ALTERNATIVE PAYMENTS

TRACKER®

APRIL 2022

PYMNTS.com | Socure

Read the previous edition

MARCH 2022

Alternative Payments Tracker®

ALTERNATIVE PAYMENTS TRACKER®

PYMNTS.com | Socure

ACKNOWLEDGMENT

The Alternative Payments Tracker® was produced in collaboration with Socure, 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.

TABLE OF CONTENTS

EDITOR'S LETTER

Cryptocurrency has offered a roller-coaster ride since its introduction more than a decade ago, fluctuating between extreme highs and lows in value to the surprise, delight and dismay of its investors. As of 2022, it has gained more mainstream recognition than ever before, from A-list celebrities endorsing it in Super Bowl commercials to non-fungible tokens (NFTs) selling for hundreds of thousands of dollars.

This mainstream acceptance belies its still-considerable security risks, however. The United Kingdom, for example, saw more than £146 million ($192 million USD) stolen in cryptocurrency heists in 2021 alone, up 30% from 2020. The cryptocurrency transaction volume associated with illicit activity also jumped from 0.34% in 2020 to 0.62% in 2022. This may seem like a small fraction of the total amount of cryptocurrency changing hands, but a nearly 100% increase in fraud rates should not be discounted.

Stopping this fraud will require diligent user authentication and know your customer (KYC) protocols, but many cryptocurrency exchanges have a long way to go on this front. More than half of all exchanges have no sort of KYC system in place at all, and even those that do often find their security systems sorely lacking. One favorite method is document verification, which fails to accurately assess customers in possession of fake IDs and can be a waste of time for legitimate customers looking to become part of an exchange without necessarily transacting on it.

More seamless and effective authentication methods are necessary to curb fraud and allow cryptocurrency to grow safely in value and popularity. Some exchanges are moving the authentication step to the time of transactions rather than at sign-up, while others are deploying new techniques such as biometrics. Any verification solution would be an improvement to an ecosystem that has traditionally balked at authentication of any kind.

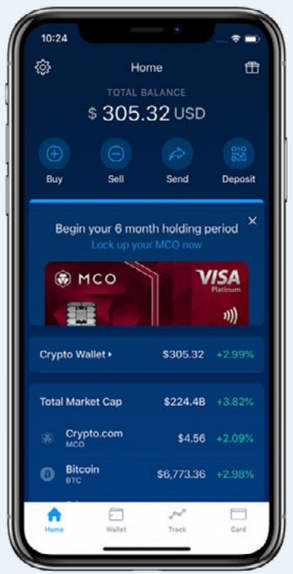
This edition of the Alternative Payments Tracker®, a PYMNTS and Socure collaboration, examines how fraudsters attempt to scam cryptocurrency exchanges, merchants and customers. It also explores how user authentication systems can help businesses reduce fraud without introducing frictions into the customer experience.

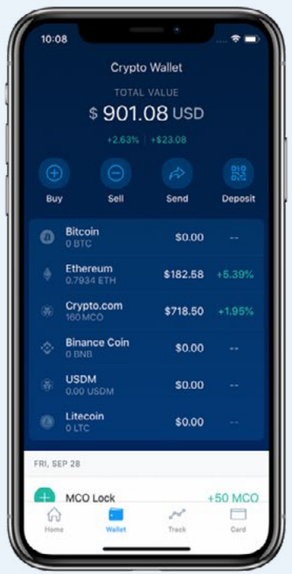
Thought Leadership Team

PYMNTS.com

Feature Story

How crypto.com Verifies Users Without Compromising A Convenient Experience





CRYPTOCURRENCY IS NOW OFFICIALLY IN THE MAINSTREAM,

having completed its evolution from an obscure hobby for computer enthusiasts to a multi-billion-dollar industry with advertisements on national television. Thousands of different cryptocurrencies are now on the market and used for everything from NFTs to Tesla purchases.

Serious concerns remain about the security and fraud issues surrounding cryptocurrency, however, such as account takeovers, money laundering and a range of other complications. These concerns have put a damper on the more widespread acceptance of cryptocurrencies for everyday purchases such as groceries or merchandise, as retailers run the risk of holding the bag if a cybersecurity incident happens on their watch.

"[Just] 4% of surveyed merchants indicated they are equipped to accept crypto as a method of payment today, leaving a significant gap in fulfilling customer interest in crypto commerce," said Eric Anziani, chief operating officer at Crypto.com. "With limited to no opportunity to conduct direct transfers from customer to merchant crypto wallets today, customers are typically forced to take the additional step of converting crypto to fiat before making purchases."

Enhanced cybersecurity measures will be critical to promoting the more widespread use of cryptocurrency. Anziani discussed the most effective ways to do so in a recent interview with PYMNTS.

PROTECTING CRYPTOCURRENCY PAYMENTS

Customer verification must be a tough nut to crack for potential fraudsters while not inconveniencing legitimate customers. To accomplish this, Crypto.com deploys different security measures for its “hot wallets,” which are internet-connected wallets vulnerable to online attacks, and “cold wallets,” which are not connected to the internet and are considered more secure but less convenient with which to transact.

“For hot wallets, it is straightforward, with a 12-word phrase on MetaMask, private and public keys,” said Anziani. “For cold wallets, like Ledger, with whom we have a strategic partnership, there is a 24-word phrase with both private and public keys. Ledger does not have access to the customer funds.”

Many customers prefer to transact through their smartphones, as cryptocurrency values fluctuate quickly and users need immediate access to their wallets. It is critically important that this potentially vulnerable gateway be secured as well.

“For the Crypto app, we use multifactor authentication with a form of biometric authentication and wallet white-listing of external addresses,” said Anziani.

Ensuring cryptocurrency’s security could go a long way toward promoting its more widespread acceptance for everyday purchases. Anziani also offered PYMNTS a glance at what this potential future could look like.

ENSURING A PROSPEROUS CRYPTOCURRENCY FUTURE

Consumers are ready to use cryptocurrency payments, said Anziani, but the problem is that they lack outlets with which to do so. Retailers and payment providers that handle cryptocurrency are seeing a boom in business, however, indicating pent-up consumer demand.

“We know an overwhelming number of customers are interested in purchasing goods or services with cryptocurrencies, [according to a] Crypto.com and Worldpay from FIS study: 75% of more than 110,000 users across geographies and demographics,” Anziani explained. “And despite the current lack of merchant infrastructure to support crypto payments, there continues to be a growth in commerce use cases. For example, approximately 65% of Crypto.com customers use our Crypto.com Visa Card.”

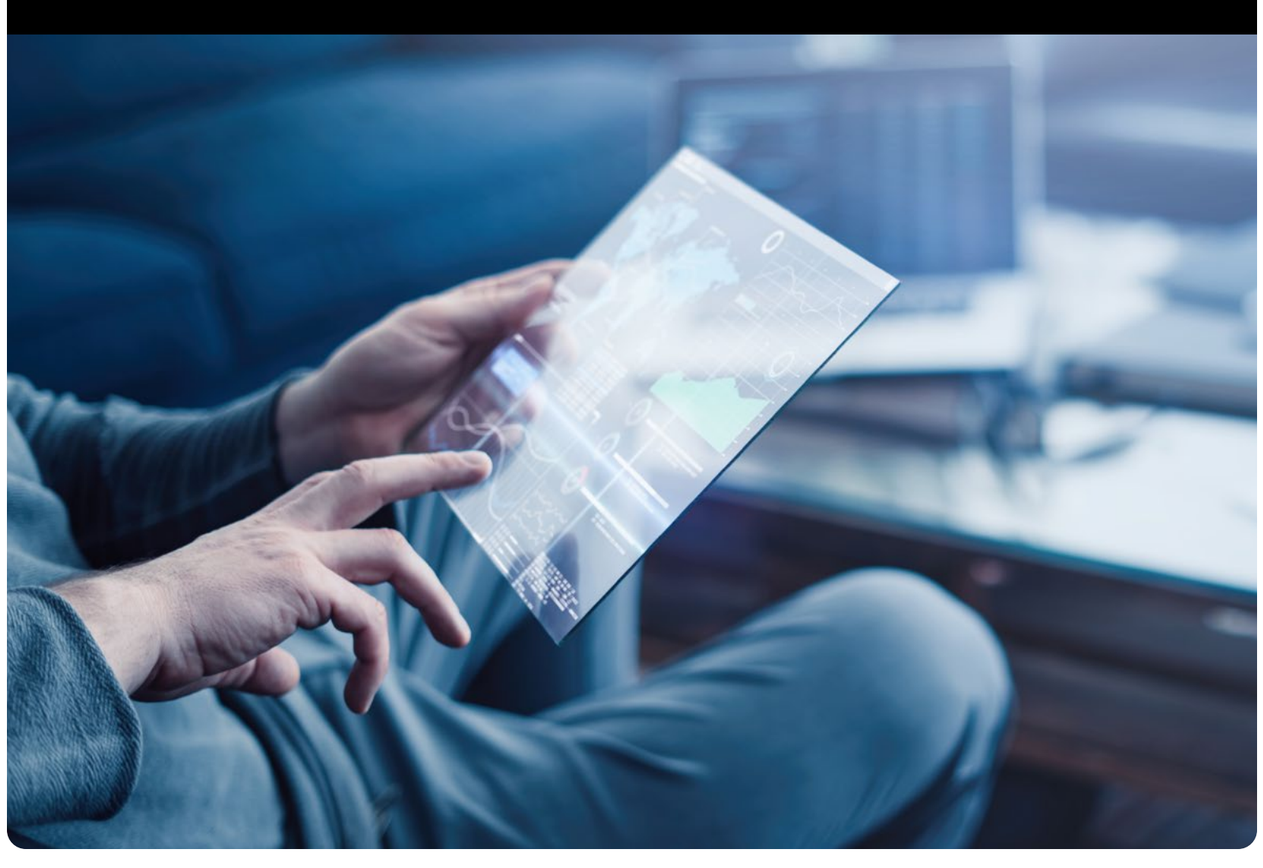
Security is just one of many factors limiting cryptocurrency’s broader adoption, but it is a solvable problem. Making these payments less vulnerable to fraud could open the door to acceptance across the board.

“As the crypto space continues to evolve and pivots toward a multichain ecosystem, we might soon see merchants and customers not only transacting and interacting with cryptocurrencies but [also] doing so across a whole suite of cryptocurrencies,” said Anziani. “There is still a long way to go, but with consumer interest and the continued merchant pivot to digital pointing the way, this scenario is a possible future state.”

For now, however, cryptocurrency largely remains an investment vehicle, but that makes it no less imperative to secure. Technologies such as biometrics and multifactor authentication are key for keeping fraud at bay.

PYMNTS Intelligence

How **Cryptocurrency Exchanges** Can Improve **User Authentication**



Cryptocurrency has gone from an obscure hobby to a household name in just more than a decade — a meteoric rise by any standard. The number of cryptocurrencies on the market has risen from 66 in 2013 to 7,557 in 2021, with individuals transacting from their phones, personal computers or the nearly 34,000 cryptocurrency ATMs scattered around the world. A-list celebrities, including Matt Damon, LeBron James and Larry David, are paid millions to pitch global cryptocurrency exchanges, and 80 million individuals worldwide now have blockchain wallets to buy and sell their favorite cryptocurrencies.

The growing enthusiasm for cryptocurrency can downplay the serious security concerns that still exist in the field, however. The U.K. saw more than £146 million ($192 million USD) lost to cryptocurrency fraud in 2021, a 30% jump from 2020. Swindlers are growing bolder in their schemes as well, with five of the 10 largest cryptocurrency thefts of all time occurring in the past 12 months, including the largest attack in history, which stole more than $600 million.

Cryptocurrency exchanges are not blind to these fraud risks, but many of their security measures, including document verification, have proven ineffective. The following PYMNTS Intelligence explores the scope of the cryptocurrency fraud threat and why a new security approach could better protect users.

Increase in cryptocurrency lost to fraud in the U.K. in 2021

FRAUD THREATS AND SECURITY WEAKNESSES

Bad actors have stolen more than $7.6 billion worth of cryptocurrencies since 2011, with $2.8 billion of this total pilfered through security breaches and $4.8 billion stolen through scams. There were more than 400,000 cryptocurrency scam incidents in 2020, up 40% from 2019, and fraudsters stole more than $14 billion in cryptocurrency in 2021. One of the single largest thefts on record occurred in 2018 when fraudsters stole $534 million in NEM coins from the cryptocurrency exchange Coincheck. More than 260,000 Coincheck customers were affected by the theft, and the thieves quickly unloaded the currency at a fraction of its price on dark web marketplaces. These thefts are nearly impossible to reverse after the fact due to the nature of cryptocurrency and the blockchain, making the thieves' capture and the victims' compensation unlikely at best.

Cryptocurrency exchanges are aware of fraud risks, but their existing security measures can fail to stop bad actors and may impede legitimate customers attempting to transact. Document verification is one common method for onboarding users, but this technique has weaknesses, including vulnerability to fake IDs. It can also hinder customers when they onboard, particularly if they plan to hold cryptocurrency as an investment rather than transacting with it. Many customers who sign up for cryptocurrency exchange accounts never transact with them at all, making this verification step unnecessary. This obstruction, combined with false positives, lengthy manual reviews and low accuracy, has led to customer approval ratings falling below 80%.

Cryptocurrency exchanges have several options available that promise to streamline the verification process and provide a more secure environment for their users.

IMPROVING USER VERIFICATION

One effective method of verifying cryptocurrency users is to move the document verification step to the time of purchase rather than having it at sign-up. This shift will limit the verification friction for many users by requiring authentication only when there is a risk of malfeasance, which naturally occurs when funds are moved around. Companies can also streamline and improve the document verification process: Socure's KYC solution, for example, leverages

Portion of cryptocurrency exchanges worldwide that have no KYC solutions in place

algorithmic name and date-of-birth matching in its document verification protocols, allowing it to achieve automatic customer approval rates of up to 98%.

There are other verification techniques available to cryptocurrency exchanges that can seamlessly verify users and limit the risk of cybercrime. One emerging technique is biometrics, which come in various different forms, such as face and fingerprint scans. Crypto.com, the largest exchange currently operating in the United States, recently implemented biometric login on its mobile app to verify customers.

Most cryptocurrency exchanges are happy with the status quo, however. Studies have found that 56% of exchanges worldwide have no KYC solutions in place. Any step to ensure the veracity of their customers could go a long way toward improving cybersecurity. While some methods are more effective than others, something needs to be in place to ensure that cybercrime does not run rampant.

NEWS & TRENDS

PAYMENTS FRAUD TRENDS

FTC SAYS AMERICANS LOST A TOTAL OF $5.8 BILLION IN 2.8M FRAUD INCIDENTS LAST YEAR

Fraud has become a common concern in consumers' lives, and even those who have not fallen victim to it still need to be on the alert for potential bad actors. The Federal Trade Commission (FTC) recently reported that American consumers lost more than $5.8 billion to fraud last year, with 2.8 million consumers filing reports. This total marks a 70% year-over-year increase compared to 2020 and is still unlikely to reveal the extent of the problem, as many instances of fraud go unreported. Approximately half of these fraud reports consisted of identity theft, which accounted for 1.4 million incidents. Other popular scams included fraudulent savings and checking accounts, which increased 64% from 2020. Reports of fraudulent mobile telephone accounts, meanwhile, declined 22%.

Younger generations were likelier to lose money to fraud, with 41% of consumers ages 20 to 29 being victimized compared to 18% of those ages 70 to 79. Seniors tended to lose more money per incident, however. The median loss for consumers ages 80 and older was $1,500 per claim, whereas those in their 70s lost $800 per incident.

CRYPTOCURRENCY SCAMS ARE NOW THE SECOND-RISKIEST TYPE, BBB REPORTS

Cryptocurrency is now a hot topic in households across the U.S., and the scams associated with it are growing increasingly perilous. The Better Business Bureau (BBB) recently announced that cryptocurrency scams were the second-riskiest type in 2021 behind online purchase schemes. The average dollar loss in each scam hit $1,200 last year, far surpassing an average of just $169 per incident in 2020 when such scams were ranked the seventh-riskiest.

The BBB said that 66% of consumers targeted by cryptocurrency scams lost money, with most bad actors perpetrating schemes that promised consumers a high return on investment. Many fraudsters leveraged social media to pitch these false investments, typically hacking into accounts and scamming the users' online friends.

COMBATING FRAUD

WHITE HOUSE ANNOUNCES CRYPTOCURRENCY REGULATION STRATEGY

Cryptocurrency has become so mainstream that the White House is exploring regulatory measures for the first time. President Joe Biden recently issued an executive order to introduce a regulatory strategy addressing its potential risks. The order directs the U.S. Department of Commerce to develop a comprehensive framework for cryptocurrency regulation and supports the Federal Reserve's current research into creating a U.S.-backed cryptocurrency. The order currently has no actionable effects but launches a regulatory process that will likely take years to develop.

"The rise in digital assets creates an opportunity to reinforce American leadership in the global financial system and at the technological frontier," the White House stated in a press release, "but also has substantial implications for consumer protection, financial stability, national security and climate risk."

NFT ENTHUSIASTS SLAM KYC PARTNERSHIP BETWEEN BORED APE YACHT CLUB AND ANIMOCA BRANDS

Handling KYC requirements has been an ongoing challenge for cryptocurrency exchanges. Many platforms lack any form of verification at the behest of their customers, many of whom view such policies as tantamount to privacy violations. This laissez-faire attitude has led many NFT fans to balk at a new partnership between NFT collection Bored Ape Yacht Club (BAYC) and Animoca Brands, the latter of which requires KYC verification for its customers. This move makes it mandatory for BAYC NFT owners to submit photo identification to be eligible to take part in the latest BAYC projects.

Many objectors said that the KYC requirement goes against cryptocurrency's values, one of which is anonymity during transactions. Others protested the terms of the partnership that allowed the creator of BAYC and Animoca Brands to "license, adapt and commercialize any portion of users' current and future content produced through or connected to the new project." Art theft is rampant in the NFT community, however, with or without KYC protocols in place.

SOCURE AND OSAAS PARTNER ON NEW IDENTITY VERIFICATION SOLUTION FOR STATE AND LOCAL GOVERNMENTS

Government agencies also contend with fraud, with cybercriminals hacking into government accounts to install ransomware or steal consumers' personal data. Digital identity verification and fraud solution provider Socure recently partnered with technology solutions-as-a-service public sector integrator OSaaS on a new identity verification platform geared toward government entities. The platform allows these entities to flag potentially risky applicants for programs such as mortgage relief or benefits distribution. The application aims to reduce manual review queues, thereby enabling faster processing for legitimate applications without increasing the risk of fraud.

Fraud losses from government programs can be staggering. The U.S. Secret Service estimates that fraudsters stole $100 billion from pandemic relief funds, for example, and California lost $20 billion to false unemployment benefits during the pandemic so far. Reducing these losses could go a long way toward solidifying individuals' trust in government institutions.

ALTERNATIVE PAYMENTS TRACKER®

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.

Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from email, phone, address, IP, device, velocity and the broader internet to verify identities in real time. The company has more than 750 customers across the financial services, gaming, healthcare, telecom and eCommerce industries, including four of the top five banks, seven of the top 10 card issuers, three of the top MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers and more than 100 of the largest FinTechs. Marquee customers include Chime, SoFi, Varo Money, Public, Stash and DraftKings. Socure customers have become investors in the company, including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, Voyager and Synchrony. Additional investors include Accel, funds and accounts advised by T. Rowe Price Associates, Inc., Bain Capital Ventures, Tiger Global, Commerce Ventures, Flint Capital, Scale Venture Partners, Sorenson, Two Sigma Ventures and others.

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