

AML/KYC

TRACKER®

DECEMBER 2020

FEATURE STORY — 7

BitGo On Providing
Secure AML/KYC
Compliance For
Cryptocurrency

NEWS & TRENDS — 11

56 percent of cryptocurrency
exchanges have weak or
nonexistent KYC guidelines

DEEP DIVE — 19

Tamping down on cryptocurrency
exchange cybercrime with AML/
KYC compliance

Table Of

C O N T E N T S



PYMNTS.com

3 WHAT'S INSIDE

A look at recent AML and KYC developments, including \$2.8 billion laundered through cryptocurrency exchanges and the government and private efforts intended to stop it

19 DEEP DIVE

An in-depth examination of the skyrocketing cybercrime on cryptocurrency exchanges and the pressures they are facing from world governments and regulators to step up their AML and KYC processes

7 FEATURE STORY

An interview with Anthony Botticella, CEO of BitGo Trust, about how the company deploys a multilayered AML/KYC system to prevent and monitor for suspicious activity on its platform

22 ABOUT

Information on PYMNTS.com and Trulioo

11 NEWS & TRENDS

The latest headlines from the space, including Metal Pay's recent partnership with Trulioo to help root out money launderers and why 56 percent of cryptocurrency exchanges don't follow KYC guidelines

ACKNOWLEDGMENT

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

What's INSIDE

Money laundering is a global plague, with the estimated amount in a given year [ranging from \\$800 billion to \\$2 trillion](#) — or anywhere from 2 percent to 5 percent of the global gross domestic product (GDP). The growing popularity of online banking has also pushed money laundering into the digital realm as drug dealers, terrorists or human traffickers who might once have set up brick-and-mortar businesses to launder their ill-gotten funds can conduct the same operations today completely virtually, even establishing multiple websites as backups in case authorities catch on.

One particularly common avenue for money laundering is through cryptocurrency — a burgeoning market expected to be [valued](#) at \$1.4 billion by 2024. Its skyrocketing popularity obscures an ever-expanding web of money laundering schemes and other cybercrimes,

however, with experts predicting that cryptocurrency-related crimes [totaled](#) \$4.3 billion in 2019, including [\\$2.8 billion](#) in laundered money. This is up from just \$1 billion laundered in 2018, and the problem is expected to continue its rise as cryptocurrencies become more popular, valuable and commonly accepted among merchants.

Governments around the world are cracking down on cryptocurrency exchanges' lax anti-money laundering (AML) and know your customer (KYC) procedures, both of which could result in a serious dent in money laundering activities if they were deployed effectively. Many cryptocurrency exchanges are denying that such a problem exists at all — and are subsequently reaping harsh fines and even jail time for their owners as a result — but others are working on improving their AML procedures with the help of third-party partners.

The very nature of cryptocurrencies means that they will likely always be a viable avenue for money laundering, but risk levels could potentially be reduced with diligence on the parts of both government regulators and the exchanges themselves.

Around the AML and KYC world

Part of what is fueling money laundering and other cybercrime on cryptocurrency exchanges is that the majority of these exchanges have few methods in place for verifying their users. One recent [study](#) found that 56 percent of cryptocurrency exchanges have weak or nonexistent KYC systems that do little to prevent money laundering. Many exchanges deliberately obfuscate their country of origin to avoid having to comply with any sort of KYC guidelines at all, exacerbating the money laundering problem.

This lack of sufficient KYC processes at many cryptocurrency exchanges is generating an absence of trust from banks and government regulators. A recent joint [survey](#) revealed that 88 percent of financial experts say that cryptocurrencies aid in money laundering and only 9 percent feel that the sector is combating this to the best of its ability. Players in the cryptocurrency market disagree, however, with only

56 percent of these professionals saying that money laundering is a significant issue and 48 percent opining that it is being sufficiently fought at exchanges.

The cryptocurrency industry is not the only one facing AML/KYC difficulties, however, with traditional financial institutions (FIs) also reporting struggles with these processes. Forty-seven percent of American banks and 40 percent of European banks declared in another recent [study](#) that regulatory compliance is their primary challenge in 2020. This is chiefly due to the fact that customer onboarding is done by a large number of smaller, fragmented teams rather than a single dedicated workforce.

For more on these stories and other AML and KYC developments, read the Tracker's News and Trends section (p. 11).

How BitGo's AML/KYC protocols detect and prevent suspicious activity

Protection of client assets is just as paramount in the cryptocurrency industry as it is in traditional finance. Digital asset financial services providers like [BitGo Trust](#) have developed multilayered protocols for AML/KYC compliance as a single layer of security is not

nearly adequate. In this month's Feature Story (p. 7), PYMNTS talked with Anthony Botticella, CEO of BitGo Trust, about how the company leverages ID verification and behind-the-scenes transaction analysis to stop bad actors in their tracks.

Deep Dive: Enforcing AML/KYC compliance at cryptocurrency exchanges

Billions of dollars flow around the world in cryptocurrency transactions, with their anonymous nature making them a prime way for money launderers to conduct their crimes. The cryptocurrency exchanges themselves are often reluctant to step up their AML procedures to prevent this, but government oversight authorities are cracking down on noncompliant marketplaces. This month's Deep Dive (p. 19) explores the various ways that money launderers exploit cryptocurrencies and examines the actions that regulators are taking to reduce the spread of cybercrime on these platforms.



FIVE FAST FACTS

VERIFICATION

Less than half of all cryptocurrency exchanges have functional KYC systems.



REGULATION

FinCEN has fined the owner of two cryptocurrency websites \$60 million for AML violations.



DISTRUST

Banks are growing increasingly distrustful of cryptocurrency exchanges' AML procedures, while the exchanges maintain they are used for valid reasons.



TEAMWORK

The EU is forming a new regulatory agency to monitor member states' AML procedures and ensure they are up to continent-wide standards.



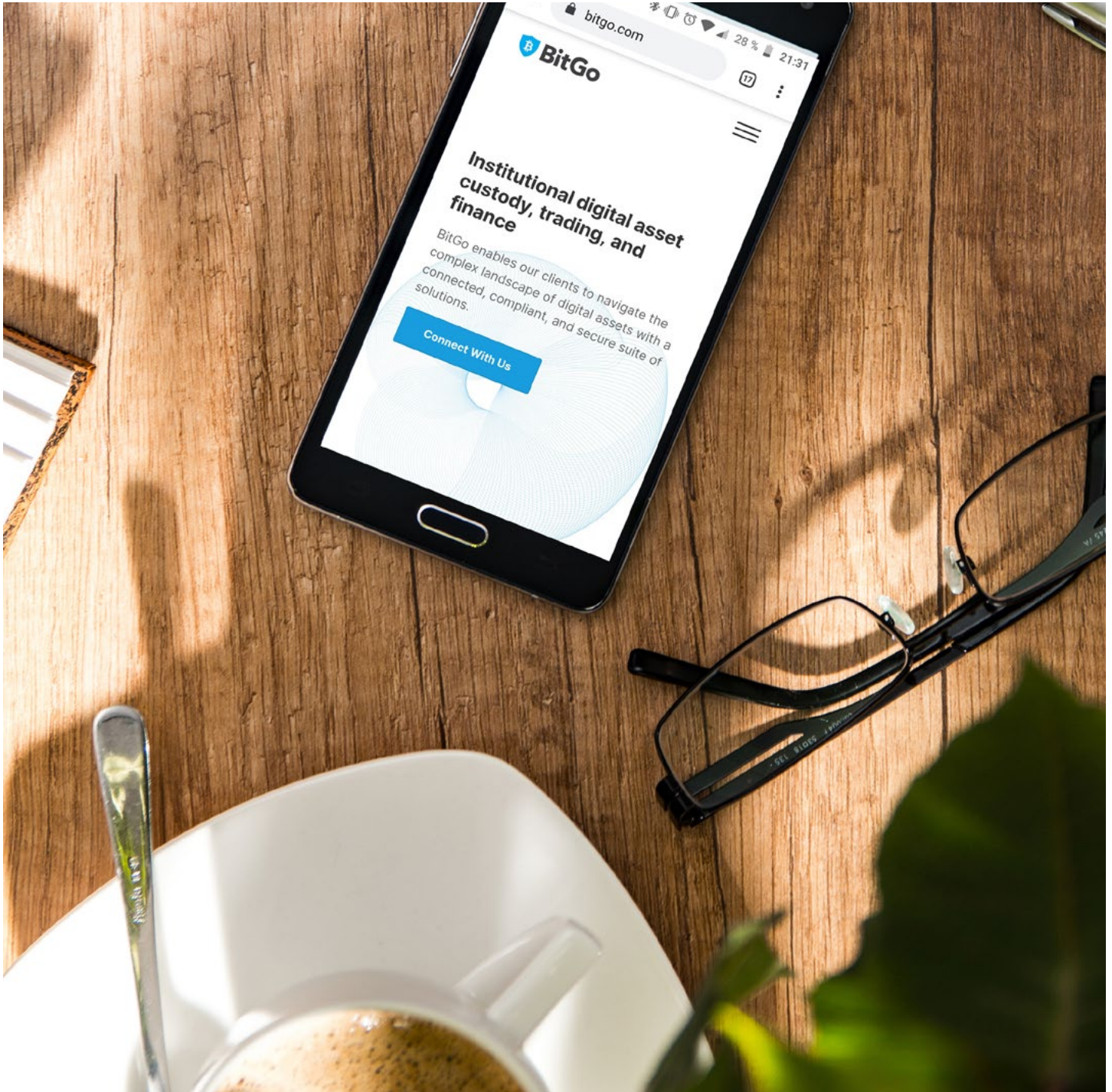
COMPLIANCE

Bank compliance staff are finding it progressively more difficult to meet AML/KYC regulations due to the distribution of this work among multiple unsynchronized teams.



Feature

STORY



BITGO ON PROTECTING CRYPTOCURRENCY EXCHANGES FROM MONEY LAUNDERERS

There are currently more than 5,500 different cryptocurrencies in [circulation](#), but the biggest name in the business — and often a metonym for the industry itself — is bitcoin. The year 2020 saw 18.42 billion bitcoins in circulation, with a market capitalization of \$117.81 billion and an individual coin valued at \$19,463 as of December. These coins often change hands, either through cryptocurrency exchanges or via digital asset financial services providers like [BitGo Trust](#).

Many cryptocurrency exchanges have faced challenges for suspicious activities, such as money laundering, but BitGo Trust, a division of BitGo Holdings, is regulated by the South Dakota Division of Banking and leverages the same onboarding protocols for AML/KYC practices as traditional financial institutions.

“Crypto is still a very new industry,” Anthony Botticella, CEO of BitGo Trust, said in a recent interview with PYMNTS. “Some of the players that are coming up may not understand all the requirements. So, we take a very educational approach when dealing with clients and we have to explain what we’re asking for, why we’re doing it and how we’re going to be compliant with U.S. regulations.”

BitGo’s AML procedures incorporate both a client authentication system at the point of sign-up and a back-end analysis system that identifies and flags suspicious transactions that could indicate money laundering.

Verification at the point of entry

The first step to detecting and preventing money laundering begins at the point of entry, when new customers sign up for accounts with BitGo. All new customers must undergo a rigorous KYC process to ensure they are not known money launderers by cross-referencing several points of personal information.

“We run [new customers] through our screening tool to make sure that they don’t hit any [Office of Foreign Assets Control] or other sanctions lists as well as background searches and verifying their identities using a government-issued

ID, like a driver's license, [along with] proof of residency," Botticella said. "Then we also require our clients to do an onboarding call, so it's an actual person versus somebody doing it anonymously on the internet and having documents. Everybody does a video verification as well."

All customers are subject to a pre-KYC call to ensure they understand the requirements for opening up an account before this process even begins. The process is often more difficult for foreign customers, who may not understand U.S. compliance regulations or have the necessary equivalent documents for verification.

"The biggest thing is document translation: What we may call articles of incorporation, they may call something else," he explained. "A country may have an ID that doesn't expire, for example. We [have to] learn every different country's rules and regulations of what's an acceptable document, what their passports and driver's licenses look like, certain things like that."

The KYC process at the point of account creation is only the first line of defense, however. Ongoing monitoring of existing accounts is also necessary to ensure that cryptocurrency exchanges like BitGo are continuously compliant with AML regulations.

Transaction monitoring behind the scenes

The second step of BitGo's AML procedure is a transaction monitoring algorithm that reviews the funds moving in and out of accounts to determine if they are received from or sent to any suspicious destinations, such as dark web marketplaces. This is supplemented by periodic reviews of all transactions to check for unusual behavior.

"We conduct annual reviews of our clients as required by regulators," said Botticella. "If necessary, we'll go back to the client, reverify who's on the account, what they're doing and if any of their business purposes have changed."



“

A country may have an ID that doesn't expire, for example. We [have to] learn every different country's rules and regulations of what's an acceptable document, what their passports and driver's licenses look like.

”

Any large transaction that is not in client transaction history may warrant further exploration, as is the case at all financial institutions.

“Similarly, we may reach out to the client to determine the reason for the transaction for both the client's and BitGo's protection.”

Warning signs for suspicious activity largely revolve around transaction values, he said. Any unusually large payment is cause for suspicion, at which point BitGo will personally check in with the customer to find out its purpose.

“During onboarding we'll ask what they think their transaction volume is, and if it exceeds

that, we'll reach back out and ask what this transaction is about, as it is not in line with [their] normal scope of business,” he noted. “If their business has changed in the last six months and led to a transaction volume change, we'll want to know the business case for that: ‘How has that changed? Where are the sources of those funds?’”

The double-layered AML/KYC system is crucial for ensuring that all BitGo customers remain aboveboard and that money launderers cannot go undetected on its service. Any single defensive layer is difficult to get around, but circumventing both is next to impossible.

News & TRENDS

AML/KYC TRENDS

More than half of cryptocurrency exchanges have weak or no KYC systems

Proper AML/KYC procedures are critical when conducting transactions to ensure that customers are who they say they are and that the funds in question are not being used for illicit purposes. A whole segment of transacting services misses the mark on these crucial processes, however: cryptocurrency exchanges. A recent [study](#) found that 56 percent of these exchanges do not follow any sort of KYC guidelines, resulting in weak or nonexistent verification systems that do little to prevent money laundering. Many of the exchanges with weak systems fail to mention any country of origin on their websites or in any of their terms and conditions, apparently in a deliberate attempt to avoid adherence to any regulations.

These deficient exchanges are located around the world, with Russia, the United Kingdom and the United States having the highest number with lax KYC protocols. Seychelles is also a potential nest for money laundering, with 85 percent of the country's exchanges failing to have proper KYC processes.

Financial decision-makers have low trust in automated AML systems, study finds

AML automation is a breakthrough technology for many businesses, enabling them to be compliant with federal regulations while avoiding the tedious and expensive manual effort of inspecting every transaction for potential violations. A recent [study](#) found that 47 percent of senior decision-makers at a variety of companies have some level of distrust in automated authentication procedures, however, with 21 percent saying



that they do not trust them at all. This distrust is reflected in usage rates among businesses, 23 percent of which lack any sort of automated AML processes.

Accountants tend to have more trust in automation than most career fields, with 32 percent

saying they fully trust automated systems. Most businesses use some form of automated customer authentication due to its cost-saving nature, however, with almost 80 percent of businesses now utilizing electronic AML checks.

NEW CRYPTOCURRENCY KYC INNOVATIONS

Metal Pay integrates Trulioo onboarding solution for fast account opening, AML/KYC compliance

Some cryptocurrency players are meeting demand for improved AML/KYC compliance by partnering with third-party providers to more effectively onboard their users. One example is U.S.-based cryptocurrency exchange platform Metal Pay, which recently [teamed up](#) with Trulioo to integrate the latter's onboarding solution to comply with the strict AML/KYC regulations required for money service providers of all types. Metal Pay needed a solution that was able to function in multiple global markets and had the capacity for quick expansion while simultaneously providing customers with faster experiences, according to Trulioo. Metal Pay currently operates in 24 countries and is compatible with more than 30 different cryptocurrencies.

BitMEX strengthens AML measures in wake of criminal noncompliance charges

Another cryptocurrency trading platform aiming to improve its AML/KYC procedures is bitcoin exchange BitMEX, which recently [implemented](#) a new risk assessment system to oversee trades and scan them for potential malfeasance. The exchange also plans to unveil a new user

Almost
80%
of businesses now
utilize electronic
AML checks.

authentication program to ensure that bad actors cannot set foot on its platform and use it for money laundering, according to its chief compliance officer, Malcolm Wright. Existing users who do not complete the platform's new KYC program will be unable to withdraw funds after December 4.

This implementation comes soon after the U.S. Commodity Futures Trading Commission leveled charges against BitMEX for violating AML

regulations and operating as an unregistered trading platform. The Department of Justice also charged BitMEX with violating the Bank Secrecy Act by failing to implement AML and KYC measures, which the platform hopes to improve with its new system. The legal proceedings are still ongoing, but BitMEX has so far denied the allegations.

REGULATORS CRACK DOWN ON CRYPTOCURRENCY KYC

FinCEN fines two bitcoin mixing websites \$60 million for AML violations

One common practice among cryptocurrency users is “mixing,” in which users mix their currencies in a pool with other users and then withdraw the same amount they put in to obscure the link between their blockchain identifiers and their real-life identities. These mixing websites are still subject to the AML/KYC laws imposed on exchanges, however, as the owner of two mixing services recently found out when the U.S. Treasury Department’s Financial Crimes Enforcement Network (FinCEN) [fined](#) him \$60 million for violating AML regulations. The agency attests that the owner violated the Bank Secrecy Act by operating an unregistered money service business, marking the first time FinCEN has levied fines against a cryptocurrency site.

FinCEN further alleges that the owner advertised his sites’ mixing services on various dark web forums, marketing his business to narcotics traffickers, counterfeiters and other fraudsters. Just one of his exchanges processed \$311 million through 365,000 transactions between June 2014 and December 2017, FinCEN noted in its report. The owner will face federal criminal charges in addition to the fine, including money laundering, operating an unlicensed money transmitting business and conducting money transmission without a license.

Cryptocurrency exchanges met with growing distrust by banks, study finds

Cryptocurrencies have skyrocketed in popularity since bitcoin was introduced 11 years ago, with a variety of names like ethereum and dogecoin joining the space in subsequent years. They may be well-known among tech-savvy consumers, but a sense of distrust for virtual currencies is growing among established FIs, according to a recent joint [survey](#) of financial experts by ACAMS, RUSI and YouGov. A full 88 percent of respondents said that cryptocurrencies aid in money laundering and only 9 percent feel the cryptocurrency sector is doing enough to combat this. Cryptocurrency users appear to disagree, with only 56 percent of users expressing

concern with money laundering and 48 percent saying that fraud is being sufficiently fought.

World governments also widely distrust the security and compliance standards of cryptocurrency exchanges. Eighty-nine percent of government-employed experts surveyed said that cryptocurrencies play a key role in dark web transactions, as opposed to 50 percent of users who said the same.

AML COMPLIANCE IN OTHER INDUSTRIES

Banks face various AML/KYC compliance challenges, studies find

Challenges with AML/KYC compliance regulations are not confined to cryptocurrency exchanges, with traditional FIs experiencing speed bumps as well. Forty-seven percent of American banks in a recent [study](#) reported that



regulatory compliance is their primary challenge in 2020, with 40 percent of European banks reporting the same. The biggest reason cited for this struggle is that the workload for meeting AML/KYC compliance regulations is often distributed among multiple teams, which have to do redundant work and effectively communicate with one another when onboarding new customers. Experts say that all AML/KYC compliance duties should ideally be conducted by a single, dedicated team, but this is a pipe dream for many FIs.

Another perennial issue is the extended period of time it often takes to onboard customers. A second [study](#) found that it can take up to 25 hours to onboard a single high-risk entity, in large part due to subpar data management practices. A third [study](#) reported that 81 percent of decision-makers at FIs said poor data management lengthens onboarding times and negatively impacts customer experiences.

Compliance professionals expect ML will play a crucial role in AML/KYC compliance

One way to potentially smooth over the frictions associated with AML/KYC compliance is through machine learning (ML) technology, according to a recent joint [survey](#) from *Compliance Week*, Guidehouse and the International Compliance Association (ICA). Eighty percent of the 364 compliance professionals surveyed said that ML

It can take up to
25 hours
to onboard a single
high-risk entity.

could potentially reduce compliance risk, with 61 percent reporting that they had already seen results in this field through the use of ML. These ML applications are in place at several banks, with nearly two-thirds of FIs devoting up to \$1 million to ML and 71 percent developing their own in-house applications.

The top perceived benefit of ML applications was improving KYC processes, according to 55 percent of respondents, with the technology enabling both faster decision-making and more

accurate risk assessments. ML programs take a significant amount of time to get off the ground, however, with the average application requiring between six and 12 months to launch and modify to a bank's particular needs and customer base.

Experts predict automation, perpetual KYC and other technologies to dominate AML/KYC field in the future

The AML/KYC field is continually evolving, both to introduce new technologies and to respond to new techniques being deployed by money launderers. One trend industry experts expect to play a larger role in the future is [perpetual KYC](#), which differs from traditional KYC in that it constantly monitors customer details rather than scanning them once at onboarding or periodically every few years. This can provide much more current data about customer habits, potentially detecting signs of wrongdoing and providing opportunities for personalization of new products or services.

Another emerging trend is automation technology that harnesses AI or ML to reduce some of the burden on human professionals. These systems will likely take advantage of large and open data sets cobbled together by many different compliance companies and regulators instead of solely relying on in-house data. This has the potential to provide much more accurate AML and KYC screening among all organizations using and contributing to this database.

AML/KYC compliance to cost financial firms \$42 billion in US and Canada in 2020

New technologies and investments can make compliance professionals' lives much easier, but they can also be extremely pricey. A recent [study](#) found that compliance at American and Canadian financial firms is expected to cost \$42 billion this year, with the U.S. spending \$35.2 billion and Canada spending \$6.8 billion. This represents a 33 percent increase over spending in 2019, according to the report, but it is still peanuts compared to financial crime compliance costs in Europe, which totaled \$137 billion last year.

This increase in compliance costs is due to both investments in new technologies and added complexity resulting from the pandemic. Conducting AML and KYC procedures remotely requires more time and effort to ensure that electronically filed documents are correct and legible. FIs are also handling a higher volume of smaller transactions rather than a smaller number of large transactions, leading to bigger costs eating away at roughly the same amount of profit.

Nevada faces new urgency for AML/KYC in cashless gambling

Casinos, cardrooms, racetracks and other gambling establishments have long been associated with money laundering, and the growing popularity of online gambling has brought this association to cyberspace. Several states [approved](#) an expansion of online gambling in the

November election, encroaching on Nevada's traditional seat as the gambling capital of America. Customers are likely to turn to new online gambling operations in other states like Colorado, Nebraska and Virginia if they feel they are safer than Nevada's operations, said Brendan Bussman, director of government affairs at Global Market Advisors, making AML/

KYC compliance a prime issue for the Nevada legislature to consider when it reconvenes in February. Nevada approved a bill in June that imposes stricter regulations on AML/KYC compliance for cashless transactions in the state, but this new paradigm does not yet apply to gambling operations.



DEEP DIVE

Cracking Down On Cryptocurrency Exchange Cybercrime With AML/KYC Compliance

Cryptocurrency is one of the fastest-moving industries in the digital world, with a market that was [valued](#) at \$1.03 billion in 2019 and is projected to reach \$1.4 billion by 2024 at a compound annual growth rate (CAGR) of 6.18 percent. Bitcoin is one of the most famous names in the cryptocurrency space, [accounting](#) for \$6 billion in daily transactions among 153 million registered user addresses. The currency is well-known for its massive value fluctuations as a single bitcoin cost just 9 cents in 2010, \$313.92 in 2015 and a staggering \$13,421.44 in 2018 before sharply decreasing to \$3,869.47 in 2019. Thousands of other cryptocurrencies began circulating on crypto exchanges in recent

years, such as ethereum, monero and ripple, many of which leverage blockchain technology to serve as a transaction database.

These various cryptocurrencies are also widely known for their roles in cybercrime, be it in their direct theft or in their use for laundering ill-gotten funds from other schemes. Cryptocurrency-related crimes [totaled](#) \$4.3 billion in 2019 — a larger sum than in 2017 and 2018 combined. The same year saw \$2.8 billion in laundered money [flow](#) through cryptocurrency exchanges, increasing from \$1 billion in 2018.

Government regulators and cryptocurrency exchanges are frantically looking for ways to regulate and prevent the laundering of stolen money through cryptocurrencies, with some methods showing more promise than others. The following Deep Dive explores how cybercriminals leverage cryptocurrency exchanges for money laundering and how government agencies are cracking down on exchanges that let launderers run amok.

How money launderers exploit cryptocurrency

Cryptocurrencies are popular for transactions in which users desire anonymity, such as when purchasing illicit drugs or adult material, and it is this same anonymity that makes them popular for money laundering. All transactions are logged in to the blockchain, but these are typically made under pseudonyms or usernames that are difficult to link to actual identities. This lack of identity information is compounded by many cryptocurrency exchanges' weak KYC procedures, with a recent [study](#) finding that 56 percent of all exchanges lacked sufficient KYC processes, often on purpose to avoid complying with AML regulations. Most of these poorly protected exchanges are located in Russia, the U.K. or the U.S., but some countries, like Seychelles and Singapore, lack KYC procedures on a large majority of their exchanges, making them hotbeds for money laundering and other cybercrimes.

Financial regulators, financial intelligence units and many cryptocurrency exchanges are expressing growing concern about the increased use of cryptocurrencies for committing cybercrimes. Seventy percent of respondents in a recent [survey](#) said that criminal activity was a top concern for professionals in the global cryptocurrency and financial industries, and such

activities take a variety of forms. Respondents said they were most concerned about money laundering at 84 percent, followed by 79 percent who were concerned about the use of cryptocurrencies to fund terrorist groups and 76 percent who were worried about their use in funding human trafficking. There was a notable gulf in opinion when it came to perceptions of cryptocurrencies' risks, however: 63 percent of banks and 56 percent of governments felt cryptocurrencies posed a significant cybercrime risk as opposed to only 9 percent of cryptocurrency industry professionals.

This gap in opinion means that any improvement in cryptocurrency exchange AML/KYC procedures will likely come about through regulatory orders rather than reliance on exchanges taking initiative.

Enforcing AML/KYC compliance at cryptocurrency exchanges

World governments have already taken a number of steps to curb money laundering on cryptocurrency exchanges by requiring them to bring their KYC processes in line with those of other FIs. FinCEN [announced](#) in November 2019 that it would begin strictly enforcing the "travel rule" for cryptocurrency exchanges. This rule forces exchanges to verify customers' true identities as well as identify any senders and recipients of cryptocurrency transfers worth \$3,000 or more.



It was originally put into place in 2013 but was only intermittently enforced over the next six years, letting many cryptocurrency exchanges continue their KYC-less practices with impunity.

The U.S. government worked to curb cryptocurrency exchanges' lax AML procedures in the same year, following the example set by other financial regulatory agencies around the world. FinCEN [charged](#) the owner of a privately owned exchange with violating the Bank Secrecy Act by failing to report more than 150 transactions that were each worth more than \$10,000 and thus required a Currency Transaction Report to be sent to the Treasury. The owner of the exchange

was forced to pay a \$35,000 fine and was prohibited from ever running a money transmission service again, sending a firm warning to other cryptocurrency exchanges about the consequences of failing to comply with AML and KYC requirements.

Cryptocurrency exchanges are therefore taking their AML/KYC compliance more seriously and even partnering with third parties to help root out potential money launderers. Exchanges wishing to provide a secure customer experience and avoid punishment from federal authorities would do well to follow this example.

A B O U T

PYMNTS.com

[PYMNTS.com](https://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](https://trulioo.com), 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 feedback@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.

AML/KYC Tracker® is a registered trademark of What's Next Media & Analytics, LLC ("PYMNTS.com").