdog the Financial Action Task Force (FATF) issued its final set of cryptocurrency guidelines last month, aiming to shed more light on digital asset transactions and prevent them from being used for criminal activities. The rules treat cryptocurrency transfers more like traditional bank transactions, requiring exchanges to collect and transmit information such as payment originators' and benefactors' names and account numbers. The Group of 20 (G20) international government and central bank forum recently declared its support for the new guidelines.

Not everyone fully agrees with the FAFT's rules, however. Regulation technology startup Coinfirm asserted that requiring senders' and receivers' identities in cryptocurrency transactions may be a step too far. Coinfirm was recently contracted to handle AML assessment for real-time gross settlement system (RTGS) Ripple's Ripple XRP digital currency, and claimed that analyzing public addresses' money laundering risks without revealing address owners' personal identities is sufficient.

New AML and know your customer (KYC) regulations are also coming to other sectors. Mobile wallet providers in India, such as

Amazon Pay and Paytm, have been scrambling to implement fast and cost-efficient user identity verification methods. The Reserve Bank of India will be requiring all such providers to capture that information under its new KYC guidelines, which were supposed to be implemented in February but will now take effect on Aug. 31. Mobile wallet providers that fail to find compliant digital KYC methods will be forced to use paper-based KYC, which can cost up to $4 per customer.

India is considering developing its own new KYC procedures to verify that individuals purporting to be chartered accountants, cost accountants and company secretaries genuinely have the qualifications they claim. The potential move follows several reports of forged signatures, seals and other credential-related issues.

Global regulatory measures appear to be tightening as governments and entities crack down on misuses and keep up with changing technologies. Remaining compliant isn't necessarily an easy task, however, and some notable companies have recently drawn regulators' criticism.

AROUND THE AML/KYC WORLD

Mobile banking app FinTech N26 is facing allegations regarding unaddressed fraudulent transactions and delayed responses Spellandet, has. German banking regulator BaFin resultantly instructed N26 to resolve

its backlogs of flagged transactions and redo KYC checks on certain customers, among a host of other steps. The FinTech previously saw trouble after 2018 reports found that consumers could use fake passports to open bank accounts.

SafeEnt, the company behind online casinos Ninja Casino and Spellandet, has similarly presented severe KYC failures and lost its operating license. Swedish gambling authority Spelinspektionen stated that there were "serious and systemic shortcomings" in the company's KYC and risk assessment processes, and has thus taken necessary steps to mitigate the issue.

Elsewhere, financial markets data and infrastructure provider Refinitiv is looking to expand into new markets by bringing streamlined risk management and KYC services to the wealth and advisory sector. This move builds on other recent expansion efforts, including a June partnership with global identity verification solutions firm Trulioo that helps Refinitiv

offer digital ID verification in the financial services industry.

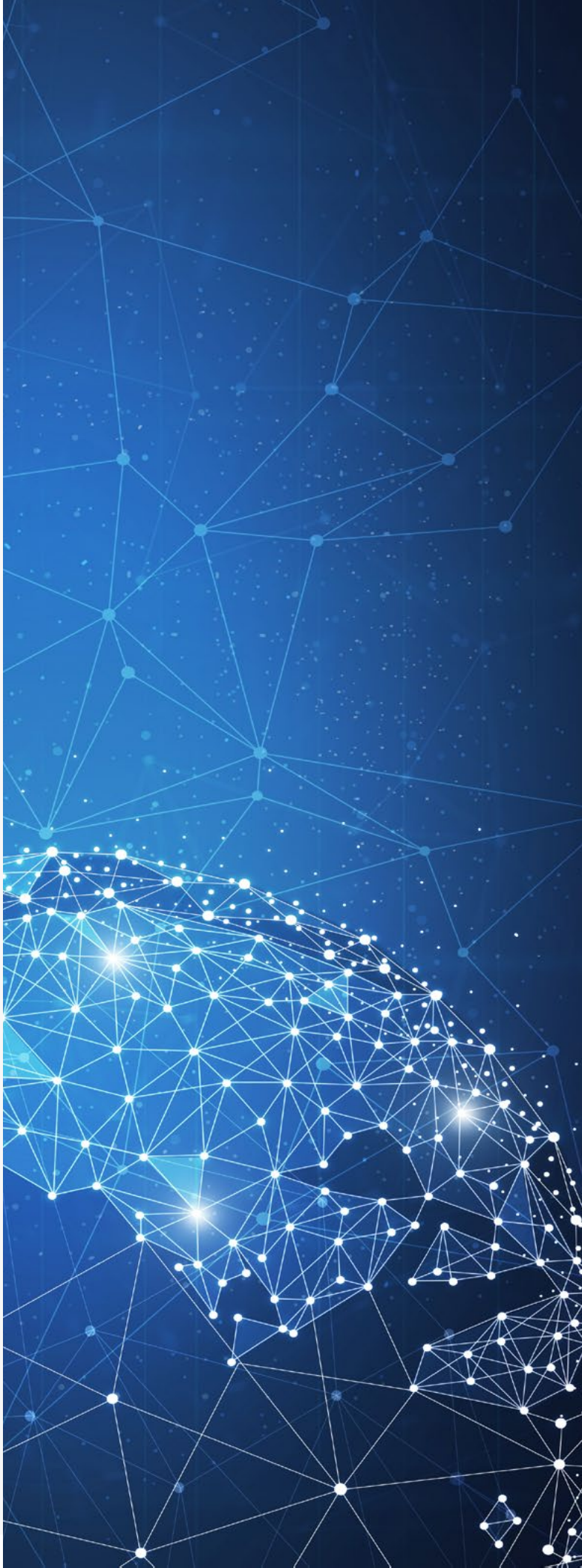
For more on these stories and other notable AML/KYC headlines, check out the Tracker's News and Trends section (p. 11).

KEEPING CRIME OUT OF CRYPTO

Major scams, theft and fraud continue to hammer the cryptocurrency space, which offers the anonymous and irreversible transactions that have become particularly appealing to criminals. Security is a top concern for trading platforms that want to keep digital asset transfers safe and compliant. In this month's Feature Story (p. 7), Adam Goldman, founder and president of Bitbuy, explains how his firm approaches security.

DEEP DIVE: ID VERIFICATION IN THE SHARING AND GIG ECONOMIES

Platforms that connect freelancers with employers and property owners with renters need to ensure that all parties can trust each other with their time, money and property. Bad actors with fake accounts often use these platforms to trick the unwary into doing work that will never be compensated or providing property that will end up stolen, and marketplaces without strong security are also targets for money laundering. This month's Deep Dive (p. 16) explores the many risks such platforms face, as well as the key strategies they can use to shore up defenses while securely and accurately identifying customers.



FIVE FAST FACTS 5

60%

Share of surveyed Asia-Pacific banks that do not have fully digital onboarding processes

$1M

Value of the fine levied on Santander by Norway's Financial Supervisory Authority for AML violations

$145,200

Value of the fine imposed on HDFC Bank by the Reserve Bank of India for KYC/AML norms violations

51%

Portion of global businesses that plan to invest more in detecting and preventing financial crime

30%

Share of surveyed FIs that said at least one of their AML components is "somewhat" or "not at all" effective

KEEPING CRIME

OUT OF CRYPTO

More than $1.2 billion is estimated to have been lost to cryptocurrency scams, thefts and fraud in Q1 2019, and cybercriminals and scammers are not the only ones putting digital asset users at risk. Canadian exchange QuadrigaCX's former CEO, Gerald Cotten, allegedly embezzled approximately $195 million of clients' funds, for example, and his recent death left the company without the passwords required to access most of its customers' holdings.

Cryptocurrency transactions' irreversible and anonymous nature and existence outside traditional banking infrastructures make them tempting targets for criminals, putting pressure on exchanges to enhance their defenses and oversight to protect users and comply with regulations.

Thwarting fraud and making usage as secure as possible are key concerns for Canadian trading platform Bitbuy. The company has focused tightly on security as it helps its user base purchase, sell and trade cryptocurrencies like Bitcoin, Bitcoin Cash, Ethereum, Litecoin and XRP. Founder and president Adam Goldman recently explained the company's approach and perspective in an interview with PYMNTS.

"A lot of criminal actors start to get it into their heads that because they'd be using the non-traditional medium of cryptocurrency, there's no course for law enforcement, so trading platforms like ourselves along with regulators need to catch these actors," he said. "But that's not the case [for businesses that are staying vigilant]."

FACING FRAUD

Cybercriminals often have a wide range of attacks at their disposal — not all of which are new. Many bad actors deploy traditional internet scams and methods like phishing and malware, while others exploit mobile phone and web browsers' vulnerabilities or software, hardware or firmware flaws. Cryptocurrency owners can also fall prey to sites that promise guaranteed returns on investment from required cryptocurrency payments, among other get-rich-quick schemes.

"Cryptocurrency, the community and the technology are simply new media for all of the existing illicit actors that commit crimes over computer networks," Goldman explained. "A lot of those actors are using their previous knowledge from the pre-cryptocurrency era to compromise certain pieces of traditional technology infrastructure in order to commit fraud or theft."

Criminals can also attempt to thwart exchanges' customer identity verification efforts by using attacks such as SIM card swaps, in which they convince carriers to switch victims' phone

numbers over to hacker-owned SIM cards. This enables fraudsters to receive their targets' incoming texts, allowing them to beat two-factor authentication measures or use password reset links to access accounts.

LOW-FRICTION KYC

Tackling such fraud issues requires cryptocurrency trading platforms to take a variety of approaches. Bitbuy has used proprietary methods to analyze transactional data for patterns and activities that could indicate red flags. The company supplements these processes with third-party assistance, such as tapping identity verification provider Trulioo to screen customers in real time. Goldman said the screening usually takes 45 seconds and enables customers to be onboarded and deposit their funds and begin trading within an hour, a quick process intended to ensure smoother customer experiences.

Bitbuy's more than 50,000 registered users are required to provide credentials such as government-registered identification forms, names, addresses and emails. The verification process includes checking IP address data, email accounts and customer information against international watch lists, with credit bureaus and through open source intelligence (OSINT) and daily investigations.

Customers who not pass automated identity checks can then undergo manual review processes. This involves additional steps, requiring users to provide two forms of government identification with photos, identification "selfies" and proof-of-address documentation like utility bills or credit card statements.

The company requests an applicant's personal information such as occupation, age and location during the manual onboarding process to further gauge risks associated with suspicious behavior. Occupation details are particularly useful in helping the company determine the likelihood that users have attained their funds through legitimate means, for example. If a prospective user intends to invest an amount equal to or greater than his or her listed occupation's average annual salary, Goldman said, that could be a red flag.

"Simple data points like asking for an occupation might indicate what may be going on here," he noted.

INTERNAL INSIGHTS

The company also inspects its internal practices by engaging an outside party to conduct "proof of reserve audits." This process includes verifying that the trading platform has the fiat and cryptocurrency holdings claimed, as well as assessing capabilities like transaction flows, private key management systems, segregated accounts and more. Goldman said a recent "proof of reserve audit" even analyzed Bitbuy's strategies for recovering customers' assets and maintaining operations in the event

of disastrous incidents, such as the death of senior management or directors. The company also uses background checks to help prevent situations in which management or employees are responsible for theft and hacking.

Exchanges must perform critical KYC, AML and other security and compliance work to ensure they support only legitimate transactions and keep customers safe from fraud as the cryptocurrency space grows. Thorough examinations of both internal practices and potential customers are key to these efforts, as is using a security approach that blends trading platforms' expertise with third-party services' transparency and impartiality. How exchanges and other parties tackle fraud and abuse will be critical to determining the future of cryptocurrency transactions.

UNDER THE HOOD

How do you expect the fraud challenges cryptocurrency exchanges face to evolve in coming years?

"The larger you grow and the more of a presence you have, the higher up you become on illicit actors' radar. The larger the presence, the more we have to mitigate against these kinds of threats. That's always a challenge. We need to stay ahead of the curve by having an internal compliance team and the right intellectual capital that helps develop the necessary security and compliance infrastructure [to] mitigate those challenges. But it never stops.

Security is an illusion. If malicious actors wish to complete their objectives — depending on how bad their objectives or end goals are — they'll most likely do whatever it takes to achieve [them]. It's a never-ending race between technology-reliant businesses and criminal actors.

The many specialists … that can mitigate against certain pain points specific to our industry would be companies like Trulioo — which offers automated KYC, leveraging global databases to highlight information — as well as custody providers that enable us to become a noncustodial exchange and keep customers safe and leveraging the expertise and tools of those focused on specific niches within this industry. … [We work with a specialist that offers] tools and services for trading platforms to law enforcement and government, helping give them insight into their potential risk exposure on the blockchain. [This partner] maintains large databases of darknet marketplaces, gambling sites, sanctions and addresses related to terrorism or other criminal activity. We're able to have those transactions flagged so that [they go] to the requisite compliance team inside our company and from there [through] the necessary process of an internal investigation and reporting it to the requisite regulatory body and/or law enforcement agency. …

As the industry progresses and technology keeps [developing], more and more tools [are created] to help [ease] the fight against criminals, frausters and security threats."

Adam Goldman

founder and president of Bitbuy

NEWS & TRENDS

SECURITY AND THE BLOCKCHAIN

COINFIRM TO PROVIDE AML FOR RIPPLE

San Francisco-based blockchain company Ripple recently inked a deal with London RegTech startup Coinfirm that sees the latter providing money laundering risk assessments of the former's XRP digital currency users. This is completed by examining factors such as whether an entity that owns a particular address is registered in a country that allows anonymous trading or is a high money laundering risk. Coinfirm will also assess how the cryptocurrency has been used, including whether it's been processed by a mixer — a tool that privately transfers funds between several counterparties — and whether large sums were transmitted by clustering, or moving small transactions from many addresses.

Coinfirm will not determine cryptocurrency owners' identities, but instead assign each user a risk score based on his or her public address. This policy falls short of the guidelines set forth by the Financial Action Task Force (FATF) intergovernmental AML body, which were officially adopted by the G20 international governmental forum in late June. FATF's suggestions require such exchanges to collect and share customer details, including names and account numbers.

WAVES INTEGRATES BLOCKPASS KYC CONNECT

Blockchain solutions company Waves recently partnered with Blockpass, a KYC, know your object (KYO), know your device (KYD) and shared regulatory compliance services provider, to make its open-source platform more secure through new KYC measures. The former is integrating the latter's KYC Connect identity verification portal for onboarding, which allows users to limit the personal information they share by providing tokens rather than personal

details. Waves users will have specialized tokens airdropped to them once the integration is complete, after which they will be prompted to download Blockpass and undergo a verification process. This information will be submitted to the company's whitelisting service when users scan QR codes on its website.

WEALTH AND INVESTMENT

REFINITIV TO EXPAND INTO WEALTH INDUSTRY KYC

A press release from financial markets data and infrastructure provider Refinitiv announced that increasing regulatory demands and desire for more streamlined processes are pushing the traditionally paper-based wealth industry toward digital onboarding and KYC. The company is looking to expand its participation in the industry by easing risk management, monitoring and onboarding processes with various KYC and artificial intelligence (AI)-based solutions. Its efforts are supported by a partnership with global identity verification provider Trulioo that will see the former implement the latter's financial services industry-focused digital ID verification and biometric solutions.

INDIA DEBATES CUSTODIAN BANK KYC

A panel led by Harun Rashid Khan, the former deputy head of the Reserve Bank of India, recently proposed a policy change that would simplify KYC requirements for foreign investors. The recommendations, which were submitted to the Securities and Exchange Board of India (SEBI), would enable global custodian banks — those handling securities and financial assets on behalf of clients and issuing licenses to overseas investors — to award foreign portfolio investor (FPI) licenses to clients from FATF-compliant countries. Such determinations would be based on documents they previously submitted in their home countries.

These clients underwent strict KYC checks to submit paperwork, thereby removing the need to collect further information. Domestic custodians objected, arguing that the policy would give their global counterparts an unfair advantage by streamlining processes for foreign investors with whom they already have relationships.

KYC IN SINGAPORE, INDIA

OCBC WORKS TO PROVIDE INSTANT CARD, PERSONAL LOAN APPROVALS

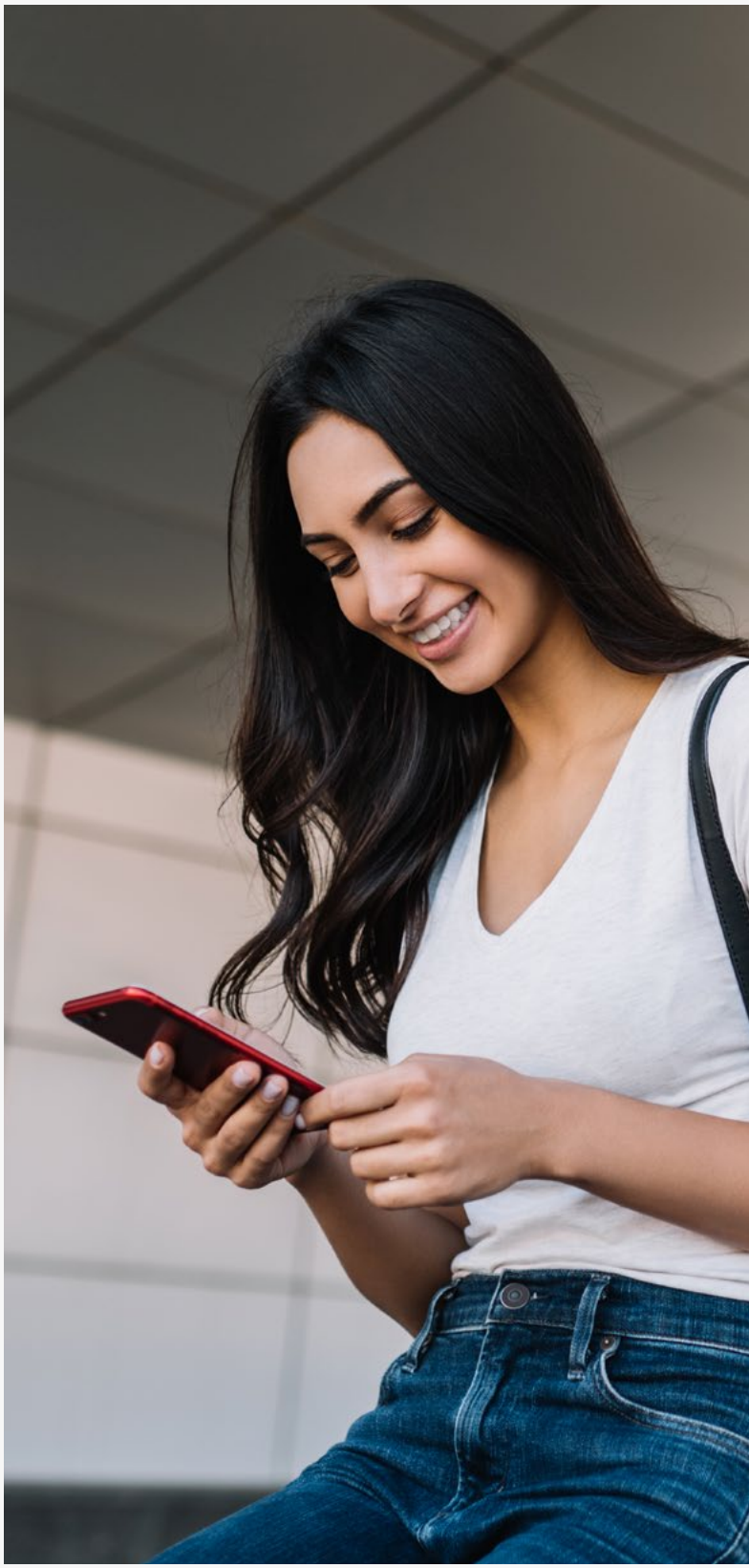
OCBC Bank, Singapore's longest-established bank, recently announced that it is working to improve its KYC processes for certain products to accelerate approval processes. The financial institution (FI) will now offer instant approvals for its debit cards, credit cards, OCBC ExtraCash personal loans and OCBC EasiCredit personal lines of credit, which will allow physical cards to be delivered on the same day applications are submitted. Personal loan funds will immediately be available.

The FI's real-time digital KYC and credit assessment process and Singapore's MyInfo national data repository allow for such speedy processes. MyInfo prefills customers' applications, while OCBC's systems validate their identities and assess their creditworthiness. The instant approval is available to the city-state's residents or permanent citizens that are existing or new bank customers. The FI also plans to implement instant approval for secured loan products, like home and car loans, according to Dennis Tan, OCBC's head of consumer financial services Singapore.

MOBILE WALLET PROVIDERS ARE READY FOR INDIAN KYC LAW IMPLEMENTATION

Mobile wallet providers in India will soon have to comply with an October 2017 mandate from the Reserve Bank of India requiring them to fully comply with KYC regulations. The mandate was originally slated for implementation in February of this year, but was delayed to Aug. 31 to give providers more time to prepare.

A supreme court ruling prevented private companies from accessing the nation's Aadhaar digital identity system, leaving mobile wallet companies fearing they would have to collect paper documents for customer validation — a time- and cost-intensive process. Some of these providers have pushed to get regulator approval for video-based KYC, which they believe could reduce costs compared to paper-based methods.



INDIA CONSIDERS STRICTER KYC FOR SMALL COURIER COMPANIES

India is also reportedly considering ways to tamp down on the exploitation of a gift policy that has allegedly enabled Chinese eCommerce companies to dodge import taxes. India does not limit the number of duty-free gifts or samples that citizens can receive, so long as they are worth no more than 5,000 rupees ($73 USD). Officials suspect that some international eTailers — Chinese companies, in particular — are labeling products as gifts to gain a competitive edge over customs-abiding companies. Some citizens received gifts every day, triggering suspicions and resulting in the government considering duty-free gift limits.

Curbing such misbehavior may require more intensive KYC regulations for the couriers that deliver such items. These companies are required to conduct KYC on delivery recipients, but Indian officials assert that smaller couriers are not always compliant.

CORRECTING SECURITY WEAKNESSES

INDIA'S MCA TO LEVERAGE ID VERIFICATION AGAINST FAKE PROFESSIONALS

India's Ministry of Corporate Affairs (MCA) is also looking at KYC, readying a mandatory process that will combat instances of individuals carrying out professional work without proper qualifications. Individuals purporting to be chartered accountants have reportedly used legitimate professionals' membership numbers to conduct audits of companies' books. Falsified signatures and seals have also become a problem.

The MCA is considering creating a registry of professionals' digital signatures and issuing a KYC form that asks for their membership numbers, phone numbers, email addresses and postal addresses. Companies will be advised against conducting business with unregistered individuals, and professional bodies related to chartered accountants, company secretaries and cost accountants will be requested to investigate.

BAFIN ORDERS N26 TO IMPROVE AML, CTF PROCESSES

German banking regulator BaFin recently instructed FinTech startup N26 to redo identity checks and KYC on several customers and resolve its transaction backlog after the former determined the latter's AML and counter terrorism financing (CTF) efforts were falling short. The order also required N26 to revise its internal processes, provide written descriptions of its workflows and increase staffing levels to manage its more than 2.5 million users.

N26 has stated in a blog post that it plans to raise staffing to 1,500 employees by the end of 2019 — achieving a ratio of approximately one staff member per 1,667 users. The company added that it must do so within

a regulator-set time frame, although it did not specify the deadline.

SAFEENT LOSES OPERATING LICENSE

SafeEnt, a subsidiary of Swedish online gaming company Global Gaming, recently lost its operating license after Swedish gambling authority Spelinspektionen found it had multiple AML and responsible gaming violations, among other issues. SafeEnt ran online casinos Ninja Casino and Spellandet, two sites that were found to be noncompliant with the revised gambling law Sweden implemented on Jan. 1.

Ninja Casino users could play without registering accounts, according to recent reports, and SafeEnt allegedly allowed them to bet large sums that surpassed players' self-imposed limits. Spelinspektionen has asserted that SafeEnt demonstrated "serious and systemic shortcomings" in its KYC and risk assessment processes.

PARTNERSHIPS AND ALLIANCES

KPMG TAPS SYNERSCOPE

Global tax, advisory and audit service firms network KPMG is looking to improve its customer due diligence, KYC and AML efforts by partnering with SynerScope, a business intelligence and big data analysis software company. KPMG advisor Leonine de Hek believes increasing its financial crimes staff will be insufficient, so the company is tapping SynerScope solutions that can analyze large quantities of data — including financial flows related to clients and their accounts. This will reveal new insights and automate processes originally handled by staff, who will now be able to focus on tasks like analyzing transactions and customers with high-risk profiles.

PROTIVITI, APPWAY COLLABORATE ON FI KYC SERVICE

Consulting firm Protiviti recently announced a new business alliance of its own with process software provider Appway. The pair aims to facilitate AML and CTF processes with an automated KYC service that will streamline the gathering, aggregation, review and validation of FIs' customer data. The product will include tools for automating blacklists, negative news and sanctions searches, as well as day-to-day case monitoring.

A Protiviti press release noted that compiling and consolidating data from various sources, verifying sources and fact-checking customer information can be particularly time consuming without such a solution. New offerings like these provide connections that minimize the hand-offs between systems — something that typically comes with legacy review processes, according to Nina Schneider, Appway's head of solutions and products.

DEEP DIVE

ID VERIFICATION
IN THE SHARING AND GIG ECONOMIES

Sharing economy platforms are opening up new opportunities for property owners and travelers. Homeowners can monetize spare rooms and visitors can secure accommodations before arriving in new cities, while car owners can turn profits on underused property and drivers can avoid the expense of purchasing items they need on a temporary basis.

Platforms facilitating these transactions must foster trust between property owners and renters if they want to be successful, but creating that confidence requires protecting both parties against fraud and bad actors. This Deep Dive explores common fraud issues affecting sharing economy or freelancing marketplaces and the identity verification strategies they can use to enhance their defenses.

MARKETPLACE ABUSE

Bad actors have various tools and techniques to steal property or launder money from sharing platforms. They tend to use stolen identity and payment credentials to establish consumer accounts on carshare sites, for example, winning over owners' trust and securing their vehicles. They then can stick someone else with the bills or make off with the cars, knowing no personal or payment information has been left behind. This makes it difficult for authorities to find them or recover stolen property.

Renters are also at risk of working with scammers who post fake listings, something that can be particularly challenging during the high-demand holiday season. Purported property owners can lure victims with low rates and post instructions for interested parties to contact them by email, rather than over the platforms' messaging systems, which allows them to act without oversight. These perpetrators will typically then ask for compensation through bank transfers, ensuring the money moves outside the platforms' safety measures like holding funds in escrow. Airbnb combats this by not releasing guests' payments until 24 hours after check-in, thereby ensuring no such problems exist.

Bad actors might also use these marketplaces to launder money by creating accounts with falsified identity and payment information. This allows them to act as both parties and channel illicit funds from one account to the other.

DEFENSE STRATEGIES

Issues like these vex users and damage platforms' reputations, discouraging buyers and sellers and harming marketplaces' revenue streams. Some sites may seek a hands-off security approach by posting warnings that they do not confirm identities, putting the burden of risk on consumers. This is not always the optimal approach, and platforms may find that it serves them better to take more responsibility by employing KYC and identity verification features.

These platforms could implement third-party identity verification or KYC services to verify freelancers' identity documents and check them for signs of forgery, or utilize methods that take advantage of videos and facial recognition technology. Onboarding procedures that only ask participants to log in with their social media accounts, rather than create new usernames and passwords, can fall short of robust verification. Platforms should instead assess the provided data by cross-referencing it against several other sources.

Bad actors on freelancing sites are also a problem, tending to offer fake profile information that asserts they have skills they do not or property that is not real. Reviews and rating systems can combat this by instilling greater

confidence in the quality — and reality — of individual users.

Smaller marketplaces may struggle to offer such solutions, however, particularly if they lack the resources necessary for in-house compliance departments. They also might be unwilling to take on the liability of protecting sensitive user data on their own servers, but third-party providers can assist these businesses with plug-and-play gateways that integrate the latest security measures.

The sharing and freelancing economy is an important sector that cannot flourish without trustworthy, well-monitored marketplaces. Identity verification often imposes extra steps in the onboarding process, but users are typically willing to endure some frictions in the interest of keeping their finances and livelihoods secure. Tackling fraudsters on these marketplaces will eventually help the entire sector grow, after all.

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.

You agree to indemnify and hold harmless, PYMNTS.COM, 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, from and against any and all claims, actions, demands, liabilities, costs, and expenses, including, without limitation, reasonable attorneys' fees, resulting from your breach of any provision of this Agreement, your access to or use of the content provided to you, the PYMNTS.COM services, or any third party's rights, including, but not limited to, copyright, patent, other proprietary rights, and defamation law. You agree to cooperate fully with PYMNTS.COM in developing and asserting any available defenses in connection with a claim subject to indemnification by you under this Agreement.