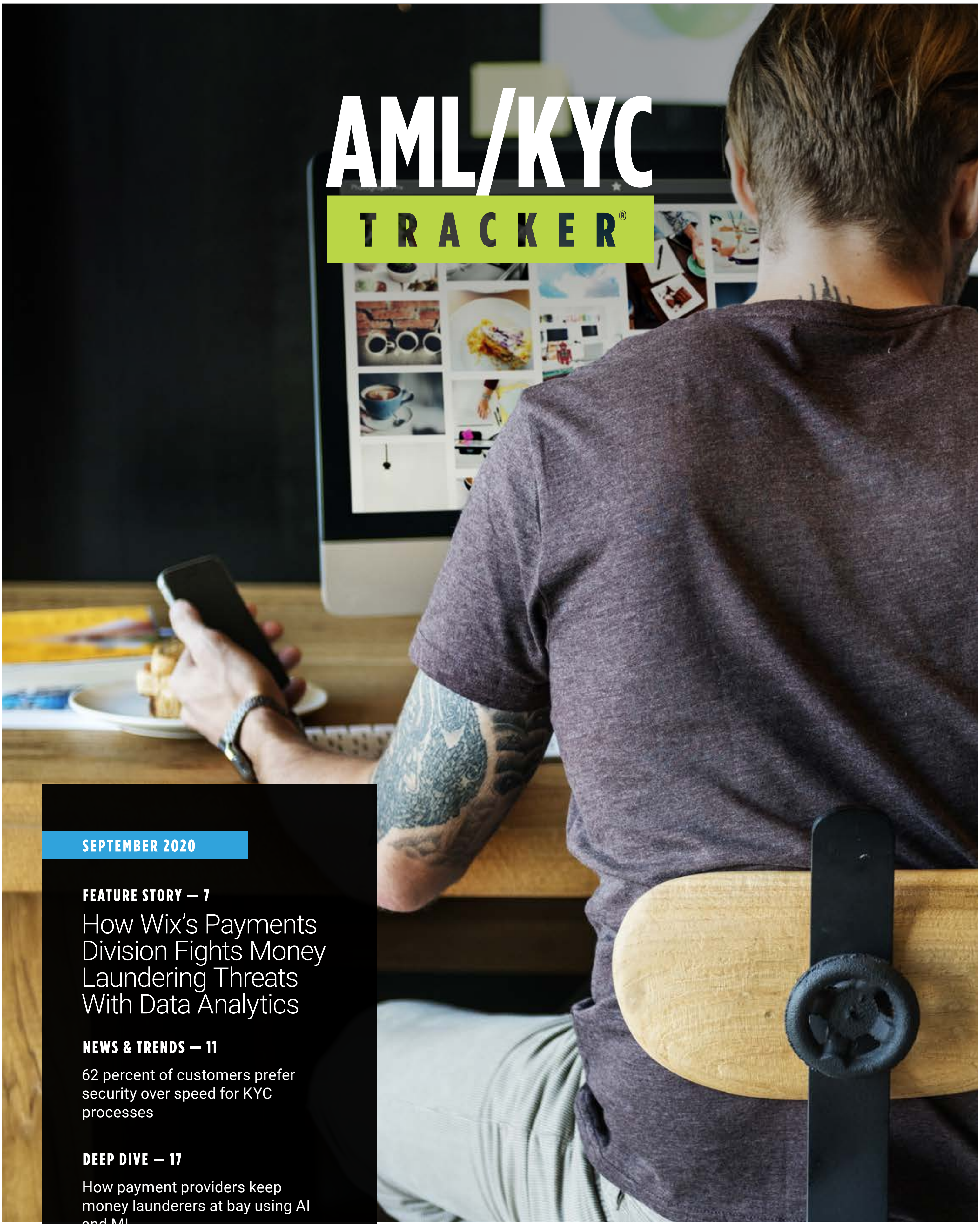


AML/KYC TRACKER®

SEPTEMBER 2020

Trulioo | PYMNTS.com

Table Of CONTENTS

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

Money laundering is a perennial criminal threat as the funds fraudsters steal from their victims often cannot be spent outright without arousing suspicion from government authorities. The United Nations estimates that up to $2 trillion — or 5 percent of the global gross domestic product (GDP) — is laundered each year, with criminals leveraging tactics as basic as exchanging gift cards and as elaborate as setting up brick-and-mortar businesses through which they can funnel cash.

The digital age has enticed many money launderers to move their schemes online, enabling them to use payment providers, eCommerce storefronts and cryptocurrencies to convert their ill-gotten gains into spendable, suspicion-free cash. Approximately $2.8 billion was laundered through cryptocurrencies in 2019, for example — up from $1 billion the year before. Other cybercriminals rely on transaction laundering, in which online businesses are used as fronts and transactions are modified to include illicit cash. Reports have pegged this method at costing $200 billion annually in the United States.

Preventing cybercriminals from abusing their systems is often incentive enough for banks, FinTechs and payment providers to crack down on money laundering, but government oversight can also keep financial institutions (FIs) honest. FIs — including large players like Commonwealth Bank of Australia, Deustche Bank and Goldman Sachs — were fined more than $17 billion between 2009 and 2019 for improper anti-money laundering (AML) procedures.

FIs, payment providers and FinTechs are deploying numerous technologies to keep money launderers away from their services and to keep oversight agencies off their backs, including artificial intelligence (AI) and data analytics. Such tools may be unable to completely stop money laundering, but they could frustrate these fraudsters enough to send them looking for easier fronts.

Around the AML and KYC world

Banks, FinTechs and payment providers around the world recognize the benefits of using AI for AML efforts, and FIs in Hong Kong appear particularly knowledgeable about what the technology can offer. A recent survey of Hong Kong banks found that 83 percent believe that utilizing AI will strengthen their AML procedures, although AI's adoption has been slow because of the difficulty in modifying their legacy systems. Ninety-one percent of the city's banks still use older, rules-based systems, but they are becoming aware of such solutions' flaws.

AI is especially handy in easing the frictions customers face when applying for accounts or services online, where stringent and often-intrusive AML and know your customer (KYC) procedures cause many to abandon the processes. A recent study found that almost half of all U.S. consumers have abandoned an online account opening process in the past year because they thought it was too difficult or untrustworthy — an increase from the 37 percent of consumers who said the same the previous year. Two-thirds of respondents also felt that companies did not adequately protect their personal information.

Consumers may find it frustrating to encounter difficulties in account opening, but they do recognize the need for ironclad security. A recent study from identity verification provider Trulioo found that 62 percent of consumers prefer onboarding experiences that prioritize security over speed across all industries except online gaming. All customers were displeased with poor account opening experiences, with 73 percent of consumers saying they have become less tolerant of these deficiencies over the past few years.

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

How Wix Payments strikes its KYC, AML balance

Knowing money launderers' typical techniques is crucial for payments providers, but knowing customers' and merchants' typical spending habits is just as important — if not more so — to detect anomalies. Wix Payments, the payments arm of web development company Wix, leverages AI and machine learning (ML) to this end, according to the division's co-heads, Amit Sagiv and Volodymyr Tsukur, but AML has a number of intrinsic challenges. In this month's Feature Story (p. 7), PYMNTS talked with Sagiv and Tsukur about how AML and KYC procedures need to be ironclad but also easy to comply with for a wide range of customers.

Deep Dive: Slowing down money laundering via AI and ML

eCommerce has become the new normal during the COVID-19 pandemic, with the industry expected to generate $4.5 trillion annually by next year. The payments processors that serve these online marketplaces are common targets for money laundering schemes, however, with cybercriminals leveraging front companies and transaction laundering tactics to process their ill-gotten funds. This month's Deep Dive (p. 17) explores how fraudsters take advantage of eCommerce payment providers and how these companies deploy AI and ML to identify suspicious transactions and stop launderers from making clean getaways.

Executive INSIGHT

Half of all U.S. consumers have abandoned account creation due to excessive friction from KYC checks. How can merchants keep these processes secure yet simple enough to retain customers?

"Identity verification plays a crucial role in helping organizations keep fraudsters away. However, as identity thieves grow more sophisticated, so do identity verification technologies. Merchants need to strengthen identity verification and fraud prevention techniques without adding too much friction to the customer onboarding process. New tools have emerged to help companies unequivocally answer the question '[Are these customers] who they say they are?' before moving forward with authorizing a transaction.

To ensure efficiency without unnecessary friction during the onboarding process, merchants should take a holistic approach through a digital identity network — a marketplace of hundreds of data sources, verification processes and tools that leverage network data intelligence to verify and authenticate identities online. Having a layered approach can help set the level of safety checks needed to verify an individual or a business while meeting AML and KYC regulations. Risk is reduced each time a layer is added.

This layered approach is validated by consumers. In fact, a recent survey commissioned by Trulioo found that 89 percent of consumers say a secure account creation process that validates their identit[ies] and protects against fraud and identity theft is very important.

The key to balancing safety and first-class customer experience is basing the selection of your identity verification provider on versatility — a solution that is flexible and allows merchants to change continuously without disrupting their onboarding process[es]."

ZAC COHEN

chief operating officer at Trulioo

FIVE FAST FACTS 5

83%

Share of Hong Kong banks that think AI can strengthen their AML procedures

50%

Approximate portion of U.S. consumers who have abandoned account creation processes due to friction

73%

Share of consumers who have become less tolerant of lackluster account opening procedures

$5.6B

Total penalties levied against banks so far this year for noncompliance with AML and KYC regulations

$200B

Annual amount laundered via transaction laundering in the U.S.

Feature STORY

HOW WIX'S PAYMENTS DIVISION FIGHTS MONEY LAUNDERING THREATS WITH DATA ANALYTICS

Money laundering is a never-ending threat to payments providers of all types, but especially to those that operate online. Verifying users' identities and the legitimacy of their business is exceptionally difficult in cyberspace, and fraudsters are taking full advantage of this challenge to process more than $200 billion in ill-gotten gains each year.

Payments providers are constantly exploring new ways to protect themselves and their merchant partners from fraudsters aiming to exploit them for the purpose of money laundering. Not only could both parties end up losing millions in false transactions, but they could also face a crackdown from government oversight agencies for not doing enough to keep launderers off their platforms. It is ultimately up to the payments provider to be the first line of defense.

"Since we are acting in the financial space, there's a lot of regulation that everybody needs to follow," said Amit Sagiv, co-head of Wix Payments, the payments processing arm of web development company Wix. "We have shared responsibility with our partners. They are taking most of the burden, but because we provide the [payments] service, we want to make sure that we do not let fraudsters come in."

In a recent interview with PYMNTS, Sagiv and his fellow co-head Volodymyr Tsukur offered an inside look at the money laundering threats that Wix faces in its daily business and how the firm and other payments processors keep a close eye on their merchant partners and lookout for any signs of suspicious activity.

The money laundering threat

"Know thine enemy" is the first rule of any fraud or money laundering prevention system, with payments providers of all types requiring an intimate knowledge of the threat they face if they have any hope of countering it. Money launderers typically come in one of two categories, according to Tsukur.

"First of all, there is what we call the merchant risk," he explained. "We know that fraudsters would like to hack the platform either for money laundering or to use stolen cards, looking for a way to swipe them virtually and get this money and then run away."

The second main threat is transaction laundering, which consists of buyers rather than merchants, said Tsukur. Their end goal is largely the same, primarily targeting payments providers to test or use their stolen credit cards. Wix's solution is the same in either case: a combination of in-depth knowledge of its customers' and partners' histories paired with analytics technology to identify questionable transactions.

Preventing money laundering analytically

The importance of understanding the habits of potential fraudsters is equal to that of recognizing legitimate customers. Having a detailed and holistic view of customers' typical transactions helps payments processors identify and flag unusual ones that could be the result of money laundering, according to Sagiv.

"We know what they're about to sell, what products they added and removed; we know where they're doing their marketing," he said. "So it's a 360-degree overview from both the buyer perspective and the merchant perspective, and with all the data points that we're collecting, we could really pinpoint the [merchants] that should be expelled from the platform."

This analysis is aided by Wix's AI and ML algorithms, which can pinpoint the unusual transactions and flag them for further analysis. These algorithms grow smarter over time, allowing Wix to catch up with money launderers' evolving techniques.

"It creates a smart model that we will teach based on our user data," Tsukur explained. "With this engine, we have a streamlined KYC process that can approve merchants within seconds."

KYC and AML measures come with their fair share of obstacles, however. Not only do these procedures have to be seamless for the convenience of legitimate customers, but they also have to account for the fact that many of their merchant partners are unfamiliar with the intricacies of AML.

Challenges in AML

The most crucial consideration when developing an AML strategy, according to Tsukur, is ensuring that the process is frictionless for legitimate customers, who may have little patience for needless checks when conducting payments. The secret is to start the AML procedure long before payments are processed.

"We don't start at the moment of payment; we start way ahead of time," Sagiv said. "We use our data [analytics system] to ensure that you have a very smooth process, so we would collect your information [beforehand] and whatever document is regulatory-required, and then we will scan you."

The other primary challenge is ensuring that the AML and KYC procedures work for all of Wix's customers as many of them are smaller merchants without the compliance resources of a large company. This means that all KYC checks have to be easy to understand and comply with, or else merchants might take their business elsewhere.

"We serve so many kinds of merchants, selling anything from glasses to virtual games to bookings for restaurants and events," Tsukur noted. "We needed the KYC process to be first and foremost simple, digestible and understood by mom-and-pops building their own businesses in their garage, and this is a huge challenge."

Failure to meet this challenge could mean lost business or, even worse, a potential money launderer slipping through the cracks. Businesses like Wix will need their AML and KYC procedures to strike the right balance between usability and security, or not only will they see launderers flock to their business but they could also face severe penalties for letting them do so.

News & TRENDS

AML/KYC TRENDS

83 percent of Hong Kong banks favor AI for AML

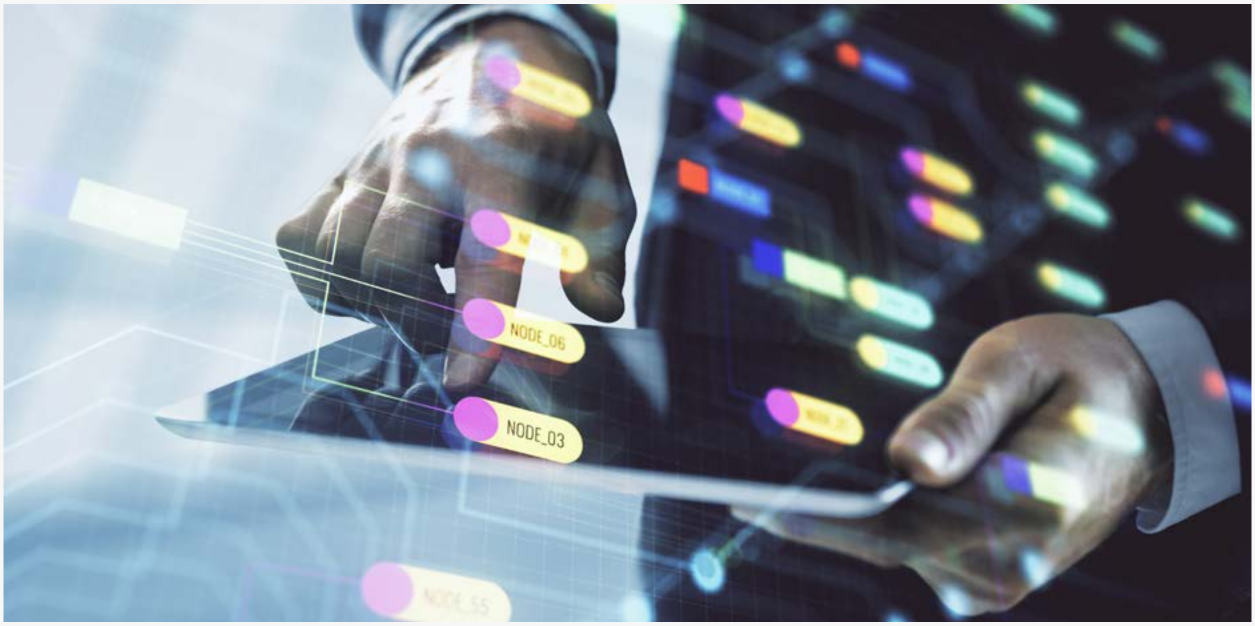
The use of AI in AML has been growing steadily more popular over the past several years and the technology's benefits have become widely recognized. A recent survey from global analytics software firm FICO found that 83 percent of Hong Kong banks think utilizing AI will strengthen their AML procedures, even though 91 percent still value existing rules-based systems for this purpose. These FIs are well aware of the flaws in their older systems, however, with many saying they are difficult to modify based on new technologies and threats.

Banks typically combine AI and rules-based systems to fight financial fraud without dramatically altering their operations, according to Timothy Choon, FICO's financial crimes leader in the Asia-Pacific region. The survey found that most multinational banks are deploying third-party AML solutions while domestic banks are likelier to leverage in-house systems.

Taiwanese banks skeptical of AI's benefits, study finds

AI's benefits for AML and KYC procedures are evidently being viewed with much more skepticism in Taiwan. Another FICO study found that only 30 percent of Taiwanese banks feel implementing AI would improve their AML efforts, with 64 percent favoring older, rules-based systems. Many Taiwanese banks are cognizant of these systems' shortcomings, however, with 26 percent acknowledging that they face significant challenges in modifying and updating them. Such issues can result in an inability to meet new compliance requirements and difficulty in addressing updated regulations.

These banks are nonetheless allocating vast sums for fighting money laundering. Eighty-three percent say they plan to invest in financial crime compliance in the coming year, with 9 percent



planning to significantly boost their investments. Many are emphasizing AML strategies that do not affect customers' experiences, with 17 percent citing this as a primary factor in their plans.

Half of US customers have abandoned account sign-ups due to friction

FIs' emphases on consumers' experiences are well-founded as customers are willing to abandon banks or businesses entirely if they feel their onboarding processes are too obstructive. A recent study found that almost half of all U.S. consumers have abandoned an online account opening process because they thought it was too difficult or untrustworthy. This represents a failure on the part of KYC initiatives, which must ensure potential customers are legitimate without driving them away.

The increase in account opening abandonment is up from last year, when the same study found that just 37 percent of consumers reported doing so. Two-thirds also felt that companies did not adequately protect their personal information, but more are starting to take action to safeguard their own details. The share of customers using two-factor authentication (2FA) is now at 35 percent, for example, compared to the 26 percent who reported doing so last year and the 19 percent who said the same in 2018.

Customers prefer slower but more secure identity verification processes, study finds

New research also suggests that customers are willing to undertake longer account creation processes if they are assured of their security. A recent study from identity verification provider Trulioo found that 62 percent of consumers prefer security over speed, favoring slower yet more safeguarded onboarding approaches over quicker processes with fewer checks. This trend extended across various generations, genders and industries with the exception of online gaming, where 53 percent of respondents valued speed over security.

Respondents expressed frustration with poor account opening experiences, however, with 73 percent saying that they have grown less tolerant of subpar onboarding procedures over time. This means that banks and other businesses must walk a fine line between security and convenience, though they must make sure to provide enjoyable experiences to avoid losing potential customers the moment their journeys begin.

Bank executives plan to improve security and reduce friction in account opening processes

Bank executives' values also appear to align with those of their customers when it comes to security, seamlessness and customer verification. A recent study of 100 bank leaders found that 80 percent cited streamlining customers' experiences as their main objective, with 60 percent reporting that failing to do so was the primary reason applicants abandoned the process.

The study also determined that security is vital, with 85 percent of respondents reporting that they experienced fraud when onboarding potential customers. Forty-nine percent admitted that their account opening procedures were not secure or only somewhat so, with 72 percent planning to reduce their application fraud losses.

62%

of consumers prefer security over speed

Legacy systems and manual identity verification processes were some of the top reasons executives gave for having suboptimal fraud detection procedures.

SMBs show strong interest in operating online marketplaces, study finds

A greater number of SMBs that traditionally did not operate online are beginning to express interest in doing so, especially as the COVID-19 pandemic shrinks or cuts off their in-person revenue streams. A recent joint study from PYMNTS and Visa found that 60 percent of SMBs that are not leveraging online marketplaces are interested in doing so, while 62 percent of businesses said that they were already taking their product offerings online. Sixty percent of the businesses currently selling online said that they would move their business to a provider that offers real-time settlement as many face cash flow issues due to not receiving their payments on time. Seventy-six percent of surveyed businesses said they had experienced cash shortages, with 27 percent saying they had to wait up to five days for their payments.

Study shows businesses are growing confident that they will weather the pandemic

The ongoing pandemic has been a grueling affair for businesses of all sizes, especially smaller firms that do not have the cash on hand to weather revenue shortages. Those that have gotten through the crisis so far are growing more confident that they will survive the entire pandemic, however, with 54 percent of respondents to PYMNTS' Main Street business survey saying they will endure. Almost one-quarter of SMBs even say they are in better financial shape than they were in the pandemic's early months.

There are some caveats to this news, however, with confident businesses largely consisting of those that were in good shape to begin with. The survey found that 69 percent of confident respondents were not very concerned that their business would fail early on during the pandemic. Only 30 percent of those that feared closure in March had changed their minds about their fears of going under.

AML/KYC OVERSIGHT DEVELOPMENTS

World's banks face $5.6 billion in AML/KYC violations so far this year

Failing to comply with AML and KYC best practices can net banks massive penalties from government oversight agencies in addition to potential fraud losses. FIs around the world faced more than $5.6 billion in such fines as of July, according to a recent study, with those in Germany, Israel, Sweden and the U.S. among the individual countries hit especially hard. Three

Swedish banks saw $536 million in penalties for insufficient AML procedures in the Baltic countries while the U.S. Department of Justice (DOJ) and other authorities exacted a $900 million fine against an Israeli bank for concealing more than $7.6 billion in various bank accounts. Countries in the Asia-Pacific region together accounted for just under $4 billion in fines, with Pakistan and Hong Kong seeing the biggest increases in fines since last year at 845 percent and 223 percent, respectively.

Feds crack down on credit card laundering

The DOJ and the Federal Trade Commission (FTC) are cracking down on a new type of scam called credit card laundering or transaction laundering. Such schemes entail fraudsters setting up websites that appear to be legitimate businesses but are actually fronts that facilitate the purchase of illicit goods. The pandemic-driven surge in eCommerce has made these scams more prevalent than ever as payment processing companies deal with massive influxes of new customers and cannot devote as much time to the AML and KYC processes of each company with which they do business.

The U.S. government is focusing on payment providers that serve as the middlemen between FIs and illegitimate businesses as well as the businesses themselves. Industry groups, such as the Electronic Transaction Association, are working with the DOJ and FTC to shut down these illicit businesses. Jodie Kelley, the association's CEO, told *The Wall Street Journal* that the organization's payments processors kicked out

more than 10,000 of their merchants in 2017 for money laundering.

Ireland belatedly adopts EU AML regulations

AML regulations are being strengthened overseas as well. Ireland officially adopted the European Union's framework for AML and anti-terrorism financing several years after the rest of the region was brought on board. The EU officially passed the Fifth Anti-Money Laundering Directive (5AMLD) in July 2018 and gave its member states until January 2020 to comply with the directive, fining Ireland €2 million ($2.3 million USD) in July for not doing so. The Irish Cabinet voted on Aug. 10 to comply with the directive.

The regulations bring the AML rules governing virtual currency and mobile wallet providers in line with those that apply to the rest of Europe's FIs. Helen McEntee, Ireland's minister for justice and equality, stated that the move was good for the safety of the nation as well as Europe, noting that the EU's open borders make it only as secure as its weakest member.

HOW THE PANDEMIC IS AFFECTING MONEY LAUNDERING

Cybercriminals alter their tactics during the COVID-19 pandemic

The COVID-19 pandemic has significantly affected life for individuals around the world, and cybercriminals are no exception. United Kingdom-based defense and security think tank RUSI said business closures due to social distancing and stay-at-home orders have limited many of the money laundering schemes criminals can deploy. This is forcing bad actors to process their finances via digital methods, which is putting the onus on online payments processors and businesses to monitor for suspicious surges in activity.

The United Nations Office on Drugs and Crime estimates that between $800 billion and $2 trillion is laundered globally every year, with just 1 percent of these funds ultimately identified and seized. Businesses' current AML tools are being pushed to the limit as much of this laundering moves online. Some of the most successful methods being used to curtail these illicit activities involve AI, but experts warn that such systems must be paired with human fraud analysis teams to ensure that the technology does not report too many false positives.

DEEP DIVE

How eCommerce Payments Providers Sniff Out Money Launderers

eCommerce has exploded in popularity over the past 20 years, with online giants like Amazon, eBay and big-box retailers' marketplaces becoming consumers' go-to alternatives to brick-and-mortar merchants. The industry is expected to generate $4.5 trillion annually by 2021, though the vast majority of eTailers are not the industry-defining giants that have driven many mom-and-pop retailers out of business. Fewer than 1 million of the 24 million eCommerce sites on the internet generate more than $1,000 a year, with the remainder consisting of minuscule online merchants that struggle to survive.

All eCommerce sites and payment providers have one thing in common no matter their size: the constant and pervasive threat of money launderers using their businesses to process ill-gotten gains, conceal the funds' sources and convert them into clean, taxable income that government authorities cannot track. Money launderers deploy numerous schemes, including transaction laundering and launching front companies, to process and hide their funds from payment providers and law enforcement officials, but payments processors are responding with new technologies that hunt down and report their deeds.

The following Deep Dive explores how money launderers are exploiting eCommerce payment providers as well as how new technologies can detect this illicit activity and deter perpetrators from using payment providers' services as a cover.

Exploiting eCommerce payment providers

Money laundering is a way to convert illicitly gotten funds into legitimate income that can be spent without suspicion. A drug dealer might open up a nail salon, for example, then put his drug money into the salon's cash flow and report it to the Internal Revenue Service as revenue from salon customers. This scheme would allow him to deposit this cash into his bank accounts and provide a plausible explanation for his wealth.

The digital age has prompted a corresponding digital shift in both the crimes that generate stolen funds and the means used to launder them. Transaction laundering, or electronic money laundering, is the most popular type of digital money laundering and involves cybercriminals exploiting payment infrastructures to process their ill-gotten gains. Transaction laundering accounts for $200 billion a year in the U.S.

Three forms of transaction laundering are especially prevalent. The first is front companies, which appear to sell legitimate goods and services but are set up by money launderers to help them fudge receipts, inflate or invent transactions or otherwise misreport their earnings to process their stolen funds. This form is most similar to traditional brick-and-mortar money laundering front businesses but exists in cyberspace instead. It is difficult to detect because it is challenging for authorities to ascertain which goods or services change hands and because the value of many services is subjective.

So-called pass-through companies offer another means of transaction laundering. These businesses are not set up by launderers themselves but allow the cybercriminals to process illicit transactions through their accounts. The third major type of transaction laundering is funnel accounts, which entail payment processors for multiple companies either knowingly or unknowingly processing illicit transactions alongside legal ones. Both of these schemes are difficult for card processors to detect because bad transactions are mixed in with legitimate ones and it is almost impossible to distinguish between the two.

There are dozens of other schemes besides these three, such as selling eVouchers on eCommerce marketplaces and pocketing the profits as legitimate income. These methods all have one thing in common, however. Perpetrators process their funds through thousands of smaller transactions rather than a few larger ones. This means individual transactions are unlikely to pop up on regulators' or tax officials' radars, thus keeping the operations under wraps.

How payment providers stop money laundering

It is incumbent upon the payment providers that process these transactions to detect and stop money laundering as they could be punished if government regulators or law enforcement notice it first and believe they acted negligently or were in on the schemes. There are various warning signs that money laundering could be occuring, including incomplete or inconsistent information, irregular money transfers or payment procedures that appear to be overly complex for no reason. Thousands of transactions occur on an hourly basis, however, making it impossible for human analysts to examine each one for signs of money laundering.

AI could be particularly suited to this task, however. It can analyze thousands of transactions in a fraction of the time it takes human analysts to do so while also drastically reducing the number of false positives. The best AI systems work in tandem with analysts, in fact, sending suspicious transactions to human teams for further review instead of rejecting them outright. This minimizes the amount of time spent combing through innocuous transactions and allows analysts to focus on the ones most likely to be associated with money laundering.

Data analytics is another critical tool that eCommerce payment providers can leverage in their AML efforts. Money laundering — especially that which is conducted online — rarely happens in isolation, and the sheer number of transactions often establishes a pattern that reveals which are used for laundering, be it in a specific geographic region with a specific product type or from customers with a specific occupation. AML staff can develop new rules-based models once they discover these patterns, dividing up transactions based on their likelihood of money laundering and devoting staff's attention to those most apt to be fraudulent.

Money laundering is unlikely to disappear completely as launderers are keen to process their illicit funds wherever money changes hands between businesses or individuals. Technologies like AI or data analytics can help ferret out these transactions and make launderers less likely to use specific services for their deeds, however, sparing payment providers from fraud as well as potential punishment from oversight agencies.

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 feedback@pymnts.com.

AML/KYC TRACKER®

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").