Coinbase doubles down on anti-politics stance with exit package offer

Enlarge / Coinbase CEO Brian Armstrong.

reader comments

253 with 107 posters participating, including story author

Share this story

In the last few years, big technology companies have faced growing pressure from employees to become involved in social justice issues. This pressure intensified this summer with the George Floyd protests. But this week, CEO Brian Armstrong of the cryptocurrency exchange Coinbase staked out a contrarian stance.

“While I think these efforts are well-intentioned, they have the potential to destroy a lot of value at most companies, both by being a distraction, and by creating internal division,” Armstrong wrote in a blog post. “We’ve seen what internal strife at companies like Google and Facebook can do to productivity. I believe most employees don’t want to work in these divisive environments.”

Armstrong’s post attracted a range of responses from online commentators. Some prominent Silicon Valley figures praised it, while critics argued it was “absolutely laughable” to believe that a company could keep politics out of the workplace.

In an internal email to employees, Armstrong doubled down on

the company's new stance, offering any employee who "doesn't feel comfortable with this new direction" four to six months of severance to leave the company, according to The Block.

"It's always sad when we see teammates go, but it can also be what is best for them and the company," Armstrong wrote. "Life is too short to work at a company that you aren't excited about."

Why Coinbase might be different

This summer, Armstrong reportedly faced an employee revolt after he declined to publicly affirm that "Black lives matter." According to Erica Joy and insiders who spoke to The Verge's Casey Newton, Armstrong eventually relented and tweeted the phrase—but only after some Coinbase engineers organized a walkout. Some critics believe that the new Coinbase policy may be an effort to make sure Armstrong doesn't face this kind of revolt in the future.

This kind of employee activism is effective because there is intense competition for talent in Silicon Valley. Programmers in the Bay Area tend to lean left on issues of race and gender, and they've increasingly used their power to pressure their employers to do more to promote anti-racist causes.

But while Silicon Valley engineers may lean left on average, the culture is far from monolithic. Silicon Valley also has a subculture of libertarian-leaning engineers who are not enthusiastic about the Bay Area's increasingly woke politics. James Damore, an engineer who got fired from Google for writing a controversial memo about gender diversity, has become one of the best-known examples.

Coinbase is effectively making a bid for this slice of the Silicon Valley workforce. The company is well-positioned to do this because the cryptocurrency world has long had an anti-government ethos that appeals to libertarians. As a result,

Coinbase’s employees probably lean more to the right on issues of race and gender than Silicon Valley engineers as a whole. The same is likely true of Coinbase’s customers.

So Armstrong is likely to face less backlash from his employees and customers than other technology CEOs would face for taking the same stance. His stance is and will be controversial in some corners of the Internet. But he’ll find support from others—and these supporters may ultimately be more important for Coinbase’s long-term success.

https://arstechnica.com/?p=1710755

Charges filed in hack that caused NFL athlete’s nude pics to be posted on Twitter

Enlarge / The Department of Justice seal as seen during a press conference in December 2019.

reader comments

27 with 25 posters participating

Share this story

Federal authorities have accused two men of hacking the email and social media accounts of multiple athletes with the National Football League and the National Basketball Association and either selling or ransoming the credentials

for profit.

In one case, according to a criminal complaint unsealed on Wednesday, the account compromises resulted in explicit photos of one of the NFL players being posted to his Twitter and Instagram accounts. The complaint didn't identify the athlete except to call him Victim-1 and to say that he lived in New Jersey and the photos appeared on June 4, 2018.

Based on the information, the player appeared to be New York Giants defensive end Avery Moss, who, according to ESPN, found naked pictures and videos posted to his Twitter timeline shortly after finishing an OTA practice on June 4. Accounts he followed were blocked, most likely in an attempt to delay Moss from learning of the postings. More explicit videos and images appeared later but were subsequently removed within about 30 minutes.

One of "multiple"

According to federal prosecutors, Victim-1 was one of multiple NFL and NBA athletes targeted in a hacking conspiracy by Trevontae Washington, 21, of Thibodaux, Louisiana, and Ronnie Magrehbi, 20, of Orlando, Florida.

The complaint charging Washington said that the man obtained account credentials belonging to the victims by sending them links to what appeared to be legitimate social media login pages but were, in fact, phishing sites. Washington, Magrehbi, and others would lock the rightful owners out of the accounts and sell access to them for amounts ranging from $500 to $1,000.

On June 1, 2018, Victim-1 made two $250 payments by Venmo and, in exchange, received a text including a password. He gained access to the account, but as soon as he tried to change the password, he was locked out again. Three days later, the explicit photos were posted. On the same day, hacking

conspirators demanded an additional $2,500 and “threatened to release additional images and videos of Victim-1 if he did not comply.” Victim-1 didn’t comply.

Washington and Magrehbi are charged with one count each of conspiracy to commit wire fraud and conspiracy to commit computer fraud and abuse. They face maximum penalties of $500,000 and 20 years in prison if found guilty. Both men are scheduled for their initial court appearances on Wednesday.

https://arstechnica.com/?p=1710750

Proposed EU rule may mean you can finally delete some apps from your phone

reader comments

135 with 86 posters participating

Share this story

European regulators once again have the behavior of the biggest US tech companies—Amazon, Apple, Facebook, and Google among them—squarely in their sights as they move forward with a proposal to reform how digital marketplaces and data sharing operate.

An early draft of the Digital Services Act, under

consideration by the European Parliament, would not only require tech forms to share data with smaller rivals but would also limit the ways companies can use customer data they've already collected, the Financial Times was first to report.

Under the proposal, tech firms with the potential to act as gatekeepers "shall not pre-install exclusively their own applications nor require from any third-party operating system developers or hardware manufacturers to pre-install exclusively gatekeepers' own application," according to Reuters. The draft also mandates that gatekeeper companies will also not be permitted to use data collected on their platforms to target users unless that data is also shared with rival firms.

There's something in the draft for every major US tech firm to object to, it seems. Apple and Google in particular are likely to object to the provisions limiting preinstalled apps on hardware, as both iPhone and Android devices come complete with a whole suite of integrated first-party programs that you may or may not ever be able actually to delete. Apple is also highly likely to object to a provision that would effectively prohibit gatekeeper firms from blocking side-loading or alternative app stores or payment methods—the entire heart of the current dispute between Epic and Apple.

Meanwhile, Google, Facebook, and Amazon—all of which rely on tying together vast reams of user and competitor data—are likely to object to the provisions requiring information they see as proprietary to be shared with rivals.

Not the first time

The European Union has taken several previous stabs at enhancing competition in the digital marketplace, but its well-intended efforts have not always proven successful. For example, in Europe, as the result of a massive antitrust case, Google is required to offer Android users a chance to select

their default search provider at device setup. The non-Google alternatives are selected by auction, however, and independent search provider DuckDuckGo this week had sharp criticism for the process after losing its position to Microsoft’s Bing.

“This auction format incentivizes bidders to bid what they can expect to profit per user selection,” DuckDuckGo wrote in a company blog post. “The long-term result is that the participating Google alternatives must give most of their preference menu profits to Google! Google’s auction further incentivizes search engines to be worse on privacy, to increase ads, and to not donate to good causes, because, if they do those things, then they could afford to bid higher.”

Google, in a submission to the Act package, pushed back on the idea of gatekeeper firms, according to the Financial Times. “In certain sectors, the platform may have market power; in others, it may be a new entrant or marginal player,” Google said, probably describing itself. “The digital ecosystem is extremely diverse and evolving rapidly and it would be misguided for gatekeeper designations to be evaluated by reference to the position of an entire company or corporate group.”

https://arstechnica.com/?p=1710598

Facebook needs to enforce misinfo rules against Trump, Biden campaign says

reader comments

78 with 49 posters participating

Share this story

After being used as a platform for massive voter-interference campaigns in 2016, Facebook promised this time would be better. The company changed its policies and swore up and down that it would work hard to mitigate the spread of misinformation and support Americans' rights to get out and vote this fall. But with five weeks to go before Election Day—and early voting already underway in some states—critics allege Facebook is not keeping up with the challenge.

The latest person to accuse Facebook of failing to manage misinformation is the Democratic candidate for president, former Vice President Joe Biden. The Biden campaign said in a letter to Facebook (PDF) last night that the company is not only failing to take long-promised additional actions, but is in fact regressing in how well it handles falsehoods.

"Facebook's continued promise of future action is serving as nothing more than an excuse for inaction," Biden campaign manager Jen O'Malley Dillon wrote. "Millions of people are voting. Meanwhile, your platform is the nation's foremost propagator of disinformation about the voting process."

Weak fact-checking

The letter pointed specifically to a video the Trump campaign shared on September 21 as its most recent case in point. That video featured Donald Trump Jr. claiming—without any evidence whatsoever—that Democratic supporters plan to "add millions of fraudulent ballots" and "cancel" ballots cast for Republican

candidates.

Facebook now appends a link to its voting information center to almost any post (from individuals or pages, in newsfeeds or groups) that mentions “vote” or “election” in any way, including posts from political campaigns and figures. Those links, however, do not present as fact-checks and do not counteract false claims, despite Facebook’s assertions that it will fact-check content “that seeks to delegitimize the outcome of the election or discuss the legitimacy of voting methods, for example, by claiming that lawful methods of voting will lead to fraud.”

“Dozens of responsible media voices and political campaigns throughout the country, including ours, brought this content to your immediate attention, as it violates both your policies and your commitment that *no one* [emphasis in the original] will be permitted to use Facebook’s tools to ‘undermine democracy,'” Dillon wrote.

“No company that considers itself a force for good in democracy, and that purports to take voter suppression seriously, would allow this dangerous claptrap to spread to millions of people,” she added. “If Facebook’s goal is to accomplish what it has publicly committed to do—i.e., ‘clear up confusion about how this election will work’—the solution should have been simple: remove Mr. Trump’s posts, which violate your policies.”

Facebook, in response, mostly ignored what the Biden campaign actually asked for and again claimed it applies its rules equally across the board.

“While many Republicans think we should take one course, many Democrats think we should do the opposite,” a Facebook spokesperson said. “We’ve faced criticism from Republicans for being biased against conservatives and Democrats for not taking more steps to restrict the exact same content. We have

rules in place to protect the integrity of the election and free expression, and we will continue to apply them impartially."

Incoming chaos

Facebook's current troubles managing misinformation do not bode well for election night and the chaos that is likely to follow. The company has promised to go into its own effective lockdown mode on election night if it has to, and it well might.

Company executive Nick Clegg said earlier this month the company would take "pretty exceptional measures to significantly restrict the circulation of content" around the election if it seems likely to lead to "chaotic" or "violent" circumstances. At the very least, high tension seems unavoidable—and as the Biden campaign observed, a great deal of it seems to be coming from inside the (White) House.

"Russia doesn't have to make fake news. They just repeat what conspiracies are coming out of the White House and the administration," one expert told NPR today, adding that election watchers are particularly worried about efforts to undermine Americans' confidence in the voting process.

The FBI, meanwhile, is warning of a heightened likelihood of election-related violence from domestic extremists, who have historically used Facebook to organize.

The president has several times in recent days hedged when asked if he will honor the results of the election if they are not in his favor, saying, "We're going to have to see what happens." He and his campaign have both continued to sow allegations of widespread, rampant voter fraud, although research shows any fraud is extremely rare and even federal election officials, appointed by Trump, say there is "no real evidence" of voter fraud. Some of those allegations of ballot

fraud have been posted on Facebook (September 25, September 27) with minimal fact-checking.

Facebook said earlier in the week that it will expand its ban on election-week ads to include a ban on political advertisements “that claim victory before the results of the 2020 election have been declared,” Fast Company was first to report. That said, however, there is nothing stopping either campaign from prematurely announcing a win *without* using paid advertisements to do so. Facebook will “add a label to their post educating that official results are not yet in and directing people to the official results” when they do. That is unlikely to be enough.

https://arstechnica.com/?p=1710355

How Internet-connected voter check-in devices can create election chaos

Enlarge / A polling-place worker holds an “I’m a Georgia Voter” sticker during the primary election on June 9, 2020 in Atlanta.

reader comments

43 with 35 posters participating

Share this story

A federal judge in Georgia has ordered election officials to print paper backups of voter data so that voting can proceed even if the digital system for checking in voters fails. This is a win for plaintiffs who have argued that flaws in Georgia's electronic-poll-book (EPB) system hampered voting in the June primary and could do so again in November.

Over the last 20 years, a lot of discussion has revolved around the risk that electronic voting machines pose to the security and integrity of elections. But there has been less attention paid to electronic poll books—another digital system that can undermine election integrity if they malfunction.

Pollworkers use EPBs to verify a voter's eligibility and then check the voter in. Malfunctions in these systems can slow down the voting process so much that some people give up voting altogether. By targeting precincts where most people vote for a particular candidate or party, a hacker could potentially swing a close election just by triggering malfunctions in electronic poll books. And while voting machines are supposed to be kept off the Internet, electronic poll books are often online throughout election day.

There's no evidence that anyone has deliberately exploited this potential vulnerability in American elections, and maybe no one ever will. But at a minimum, electronic poll books make American elections more complex and brittle. It's possible that, as with voting machines, the old paper system was actually a better choice.

Georgia's electronic poll books caused problems

Georgia has long been a battleground in the debate over electronic voting technology. Until last year, Georgia used

ancient paperless voting machines that didn’t allow for a meaningful post-election audit. Last year, US District Judge Amy Totenberg ordered the state to switch to a system of paper ballots. In the new system Georgia introduced this year, voters enter votes on a touchscreen ballot-marking machine that then prints out a paper ballot.

This year, along with the ballot-marking machines, the Peach State also introduced a new electronic-poll-book system. The KnowInk Poll Pad is an iPad running custom software that pollworkers use to verify voter eligibility and check voters in.

Problems with these machines aren’t just a theoretical concern. In her Monday ruling—part of the same case that forced an end to paperless voting last year—Judge Totenberg points to numerous examples when EPB glitches created hour-long delays during Georgia’s chaotic June 9 primary

One poll watcher visited a voting location at the Central Park Recreation Center in the Atlanta area. She reported that “the wait time to vote at 10:00 a.m. was estimated at 4 hours. Voting was almost at a complete standstill due to inoperable electronic poll books.” Unable to verify voters’ eligibility, election workers asked voters fill out provisional ballots, which dramatically slowed down the voting process.

A voter in DeKalb County, also in the Atlanta area, reported that “two PollPads were down and no one had voted after waiting for an hour after polls should have opened.” At the Dunwoody Library in DeKalb County, “voters had been waiting over an hour” and “voters were not being checked in because the PollPad equipment was down.”

There’s no evidence that these machines were hacked. By all indications, the problems with EPBs in the primary had more mundane causes like software bugs, networking problems, or inadequate training of pollworkers. But regardless of the

cause, the problems with the EPB likely prevented some voters from casting a vote. And Judge Totenberg concluded that that was a big problem.

Electronic poll books need paper backups

To help prevent the repeat of these problems in November, plaintiffs asked Judge Totenberg to order that every precinct have a paper copy of poll-book data. Precinct officials were already slated to have printouts of voter-registration data, but these printouts lacked up-to-date information about who had already cast early votes or requested absentee ballots. Pollworkers need this information to decide whether a voter can cast a ballot. Plaintiffs wanted officials to print out a copy of this up-to-date data in the brief window between the last day of early voting and Election Day.

Georgia officials argued that it would be too burdensome to print out this data for every precinct. But they had few good arguments against making the data available online for local officials to print out themselves. So that's what Judge Totenberg ordered.

Georgia isn't the only jurisdiction that has suffered EPB problems. Voters in Los Angeles experienced long lines during the March primary election in California, and a subsequent investigation pointed to problems with new electronic poll books as a major culprit. In 2018, problems with EPBs caused problems in South Dakota, Philadelphia, and Indiana's Johnson County.

So it would be wise for any jurisdiction relying on electronic-poll-book software—and there's a lot of them—to make sure to have a paper backup on hand at every polling location.

https://arstechnica.com/?p=1710388

Man refused to disband party that violated COVID order, gets year in jail

Getty Images | Caspar Benson

reader comments

327 with 164 posters participating

Share this story

A Maryland judge sentenced a man to one year in jail after finding him guilty of throwing two large parties in violation of a state pandemic order that banned large gatherings. Police were called to the man's home twice in one week, and he refused to disband the party on the second occasion, authorities said.

Shawn Marshall Myers, 42, was sentenced on Friday at the District Court of Maryland, said an announcement by the state's attorney for Charles County. Myers' legal troubles began on March 22 when "multiple officers responded to Myers' residence… for the report of a large party" violating Governor Larry Hogan's order in which "large gatherings were strictly prohibited," the state's attorney office said.

Myers allegedly hosted about 50 people at the party. "Upon

arrival, officers told Myers that his party violated the current mandate. Myers was argumentative with officers but eventually agreed to disband his party," the state's attorney office said.

Just five days later, "officers responded back to Myers' residence for another report of a party exceeding fifty people," the announcement said. "Officers told Myers to disband the party, but again he was argumentative claiming he and his guests had the right to congregate. Beyond being argumentative, Myers directed his guests to stay in defiance of Governor Hogan's Orders and the officers' lawful orders to disband the party. Officers tried to reason with Myers and obtain his cooperation to no avail. Myers was then apprehended."

The large-gathering ban has since been lifted, but Myers' parties occurred when the ban was in effect.

Second party results in jail time

Myers was found guilty of two counts of failure to comply with an emergency order. The first count resulted in a six-month suspended sentence and a $1,000 fine, which was also suspended. For the second count, Myers was sentenced to one year in jail, a $5,000 fine, and three years of unsupervised probation. He will serve the year of jail time in the Charles County Detention Center, the announcement said. Myers has filed an appeal, according to The New York Times.

An executive order issued in March banned social gatherings of more than 10 people "at all locations and venues" in order to limit spread of the coronavirus. The order classified any "knowing" and "willful" violation as a misdemeanor that can be punished with up to a year behind bars and a $5,000 fine. Myers therefore got the maximum sentence on the second count. The case was decided by Judge W. Louis Hennessy, without a jury.

Social-distancing orders have been imposed in many states as COVID-19 continues spreading throughout the country, but this is the first time we've heard of jail time being issued for violation of a large-gathering order. "The state's attorney's office said that a few others in Charles County had been charged with violating the governor's order but that Mr. Myers' case was the first to have gone to trial," the Times article said.

Hogan acknowledged in early June that enforcement was rare. "The 10-person limit is technically still in effect, because it's still not really safe to gather with people closely together, but most people are not following that and it's probably something I think every state still has in place and nobody's following it," Hogan said at a press conference.

Hogan's large-gathering ban was repeated in several executive orders including one on June 3. But a superseding order on June 10 dropped the ban. That and more recent orders, including one this week, advise residents to avoid large gatherings and crowded places but do not make it a requirement.

https://arstechnica.com/?p=1710360

Verizon, AT&T to pay $127M for allegedly overcharging government agencies

reader comments

27 with 26 posters participating

Share this story

Verizon and AT&T have agreed to pay a combined $127 million to settle lawsuits alleging that they overcharged California and Nevada government entities for wireless service. The lawsuit was filed in 2012 and resulted in a settlement approved on Thursday last week by Sacramento County Superior Court, the plaintiffs' law firm, Constantine Cannon, announced.

"Verizon will pay $76 million and AT&T $51 million to settle claims that, for more than a decade, they knowingly ignored cost-saving requirements included in multibillion-dollar contracts offering wireless services to state and local government users in California, Nevada, and other states," the announcement said. "Sprint and T-Mobile previously reached settlements totaling $11.7 million. Combined, the four major telecom providers will pay $138.7 million to settle allegations in the lawsuits." Those numbers do not include what the carriers agreed to pay in attorneys' fees, which is $23.45 million from Verizon and $13 million from AT&T.

The contracts required that carriers bill government entities "at the 'lowest cost available' and that the carrier[s] identify 'optimized' rate plans that best suited actual usage patterns that drive cost," the law firm also said. The lawsuits alleged that the carriers' contract violations "cheated California and Nevada government entities out of hundreds of millions in savings," the law firm said.

About 30 government entities in California joined the lawsuit against the carriers. Of the $76 million from Verizon, $68 million is for California entities and $8 million is for Nevada entities. AT&T is paying $48 million to California entities and $3 million in Nevada. The lawsuit alleged that

government entities would have saved 20 percent or more on their wireless-service costs if the required rate-plan optimization was performed.

The carriers denied the overcharging allegations, with Verizon saying it "settled these meritless claims to avoid a protracted legal battle," according to the Associated Press. AT&T similarly told the AP that it "'complied with our contracts and the law' and denied wrongdoing, but settled to avoid costly litigation."

Payout split among hundreds of gov't entities

Nearly 300 state and local entities will get refunds for excessive payments, with some of the biggest payouts going to the state of California itself, the California State University system, the University of California system, Los Angeles County, Orange County, and the city and county governments of Sacramento and Riverside.

About 40 percent of the settlement money will go to OnTheGo Wireless, which sued the carriers on behalf of government entities under the California False Claims Act and Nevada False Claims Act. OnTheGo created software to analyze rate plans and "concluded the carriers failed to provide contractually required cost-saving opportunities to their government customers," Constantine Cannon wrote.

"In a tentative ruling, Judge Judy Holzer Hersher found that the reward was justified in part because OnTheGo Wireless discovered and reported overcharging that was unknown to government entities," according to The San Diego Union-Tribune.

According to a motion to approve the settlement filed by the plaintiffs' attorneys, Verizon first entered into a purchasing

agreement with California in 2005. Government entities joined the lawsuit in December 2015 and, at that time, “brought additional common-law claims for breach of contract, unfair business practices, and unjust enrichment,” the motion said. The motion also said government agencies that intervened in the suit “withstood a scorched-earth discovery campaign, which taxed the resources and time of hundreds of government employees.” OnTheGo lost “all of its business providing outside optimization services to Verizon” because of the lawsuit, the document said.

The Union-Tribune article said that “San Diego County looks to receive the largest local payout from the settlement at just under $2.1 million,” while the city of San Diego will receive about $972,000.

The settlement amount “may be a rounding error to Verizon and AT&T, but this is real money to California and Nevada’s schools, local governments and state agencies, who spent years scraping through their budgets to pay what we now know were over-inflated bills,” lead counsel Wayne Lamprey said.

https://arstechnica.com/?p=1710173

Trump likely overstepped authority with TikTok ban, judge rules

Enlarge / TikTok’s US fate is up in the air, but at least you can still download and patch it.

reader comments

195 with 54 posters participating

Share this story

President Donald Trump’s attempt to ban TikTok from operating inside the United States probably exceeds the authority the president has to do such things, a federal judge has ruled.

TikTok narrowly avoided being removed from app stores last night when Judge Carl Nichols of the US District Court for DC issued an injunction late yesterday requiring the government to pause on its ban. TikTok got its reprieve, but the terms of the order (PDF) were sealed until midday today.

To meet the standard for an injunction, Nichols explained, TikTok basically needed to prove four things to his satisfaction. The first factor, however, is the most important: TikTok needed to prove its case is “likely to succeed on the merits.” In plain English, that means: is it going to win its lawsuit against the administration? And the answer, Nichols determined, is probably yes, because the actions the administration took “likely exceed the lawful bounds” of the law under which those actions were taken.

The executive order banning TikTok uses the International Emergency Economic Powers Act (IEEPA) as its legal basis. The IEEPA does allow the president to enact emergency regulations relating to international commerce after declaring a national emergency, which Trump did.

However, Nichols explained, there are two limitations in IEEPA. The law does not grant the president the authority “to regulate or prohibit, directly or indirectly” either the exchange of “information or informational materials” or personal communications. TikTok argued that its content qualifies as both informational material and personal communication, and the court agreed.

“Less substantial”

“The government has provided ample evidence that China presents a significant national security threat,” Nichols found, but the “specific evidence of the threat posed by [TikTok], as well as whether the prohibitions are the only effective way to address that threat, remains less substantial.”

“There is something to [the government’s] argument, especially as foreign adversaries’ use of information and data (and the United States’ efforts to respond to and combat those efforts) becomes ever more important,” Nichols added. But having valid concerns about China doesn’t actually make the IEEPA say what the administration claims it does, he concluded.

Notably, Nichols only suspended the part of the ban scheduled to go into effect this weekend, which would have removed TikTok from app stores, prohibiting new downloads or patches of the app. He did not address the full prohibition, which is slated to take effect November 12. TikTok’s arguments regarding the November 12 ban were sound, Nichols determined, but that’s too far in the future for “truly imminent and immediate harm” to qualify as a standard.

The “national emergency” around TikTok may or may not have been resolved by November. If a proposed transaction with Oracle goes through, then it seems likely the administration will leave off on its efforts to ban the app. That deal, however, is far from certain. Although Trump gave the transaction his conditional “blessing,” the deal still needs to pass national security review and also win approval from Chinese authorities.

https://arstechnica.com/?p=1710172

IRS may put cryptocurrency question at the top of 1040 to catch cheaters

reader comments

163 with 75 posters participating, including story author

Share this story

The Internal Revenue Service is considering adding a question to Form 1040—America's primary income tax form—asking tax filers if they dealt in virtual currency in 2020. It would be the agency's latest attempt to crack down on underreporting of cryptocurrency profits.

If an American buys bitcoin, ether, or another cryptocurrency and then sells it later at a profit, she or he will typically owe capital gains tax on the difference. But blockchains do not have the tax reporting infrastructure that has become standard for conventional financial institutions. So the IRS doesn't have an easy way to figure out who has received a cryptocurrency windfall. In the early years of the bitcoin boom, many taxpayers failed to report large bitcoin-related profits.

In recent years, the IRS has increased pressure on cryptocurrency traders to comply with tax laws. A 2014 bulletin laid out the basic rules for paying taxes on virtual

currency price gains. In 2016, the IRS sought transaction data about thousands of users of Coinbase, a popular US-based cryptocurrency exchange. Coinbase complied with the request in 2018 after some legal wrangling.

But chasing down individual cryptocurrency investors after the fact is a lot of work for the IRS. The agency would much prefer American taxpayers voluntarily comply with the law. And that's where the new question on Form 1040 would come in.

In the past, it was easy for taxpayers to leave out cryptocurrency earnings and then claim ignorance if the IRS catches them. It was hard for the IRS to prove that this was deliberate tax evasion rather than an honest oversight.

Last year, The Wall Street Journal reports, the IRS added a question about cryptocurrency to tax forms. But it was in a part of the return that not every taxpayer had to fill out.

On the 2020 version of the 1040, the cryptocurrency question could be the very first one taxpayers answer after giving their name and other identifying information. A draft of the 1040 posted to the IRS website asks taxpayers: "at any time during 2020, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?"

If taxpayers check "yes," the agency can double-check that virtual currency transactions were reported correctly. If taxpayers check "no," they could be prosecuted for tax evasion if the IRS later discovers they were lying. The prominent placement of the question will make it harder for a taxpayer to convince a jury that a failure to report cryptocurrency profits was an honest mistake.

Ed Zollars, a CPA with Kaplan Financial Education, told The Wall Street Journal that this strategy helped the IRS crack down on the use of offshore bank accounts a decade ago. Adding an explicit question about offshore bank accounts to tax forms

increased compliance with reporting rules and has added billions of dollars to the federal treasury.

https://arstechnica.com/?p=1710158

Nikola founder bought truck designs from third party

Enlarge / A 2018 Nikola video showed the Nikola One prototype rolling down a shallow hill in Utah. Nikola now says it never claimed the truck was driving under its own power.

reader comments

65 with 50 posters participating

Share this story

The original design for Nikola's flagship truck was purchased by founder Trevor Milton from a designer in Croatia, according to two people with knowledge of the matter, despite company claims in a 2018 lawsuit that the vehicle was initially designed by Mr. Milton "in his basement.."

The truck, the Nikola One, is at the centre of a $2 billion lawsuit with Tesla, in which Nikola alleges its rival infringed on its patents. Nikola claims in that lawsuit that Mr. Milton began designing the model in 2013, with other company staff later working on it.

In a rebuttal to the lawsuit filed last week, Tesla alleged

that Nikola could not protect the designs because they did not originate from the company itself, but from Adriano Mudri, a designer based in Croatia.

Two people with knowledge of the transaction told the Financial Times that the Nikola founder bought the designs in 2015 after meeting Mr. Mudri while visiting electric supercar maker Rimac in Croatia.

While Tesla's filing identifies the designer as the source of the original truck drawings, it does not contain details about the transaction, explain that money was exchanged, or that Mr. Milton himself orchestrated the purchase.

The latest twist comes with Nikola still reeling from accusations earlier this month that it passed off purchased technology as its own, covering supplier names on key components with stickers when making promotional videos. Nikola said it never claimed it made the components.

In a report that sent Nikola's shares tanking, Mr. Milton was accused of spreading an "ocean of lies" about the company's technology and its products by short seller Hindenburg Research.

A little over a week later, Mr. Milton decided to leave the company, telling staff he planned to defend himself "against false allegations levelled against me by outside detractors." The 39-year-old founder has repeatedly insisted that he has not lied to or deceived anyone about the trucks.

The lawsuit with Tesla, filed during Mr. Milton's tenure, centers on the origins of the designs for the "Nikola One" truck.

The company claims that Mr. Milton worked for two years on the truck before, unsatisfied with his designs, he hired designer Steve Jennes in 2015. The lawsuit says the pair then crafted the final design between them in a lengthy process.

When it was finished, Nikola had spent “several million dollars developing the Nikola One,” according to the lawsuit.

In its rebuttal, Tesla said that the designs for the model originated from Mr. Mudri, a designer at Rimac, who had dubbed it the “Road Runner.” The design’s origins could raise further questions about Nikola’s intellectual property.

“Trevor Milton chose not to disclose the Road Runner concept truck to the [US Patent and Trademark Office] with deceptive intent,” Tesla said in its filing.

Nikola said: “The Nikola One truck was designed and patented by Nikola. It is commonplace to license third party designs during vehicle development, and although early in the process Nikola purchased a license to Adriano Mudri’s designs, he was not part of the design team and his designs are materially different from the design invented by Nikola for the Nikola One.”

According to several people with knowledge of the deal, Mr. Milton sought, unsuccessfully, to collaborate with Rimac on a range of projects in 2015.

On a trip to Rimac’s headquarters on the outskirts of Zagreb, he met Mr. Mudri, the company’s designer, who had designed a futuristic truck as part of an earlier diploma project.

Mr. Milton purchased the computer drawings and virtual 3D model of the vehicle for several thousand dollars from Mr. Mudri, according to two people.

The Road Runner name lingered for months. A person familiar with the development of the Nikola One said that “Road Runner… was the internal name for Nikola’s project the entire time we worked on it.”

A screenshot of a Nikola document seen by the Financial Times shows 13 people being invited to collaborate on the “Nikola

Roadrunner Prototype Project.”

Another screenshot shows an early version of Nikola’s website depicting a truck that appears identical to the Road Runner in Tesla’s court filing.

Nikola did not mention Mr. Mudri, or Rimac, or say that the designs were purchased, in its 2018 filing against Tesla.

Representatives for Mr. Milton declined to comment. Rimac also declined to comment.

© 2020 The Financial Times Ltd. All rights reserved. Not to be redistributed, copied, or modified in any way.

https://arstechnica.com/?p=1710025