AUGUST 2021

PYMNTS.com | Trulioo

AML /KYC Tracker®

FEATURE STORY
OKEx on protecting cryptocurrency exchanges from money launderers and other threats (p. 10)

NEWS & TRENDS
More than half of cryptocurrency exchanges suffer from weak or nonexistent AML and KYC measures (p. 14)

DEEP DIVE
How eCommerce marketplaces can enhance their AML and KYC processes as more consumers use their platforms (p. 20)

PYMNTS.com | Trulioo

AML/KYC Tracker®

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

PYMNTS.com | Trulioo

Consumers have made sweeping changes to their shopping habits over the past year and a half, and one of the most notable has been the shift toward all things digital. eCommerce platforms such as Amazon, Mercado Libre and others have been particularly popular in recent months as new customers join their already swelling ranks to purchase everyday essentials digitally rather than venturing into stores.

These shifts have not been without challenges, however. Cross-border purchases among digital marketplaces continue to face several logistical hurdles, including those involving regulatory compliance. This global boom in digital transactions is proving to be irresistible for cybercriminals, who also are flocking to eCommerce marketplaces and other sites to conduct their schemes. More than 50 percent of organizations in the United States and the United Kingdom that make cross-border payments now cite fraud as their biggest concern, in fact, noting that activities such as money laundering and terrorism financing are particularly prevalent issues.

eCommerce platforms have long been responsible for complying with anti-money laundering (AML) and know your customer (KYC) requirements to curb these issues. Nevertheless, almost 50 percent of organizations say they do not conduct due diligence checks to decrease financial risks, resulting in fines for AML and KYC noncompliance that topped $10.6 billion last year.

Consumers are showing no signs of slowing their usage of digital marketplaces. This means these platforms will need to ensure that they are complying with all relevant regulations and verification procedures to safeguard customers' data and prevent criminals from taking their digital misdeeds global.

Around the AML/KYC space

Numerous online marketplaces have recognized the need to better safeguard their platforms as consumers go digital, including Argentina-based digital eCommerce platform Mercado Libre. The company recently announced that it is ironing out a new KYC process to verify sellers and individuals on its platform as well as those using Mercado Pago, its FinTech solution. Juan Chichero, the marketplace's head of brand protection, said the move already has helped the company cut down on the number of fraudsters who repeatedly attempt to open accounts.

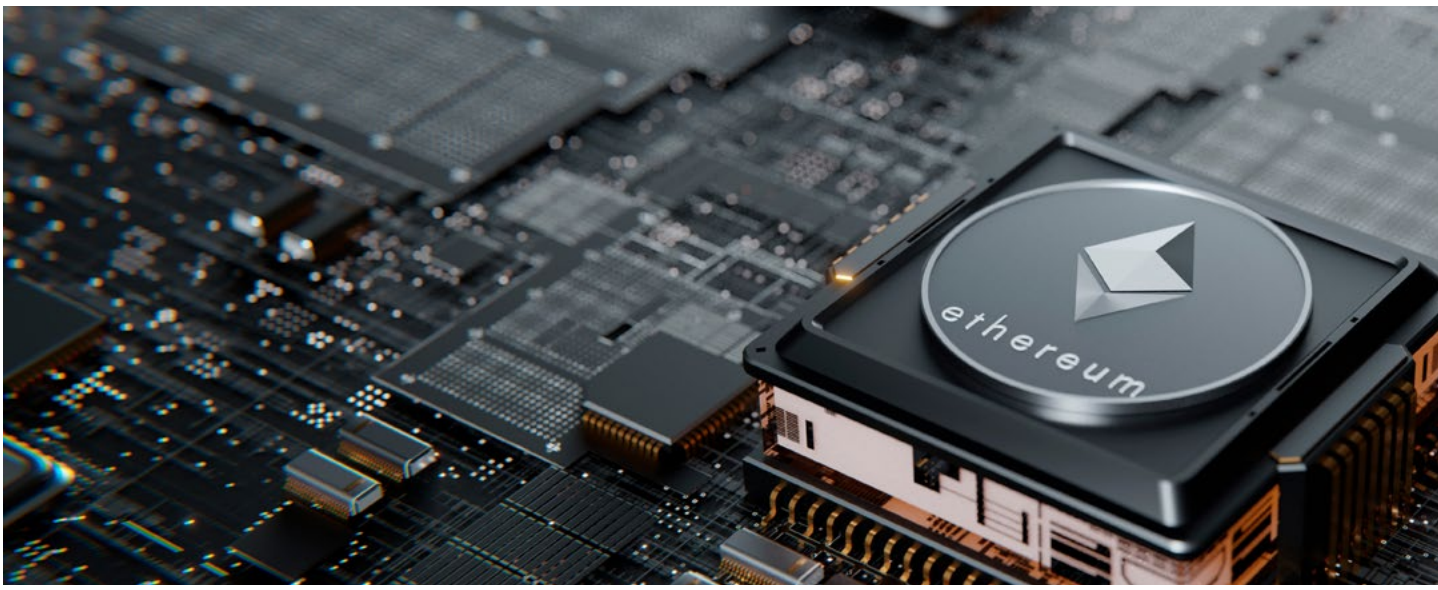
The cryptocurrency industry currently is making waves around the globe, but cryptocurrency firms in the U.K. still are struggling to meet regulations intended to curb money laundering, according to the nation's Financial Conduct Authority (FCA). The agency recently explained that a "significantly high" number of these firms had failed to meet its AML requirements. This prompted it to extend a provisional licensing program, called the Temporary Registration Regime, from July 9 until March 31, 2022, to prevent an "unprecedented" number of crypto firms from withdrawing their trade applications due to noncompliance.

Some payment providers have recognized that they need to employ more advanced identity verification services to protect their customers as cross-border commerce booms. Global identity verification solutions provider Trulioo recently reported that four payment providers — PayDo, Pollen Technologies, Sokin and XanderPay — had begun using its solutions, which leverage biometrics in addition to examining phone records and other forms of analysis to satisfy cross-border KYC requirements. Trulioo CEO Steve Munford said more payment providers will need to tap into robust identity verification tools as they aim to offer seamless yet secure payment solutions for customers.

For more on these stories and other headlines from the AML/KYC space, visit the Tracker's News and Trends section (p. 14).

How customer authentication and transaction analysis can prevent cryptocurrency money laundering

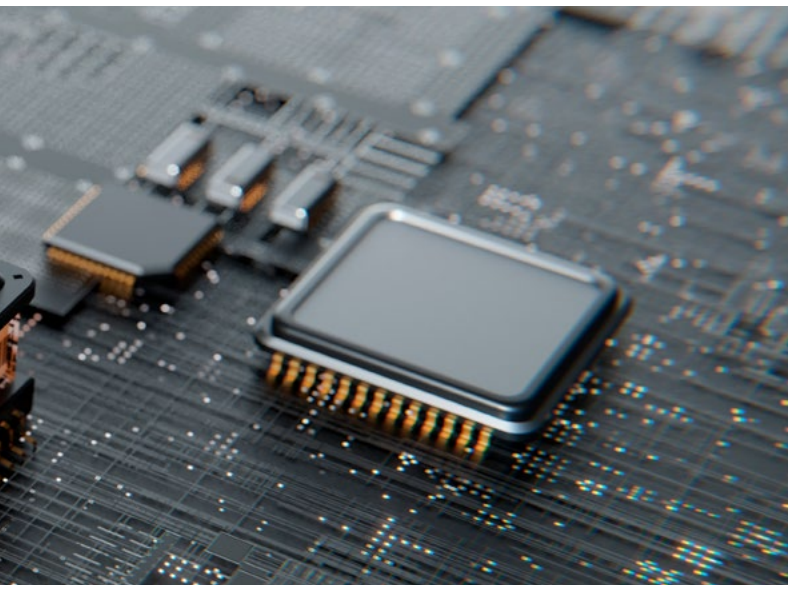
The cryptocurrency space is an appealing target for money launderers due to its largely anonymous nature and historical lack of regulation. These trends are changing quickly, however, as world governments and international regulatory organizations begin to crack down on this fast-growing industry. In this month's Feature Story (p. 10), PYMNTS talks with Jay Hao, CEO of cryptocurrency exchange OKEx, about how the exchange



leverages customer authentication and transaction analysis to thwart money laundering and remain compliant with AML and KYC regulations.

Deep Dive: How fortifying their AML and KYC measures can help eCommerce platforms clamp down on crime

eCommerce platforms are becoming crucial channels for customers looking to purchase essential items without heading into stores, leading to robust global growth in the space. Cybercriminals are hot on their heels, however, and remain eager to conduct their illicit activities amid all of this increased traffic. This month's Deep Dive (p. 20) examines how digital transactions, particularly those conducted via eCommerce marketplaces, are becoming more commonplace and how these platforms can bolster their AML and KYC measures to keep fraud and money laundering at bay.



EXECUTIVE INSIGHT

eCommerce platforms must comply with AML and KYC requirements as they expand their operations overseas. Which tools or approaches can help these marketplaces?

Incorporating a variety of identity verification processes, data sources and strategies is a key approach for globally scaling eCommerce platforms that want to deliver convenient yet secure digital experiences. In other words, the orchestration of different identity proofing techniques ensures that legitimate users receive a level of friction appropriate for their risk profile. Meanwhile, a bad actor who might display risk signals will be flagged for further or enhanced due diligence. In this way, legitimate users do not have to go through unnecessary checks and can proceed on the customer journey with minimal disruption, and bad actors are prevented from moving through the onboarding process.

This holistic and layered approach allows businesses to act in an agile way because processes are tailored to the unique characteristics and demographics of each region their customers are located in. This also enables eCommerce platforms to understand the operational and business risks that pertain to a specific region, as well as stay abreast of AML and other compliance requirements.

ZAC COHEN
Chief operating officer
Trulioo

FIVE FAST FACTS

eCOMMERCE

Mercado Libre says it is undertaking a KYC initiative to better verify the sellers and individuals on its platform.

CRYPTOCURRENCY

The U.K.'s FCA says a "significantly high" number of cryptocurrency firms are missing the mark on AML requirements.

FINANCIAL SERVICES

Banks and other financial services players are beginning to reexamine their KYC measures to keep digital-first consumers more secure.

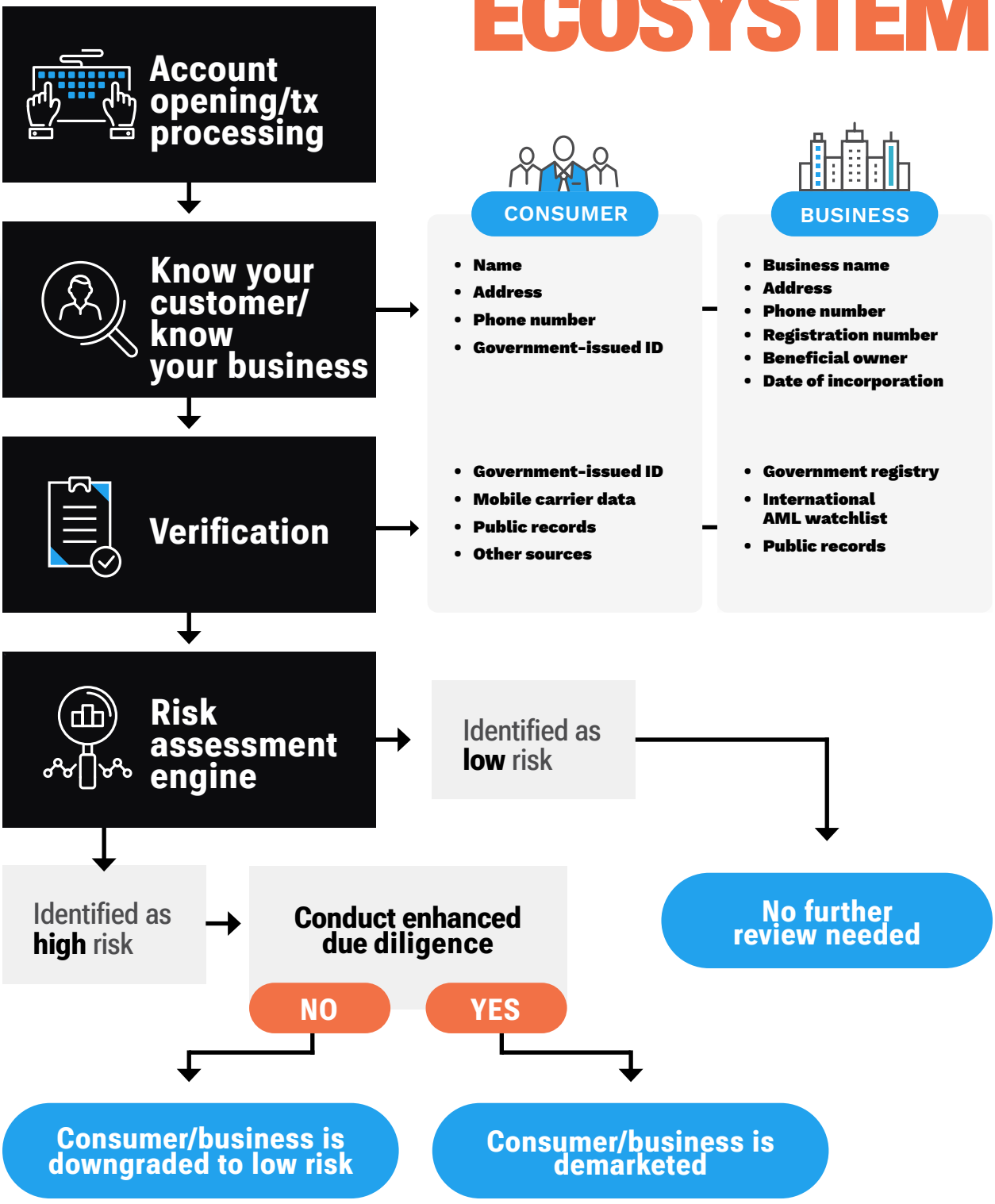
REGULATIONS

The EU recently proposed legislation that would overhaul its AML and counterterrorism financing rules.

COMPLIANCE

Businesses worldwide are spending billions annually to comply with various financial regulations.

AML/KYC ECOSYSTEM



Feature Story

PYMNTS.com | Trulioo

OKEx On Protecting Cryptocurrency Exchanges From Money Launderers And Other Threats

Cryptocurrency exchanges are under constant threat from money launderers, with criminals using bitcoin addresses to send more than $3.5 billion in 2020. These instances of fraud typically are conducted from individual, high-value accounts rather than on a wide scale, and experts found that just 270 blockchain addresses were responsible for 55 percent of all cryptocurrency-linked money laundering.

Keeping cryptocurrency accounts from being used in high-roller money laundering schemes is a top priority for exchanges such as OKEx. The Seychelles-based company had a trading volume $188 billion in February alone, which could make it a tempting target for money launderers without robust AML and KYC systems in place.

“Money launderers often use various means to disguise the source of funds for layering purposes,” OKEx CEO Jay Hao said. “Digital asset exchanges could be a channel for them to do such layering and, therefore, services like ours must be vigilant about such risks.”

Hao spoke to PYMNTS in a recent interview about how the exchange deploys sanction screening, identity verification and other tools to keep money launderers at bay.

Using customer identification and screening to prevent money laundering

Checking customers at the virtual door is the first step in OKEx’s money laundering prevention process. Governments around the world maintain sanctions lists of known money launderers and cybercriminals, and while many cryptocurrency exchanges do not require any sort of identity verification, OKEx takes steps to ensure its customers are who they say they are and not money launderers in disguise.

“OKEx conducts identity verification for our customers to gain customer information,” Hao said. “Sanction screening is crucial, as we have to make sure that customers are not on the sanctions lists.”

Some money launderers attempt to launch their schemes only after they have infiltrated the systems of cryptocurrency exchanges, however, meaning they would not show up on any sanctions lists during the onboarding. This is where behind-the-scenes transaction monitoring comes into play, Hao explained.

“We perform ongoing transaction monitoring to review our customers effectively,” he said. “When there is abnormal trading behavior, our system will trigger an alert to our compliance team for further investigation. We also provide assistance to law enforcement agencies and keep a record of such suspicious transactions in our database to prevent them from using our platform. Once there is reasonable ground to believe that a customer is behaving suspiciously, OKEx will freeze the user’s account and will consider terminating the account at our discretion.”

AML and KYC compliance becomes more complicated when transacting across borders and when anticipating future threats, but OKEx believes it has a firm handle on these potential challenges.

Complications in AML and KYC

Cross-border payments can lead to complicated AML and KYC processes, as the governments on either end of any given transaction may have complex and sometimes contradictory compliance regulations. These regulations pose little issue for cryptocurrency exchanges such as OKEx due to their blockchain-based nature, however.

“Blockchain transactions and the trading of digital assets are borderless,” Hao said. “The same stringent level of internal control and ongoing transaction monitoring are adopted in order to detect abnormal trading behavior.”

Sanction screening is crucial, as we have to make sure that customers are not on the sanctions lists.

Other developments are looming on the horizon for exchanges, including new recommendations from the Financial Action Task Force (FATF), which recently instituted a “travel rule” that mandates cryptocurrency exchanges have KYC information from both the sender and recipient of each transaction.

Hao said OKEx still is working to adapt its KYC processes to account for this new regulation but is confident the exchange can continue transacting securely.

"There are a few major trends in the digital asset industry due to the recommendations made by the Financial Action Task Force," he said. "OKEx is working on the understanding and analysis of recommendations such as the so-called travel rule, which requests that virtual asset service providers including OKEx collect data from our customers and share it with the necessary parties in a compliant manner."

The world of cryptocurrency is growing quickly. Any exchange should be agile enough to keep up with the latest fraud and money laundering trends as well as the compliance regulations intended to stop them.

News & Trends

PYMNTS.com | Trulioo

eCommerce transactions and AML/KYC compliance challenges

ID verification solutions provider Trulioo adds clients as cross-border commerce picks up

Payment providers worldwide are turning to identity verification services to ensure they are safeguarding their clients' and customers' platforms from fraud as more commerce is conducted across borders. Global online identity verification solutions provider Trulioo, for example, recently announced it has added four new European clients to its ranks. The payment providers — PayDo, Pollen Technologies, Sokin and XanderPay — all are tapping Trulioo's solution, which leverages biometrics and other tools to comply with cross-border KYC requirements. The service also examines phone records, checks in with credit bureaus and conducts other forms of analysis for verification.

Consumers focusing more on data security, compliance during eCommerce transactions

Consumers have grown more reliant on eCommerce and in-store digital payment methods over the past year and a half, with one study showing that 92.3 million U.S. adults used mobile devices to make payments in stores over a six-month period. It is no surprise that online shopping can give customers convenience and hyper-personalized experiences, but the technology underpinning these experiences can be a limiting factor. eCommerce merchants must get the experience right, as 47 percent of consumers say payment frictions can determine whether they will complete transactions. Customer checkout also is more than just user experience: It requires addressing consumers' fears, particularly those regarding data security. Third-party developers are beginning to create applications for the commerce and finance industries, leading customers to scrutinize how their data is being handled and whether merchants are adhering to the

necessary KYC compliance measures. This makes it imperative for organizations to respond thoughtfully in how they accept, store and leverage consumer data to provide secure and compliant experiences.

Online marketplace Mercado Libre focusing on KYC efforts amid surge in digital shopping

Seamless cross-border transactions have become table stakes over the past year, meaning online marketplaces must safeguard customers using their platforms or risk seeing them defect to competitors. Argentina-based eCommerce platform Mercado Libre recently reported that it is working to meet customers' new expectations by revamping its KYC process. It is unveiling a new KYC initiative aimed at verifying both individual sellers and businesses on its platform, as well as those that use its FinTech service Mercado Pago.

Juan Chichero, the marketplace's head of brand protection, noted that the initiative is intended to protect the platform from fraud and is currently being used in Argentina, Brazil and Mexico. He explained that it has been invaluable in helping Mercado Libre reduce the number of fraudsters that repeatedly try to open false accounts. Such tools will continue to come in handy as consumers around the world flock to eCommerce platforms for more of their products.

AML/KYC and the financial services sector

How banks can evolve and bolster their KYC processes to support digital-first customers

The global increase in online transactions is leading to a corresponding rise in cybercrime, prompting financial institutions (FIs) to reexamine their KYC measures. Research shows that digital fraud against consumers increased by almost 24 percent for the period of January to April 2021, compared to the period of September to December 2020. Consumers appear to be willing to roll the dice somewhat despite these issues, however, with 44 percent saying they still would order goods and services online from virtual storefronts even after hearing of security or privacy issues. Nearly half of consumers also reuse the same usernames and passwords across virtual accounts and spend less than 10 minutes when opening an account online, indicating that in many cases, digital financial transactions are more about convenience than safety.

FIs have responded to these shifts with stricter measures to protect consumers and adhere to regulations. Refining their KYC processes and adding identity verification technology to enhance compliance can help them provide more transparency and control, which could give them an edge as they try to keep customers loyal.

FIs around the globe were fined more than $10.6 billion for regulatory noncompliance, including AML/KYC noncompliance.

Crypto's AML and KYC challenges

Subpar AML and KYC compliance is hindering broader expansion of the crypto industry

FIs are continuing to adjust their AML and KYC efforts, but compliance fines are mounting as they struggle to manage regulatory requirements across borders. Recent research found that FIs around the globe were fined more than $10.6 billion in total for noncompliance

with government-related AML, KYC and related regulations designed to curb illicit activities conducted via digital transactions.

One of the biggest hurdles the crypto space confronts is money laundering, with $3 billion laundered via cryptocurrency exchanges in 2019 alone. Many of these issues stem from the space's relative lack of adoption when it comes to AML and KYC measures, with one study finding that more than 50 percent of these exchanges suffered from minimal or nonexistent KYC processes. Many cryptocurrency platforms have begun to heed the message, however, as they now realize that the future of the industry and its broader adoption around the globe hinge on adhering to effective AML and KYC measures.

UK FCA warns that many crypto companies are missing AML mark

Cryptocurrency companies also are running into hurdles in the United Kingdom. The group of four nations' financial services board, the FCA, recently noted that a "significantly high" number are as yet unable to meet its AML requirements. The FCA had created a provisional licensing program, the Temporary Registration Regime (TRR), that would allow companies with pending applications to continue trading during review.

The TRR was slated to lapse on July 9, but the FCA since has decided to extend it until March 31, 2022, to prevent an "unprecedented" number of businesses from withdrawing their applications. Only five cryptocurrency firms currently are registered with the authority.

Compliance and digital ID efforts

EU moves to strengthen AML rules and create new agency to combat money laundering

eCommerce platforms, FIs and cryptocurrency exchanges are hardly the only entities looking to combat money laundering and fraud. Governments also have a vested interest in beefing up their AML efforts. The European Union recently proposed legislation that would bolster the region's rules regarding AML and counterterrorism financing (AML/CFT). In addition, the move would create a new panel designed specifically to fight money laundering. The proposal aims to help entities subject to AML/CFT rules better spot illicit or suspicious transactions and close loopholes through which cybercriminals finance terrorist activities or launder money.

The new panel created to oversee the nation's AML efforts would be called the EU-Level Anti-Money Laundering Authority and would be tasked with coordinating with various member states to ensure that the EU's rules are enforced consistently across the region.

More organizations eyeing corporate digital ID to streamline verification, KYC

Companies are conducting more of their business online, leading many to examine the benefits of corporate digital ID. Businesses can use these identifiers to make verification faster and clearer, and unlock numerous other functions. The data points for such identification can include everything from

bank account information to digital corporate numbers, and these solutions could make digital transactions such as tax payments more seamless and secure. Another prime benefit includes streamlined KYC processes, as corporate digital ID can help firms reduce false positives and distinguish themselves from companies with similar names.

Though corporate digital identity technology exists, companies will need to collaborate to create standards that encourage interoperability as these solutions catch on with more firms. The rewards likely will be manifold, however, especially as businesses work to ease their cross-border transactions and interactions in the years ahead.

Deep Dive

PYMNTS.com | Trulioo

Improving AML/ KYC Compliance Measures To Enhance Cross-Border Payments Infrastructure

The “fifth industrial revolution” — in which AI continues to help drive mass customization and personalization for humans — may not be here just yet, but, due to the digital transformation that took place in 2020, many experts agree society is getting closer. The shift toward an ever more digital world also calls attention to the weaknesses in existing technological infrastructures that hinder our entrance into the fifth industrial revolution, such as technology challenges in the cross-border payments space.

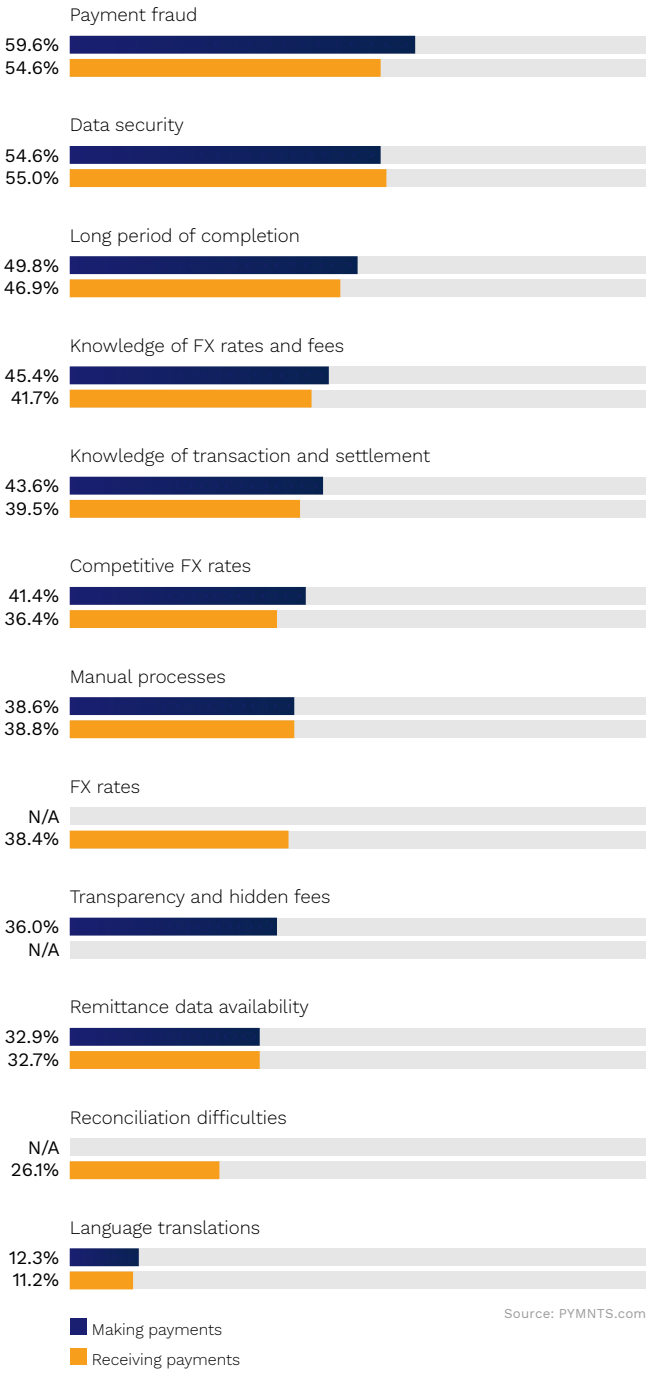
Research indicates that the pandemic increased online spending more than 77 percent in May 2020, the height of the pandemic’s first wave. Even countries previously less reliant on eCommerce marketplaces and online shopping made shifts in their purchasing behaviors. For example, 13 million Visa cardholders in Latin America made online purchases for the first time in 2020 because of the pandemic. Consumers growing more accustomed to the convenience and pace of digital transactions they expect seamless experiences, whether an online purchase is made from a vendor locally, domestically or internationally.

Modern cross-border payment technology is rife with turbulence, however. In addition to well-documented issues including slow and opaque payment processing, exorbitant fees and outdated operational systems, the global pandemic also has drawn increased attention to a far darker side of cross-border payments: the ability to easily exploit the system for illicit activity.

This month’s Deep Dive will examine the efforts being made to secure and enhance cross-border payments infrastructure.

FIGURE 1:

Primary cross-border payments frictions
Share of surveyed businesses that worry about select payments pain points



Source: PYMNTS.com

The state of compliance for cross-border payments

There is room for improvement in the cross-border payments space. A recent study conducted by PYMNTS revealed that nearly 60 percent of organizations in the U.S. and United Kingdom now believe payment fraud is the biggest friction with cross-border payments, with data security a close second.

Vulnerabilities in cross-border payments were not created because of the pandemic, but they were certainly magnified. Experts also agree that the global pandemic of 2020 created even more opportunities for fraudulent activity in the financial realm. Research indicates that every year, between 2 percent and 5 percent of the global gross domestic product (GDP) is laundered through digital financial networks; however, less than 1 percent is stopped.

Across the globe, from Asia to America, businesses already invest billions of dollars in compliance. However, an influx in digital transactions — which many organizations weren't entirely equipped to handle — outpaced the ability for businesses to perform optimal due diligence on cross-border payments.

Seventy-three percent of companies in a recent global survey said they faced mounting pressure to grow their bottom lines amid the pandemic, 65 percent of respondents fell short on KYC compliance in response to the pressures felt and less than 50 percent conducted formal customer or third-party due diligence checks at all.

The digital transformation of 2020, which caters to accepting more digital transactions, leaves businesses wondering what the next iteration for the cross-border payment process — that allows organizations to protect both themselves and consumers from growing illicit activity in the space — will be.

What's next for cross-border compliance?

A globalizing world means that companies, financial institutions and government bodies need to also think globally when it comes to their payment architecture, especially as cryptocurrencies, an inherently anonymous form of digital currency, continues to grow in acceptance and further muddies the already opaque cross-border payment process. To improve the existing process and combat fraud, a slew of solutions can be leveraged.

The banking industry and disparate governmental bodies first need to come together and lead the charge when it comes to the controls and standards that can prevent illegal use of the financial system. ISO 20022, the international payment messaging standard, is embraced by a mere 70 countries around the world, for example. Banks and politicians will have to help drive adoption and interoperability. Secondly, AML and KYC compliance strategies should become seamless regardless of jurisdiction and business type. The EU already is making movement to break down the barriers that impact its ability to crack down on money laundering and terrorism-financing. The 27 member states of the EU actively are working on a new authority to close the gaps that criminals exploit in the existing global financial system.

Additionally, adaptive technology to keep up with a changing financial landscape is essential. Identity verification services that can help organizations adhere to KYC requirements and the SWIFT gpi standard, which can help organizations prevent and detect illicit activity by creating signals and next-step actions in real time should a suspect transaction occur, are two critical pieces of technology to implement.

Though there are a number of issues to work out to smooth cross-border payments, solutions are becoming available and improving in performance every day. With no signs of online commerce or cross-border payments slowing down, making moves to ensure compliance and safety of digital transactions is in the best interest of everyone from consumers to legislative bodies.

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.