You’re probably not going to get your $125 from the Equifax settlement

Enlarge / A monitor displays Equifax Inc. signage on the floor of the New York Stock Exchange (NYSE) in New York on Friday, September 15, 2017.

reader comments

215 with 117 posters participating

Share this story

If you haven’t already filed a claim for cash compensation in response to the Equifax breach, you might be out of luck. The company is no longer offering payouts in lieu of credit monitoring.

The Federal Trade Commission page devoted to the settlement it announced with Equifax last week was updated July 31 to say that any consumer affected can claim up to 10 years of free credit monitoring. “Previously, a cash payment was identified as an option,” the site now adds, “but there are limited funds available.”

The FTC said in a statement that “public response to the settlement has been overwhelming.” In a separate blog post, the commission said the “unexpected number of claims” would result in claimants not getting the money they thought.

Is the response really so “unexpected?”

In return for leaking highly sensitive personal data on about 147 million consumers, about 45% of the entire US population, the company will pay at least $575 million. A minimum of $300 million goes into a fund to pay for compensating consumers who were affected, and that fund can get boosted by another $125 million if the initial $300 million isn’t enough to compensate all consumers who make claims.

Equifax will pay another $175 million in fines to be split up among the 50 attorneys general who agreed to settle their suits, representing 48 states, Washington DC, and Puerto Rico, and $100 million in penalties to the Consumer Financial Protection Bureau.

Under the terms of the settlement, consumers can make three separate kinds of claims: one for credit monitoring, one to compensate for time spent dealing with Equifax’s mess, and one to reimburse you for actual identity theft or fraud suffered as a result of the breach.

Initially, consumers who already have credit monitoring services (as millions do) could choose to claim a $125 cash payment in lieu of the service. Legions of sites, including us, suggested their readers do so, as credit monitoring solutions are not only ubiquitous but also frequently ineffective.

However, the bucket for paying out cash-alternative claims is capped at $31 million—about 10% of the overall claim compensation fund Equifax set aside. The obvious question, therefore, is: what is the other 90% getting used for?

Equifax in a statement last week said the fund was to “pay benefits to consumers, court-approved fees and costs of class counsel and service awards to the named class representatives,

and other expenses.” Consumers can also claim up to $500 for time spent and up to $20,000 for suffering identity theft, to be paid out from the same fund. But it seems likely there will be many fewer claimants seeking high-value reimbursement than claimants seeking the $125 credit monitoring alternative, as those claims require a much higher bar of proof.

We’ve reached out to the FTC for comment and will update this story if we hear back.

https://arstechnica.com/?p=1544039

Amazon writes scripts for cops to sling Ring home cameras, report says

Enlarge / Your local police might like to interest you in this product.

reader comments

171 with 101 posters participating

Share this story

Amazon and its subsidiary Ring, maker of home surveillance equipment, have a very cozy relationship with law enforcement. So cozy, according to reports, that Amazon not only requires police departments it partners with to market its product, but the company writes the copy for them.

Gizmodo obtained emails and documents showing Ring pre-wrote messages used by police on social media and in press releases used in at least three states.

Ring also demands police departments in partnerships with it give the company final review on all its statements about Ring products, Gizmodo reports. That arrangement led to the city of Boca Raton, Florida waiting three weeks to announce a Ring partnership already in progress.

Gizmodo also obtained copies of the "press packets" Ring issues to law enforcement partners, which include template social media posts for Facebook, Twitter, and Next-door; template press releases; sets of key talking points to stick to; and scripted answers to frequently asked questions.

Neighborhood watching

Amazon purchased Ring in early 2018 for about $1 billion. "Our mission to reduce crime in neighborhoods has been at the core of everything we do at Ring," the company's CEO said at the time, adding that the acquisition would "accelerate" the company's business.

Consumers buy the camera systems for their homes. Law enforcement can then access a portal site, showing a map of all the cameras in their jurisdiction, allowing them to request footage from specific private individuals as desired. It's the modern version of a neighborhood watch.

(After we published this story, a spokesperson from Ring reached out to specify that law enforcement can only submit video requests "in a given area" when actively investigating a case, that user consent is required for sharing footage, and that law enforcement can't see who received a request or declined to share their footage.)

More than 200 law enforcement agencies around the country have

partnerships with Ring, Vice Motherboard reported Monday. Those partnerships provide police departments with portal access and a certain number of free devices, as well as discounts for officers to buy their own. But this deal also essentially require cops to become auxiliary salesmen.

“Officers are NOT sales reps for RING and need to be careful not to suggest this company over other competitors,” an officer wrote in one of the emails Gizmodo obtained. But, the officer added, “We want to encourage downloads of the app.”

A separate Motherboard report outlines the agreement Amazon has with police in Lakeland, Florida, which includes the requirement for police to “engage the Lakeland community with outreach efforts on the platform to encourage adoption of the platform/app.”

Problems abound

The devices, while convenient for homeowners, may cause more trouble than they solve. Cnet reports today that Ring systems tie up police resources with copious false alarms. The system throws up flags for such threats as cars driving in neighborhoods or people walking nearby, a police representative told Cnet.

The constant notifications users receive, false alarms or not, may also be giving owners the impression that crime is pervasive in their area, even when the opposite is true. This can lead to a sense of “paranoia,” as The Outline put it.

The result can be anti-neighborly behavior, promoted by a service that purports to improve your neighborhood.

Privacy risks abound for anyone and everyone who lives in a Ring-filled neighborhood—and of course, the negative effects are not evenly distributed. People of color are far more likely to be targeted by police, and Ring doesn’t help.

“Amazon is dreaming of a dangerous future, with its technology at the center of a massive decentralized surveillance network,” ACLU attorney Jacob Snow wrote in December.

In ACLU testing, Snow said, the facial recognition software Amazon has proposed adding to Ring frequently churns up incorrect results, especially for women and people with dark skin, making bias more likely, not less.

Update:

https://arstechnica.com/?p=1543855

Cybersecurity officials warn state and local agencies (again) to fend off ransomware

Enlarge / Georgia State Police and Capitol Police had their laptops taken offline by ransomware in the latest of many attacks on state and local government agencies.

reader comments

34 with 23 posters participating

Share this story

Yesterday, the Georgia Department of Public Safety revealed that laptop computers in state police and Capitol police

vehicles—as well as laptops used by Georgia's Motor Carrier Compliance Division (the officers who operate trucking scales and safety spot checks)—had been taken offline by ransomware. The attack comes a week after Louisiana Governor John Bel Edwards declared a statewide emergency after "a malware attack on a few North Louisiana school systems," bringing state resources to assist in the response. And also last week, the city power company in Johannesburg, South Africa, was hit by ransomware, taking down payment systems and causing power outages.

These are just the latest episodes in a long line of state and local government organizations that have fallen to ransomware attacks. As Louisiana was declaring a state of emergency, the Board of Estimates of the City of Baltimore was approving $10 million in spending to recover from the city's nearly month-long IT outage caused by the RobbinHood ransomware. So today, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) issued a warning urging organizations to take immediate steps to protect themselves against ransomware attacks. The hope is that state and local agencies will heed the warning and blunt the damage being done by recent ransomware variants.

The three steps urged by CISA, MS-ISAC, NGA, and NASCIO are fairly basic security hygiene: run daily backups, train staff on "cybersecurity awareness," and "revisit and refine cyber incident response plans." Unfortunately, these three steps may be beyond the capabilities of the organizations most likely to be hit by ransomware—school districts, government agencies, and small and mid-sized businesses that have IT budgets that place them below the information security poverty line.

Monroe City Schools in Louisiana apparently had backups in place and managed to respond quickly to what Superintendent

Brent Vidrine confirmed was a targeted ransomware attack. The attack shared techniques used in the Ryuk ransomware strikes on a pair of Florida local governments and Georgia's Judicial Council and Administrative Office of the Courts last month.

"They were given some email addresses, but we did not contact anybody," Vidrine said during a July 16 school board meeting. "We had our systems protected."

The school system's IT department restored servers from a previous backup and was sweeping all computer systems for remaining malware before bringing them back onto the network. An investigation is ongoing.

But many school systems remain at risk. As Ars has previously reported, many districts are particularly vulnerable to ransomware attacks; based on security scan data, many school districts in the United States still have systems running vulnerable versions of the Windows SMB file sharing protocol directly exposed to the Internet. A review of recent data found more than 600 servers associated with school districts still running SMB version 1 on systems exposed to the Internet—more than two years after Microsoft issued patches and warnings about the vulnerability of those systems and a National Security Agency exploit of that vulnerability was leaked by Shadow Brokers.

In a press release today, a spokesperson for Louisiana's Sabine Parish School Board said that the attack on the school system's networks is "still under investigation," and that state agencies—including the Louisiana Office of Technology Services, National Guard and Air National Guard "are aiding in these efforts." The spokesperson said that there was no evidence that student or staff personal data was stolen in the attack. School is scheduled to open on August 12 in Sabine Parish; there's no word on whether the ransomware attack will affect that scheduled start date.

https://arstechnica.com/?p=1543587

Privacy group asks court to reconsider FTC’s $5 billion Facebook deal

Enlarge / Thumbs down.
Getty Images | Ted Soqui

reader comments

37 with 26 posters participating

Share this story

A group of privacy and consumer organizations is asking a federal court to slow its roll on approving the Federal Trade Commission’s $5 billion settlement with Facebook, saying it doesn’t do nearly enough to protect individuals.

The Electronic Privacy Information Center (EPIC) filed the motion to intervene (PDF) with the US District Court in Washington, DC, on Friday, asking the court to let it and other privacy advocacy groups file comments in a “careful review of the fairness and adequacy” of the proposed settlement.

The agreement between Facebook and the FTC, as announced last week, includes a record-setting $5 billion fine and mandates changes to Facebook’s reporting structure and oversight for

privacy-related matters.

As with any other settlement, the consent decree between Facebook and the FTC is not final until after a judge approves. EPIC is specifically asking the court not to rubber-stamp it but instead to allow it and other privacy organizations to file briefs to the case and to schedule a hearing to review privacy-related issues.

The settlement is not "adequate, reasonable, or appropriate," EPIC said in its filing. "Its scope goes far beyond the dispute in question, extinguishing all 26,000 pending consumer complaints" made about Facebook prior to June 2019.

"The proposed settlement is clearly not in the public interest, as it leaves consumer complaints unaddressed while still failing to ensure consumer privacy on Facebook," the group continued. "This court has a mandate not to 'stand by and approve any consent decree placed before it' and 'is not obliged to accept one that appears to make a mockery of judicial power' like the consent decree proposed in this case."

A collection of other advocacy groups, including Public Citizen, the Consumer Federation of America, the Center for Digital Democracy, the Campaign for a Commercial-Free Childhood, Color of Change, and Open Markets, all issued statements supporting the suit and expect to be involved with it going forward if the court allows.

"The public has a right to know what laws Facebook violated," said Color of Change Senior Campaign Director Brandi Collins-Dexter. Corporations should face consequences for violating the public trust, not be given a rubber stamp to carry out business as usual."

EPIC and the groups joining it are far from alone in criticizing the settlement. Other groups, such as Consumer Reports and the EFF, called for Congress to pass some kind of

legislation protecting consumer privacy going forward.

https://arstechnica.com/?p=1542739

WannaCry slayer, malware author Marcus Hutchins sentenced to time served

Enlarge / Hutchins, right, walks to court with his lawyers in 2017.
Joshua Lott/Getty Images

reader comments

20 with 14 posters participating, including story author

Share this story

British security expert and onetime malware developer Marcus Hutchins has been sentenced to time served, he announced in a Friday tweet.

Hutchins became famous in the security world in 2017 after he inadvertently stopped the WannaCry malware outbreak by registering a domain name that served as a kill switch for the sophisticated malware. Yet Hutchins, now in his mid-20s, had a dark past, having developed banking malware earlier in his life. At the time of his WannaCry efforts, Hutchins was already under investigation by US authorities for creating two banking trojans in the early 2010s.

Hutchins was arrested in August 2017 during a visit to the United States. He initially denied any role in developing malware. However, during his detention, federal prosecutors intercepted phone conversations in which he reportedly made incriminating statements. Under pressure from the authorities, Hutchins eventually came clean, admitting to his role in developing the malware. He took a plea deal in April.

“I regret these actions and accept full responsibility for my mistakes,” Hutchins wrote at the time. “Having grown up, I’ve since been using the same skills that I misused several years ago for constructive purposes. I will continue to devote my time to keeping people safe from malware attacks.”

Hutchins could have been sentenced to as many as 10 years in prison for his crimes. Instead, he received the lightest possible sentence: time served.

“Incredibly thankful for the understanding and leniency of the judge, the wonderful character letter you all sent, and everyone who helped me through the past two years, both financially and emotionally,” Hutchinson wrote after the sentence was announced.

Hutchins developed malware for stealing banking info

Hutchins has admitted to developing two pieces of malware known as UPAS Kit and Kronos. Both pieces of software were banking trojans—Kronos was an updated version of UPAS Kit with expanded capabilities.

According to the prosecutor’s sentencing memo in the case, Kronos was “designed to give the attacker the ability to steal banking credentials from victims’ computers using a process called keylogging.” The software could also grab data from Web forms filled out by a victim and inject malicious code into a

website visited by the victim. It also included virtual network connection capabilities, allowing a hacker to remotely control a victim's computer.

Prosecutors said that Hutchins developed the software and relied on a pseudonymous co-conspirator known as "Vinny" to market it to the hacking underworld.

"Since 2014, Kronos has been used to infect numerous computers around the world and steal banking information," prosecutors wrote. Kronos usage continues today.

Hutchins hoped to earn more than $100,000 per year from the software, but he reportedly once complained to a friend that he wasn't making as much money as he expected. Now, he says he's going to devote his career to fighting against malware instead of creating it.

https://arstechnica.com/?p=1542417

Trump threatens retaliation against France over digital service tax

Enlarge / US President Donald Trump speaks during the Conservative Political Action Conference (CPAC) in National Harbor, Maryland, on Saturday, March 2, 2019.

reader comments

106 with 80 posters participating

Share this story

US President Donald Trump is threatening to retaliate after French President Emmanuel Macron signed legislation imposing a 3% tax on digital transactions.

“France just put a digital tax on our great American technology companies,” Trump tweeted. “If anybody taxes them, it should be their home Country, the USA.”

The new French tax isn’t specific to American companies, but it is designed to target big companies in general—and the world’s big technology companies are disproportionately based in the United States. Companies will need to pay the tax if they generate more than €25 million ($28 million) in French revenue and €750 million ($840 million) worldwide.

In a statement earlier this month, the office of the US Trade Representative argued that the tax “will amount to de facto discrimination against US companies” because the income thresholds are designed to tax big, global—often American—companies while “exempting smaller companies, particularly those that operate only in France.”

“We will announce a substantial reciprocal action on Macron’s foolishness shortly,” Trump added in his tweet. “I’ve always said American wine is better than French wine!”

An official White House statement made the same point in more diplomatic language.

“The United States is extremely disappointed by France’s decision to adopt a digital-services tax at the expense of US companies and workers,” a White House statement said. “France’s unilateral measure appears to target innovative US technology firms that provide services in distinct sectors of the economy.”

The White House said that Trump had shared his concerns

directly with President Macron during a conversation last week. But France passed the new legislation anyway.

It’s not clear what kind of retaliatory measures, if any, the Trump administration will take in the coming days or weeks. In recent months, Trump has been engaged in high-profile trade disputes with China, Mexico, and other countries.

https://arstechnica.com/?p=1542373

Louisiana declares state of emergency in response to ransomware attack

Enlarge / To the credit of the three school districts affected, at least nobody’s trying to pay the Danegeld.

reader comments

93 with 56 posters participating, including story author

Share this story

This Wednesday, Louisiana Governor John Bel Edwards declared a state of emergency in response to ransomware attacks on three public school districts.

There’s no word so far on which ransomware variant has hit the school districts or what the exact extent of damages is. Eddie Jones, principal of Florien High School (a school in one of

the three affected districts), told KSLA News that his technology supervisor received an alert on his phone at 4am Sunday about unusually high bandwidth usage. Shortly afterward, investigators discovered ransomware on the school servers. Jones says “anything and everything housed solely on the School District’s servers” was lost, including 17 years of his own personal documents.

The Sabine and Morehouse district ransomware attacks this week follow an attack on the Monroe City school district last week. Morehouse parish claims not to have been affected to the extent of the other two parishes, and it states that “all major systems, including payroll, are operational.”

The three school districts have all made statements to the effect that they do not believe sensitive or private information was compromised, or that any “unauthorized access” occurred. This seems to be an overly confident statement, given Jones’ statement that his district’s first awareness of the problem stemmed from unusually high bandwidth usage. Still, there’s no way to know for certain until the statewide effort to address the attacks and look for traces of their authors concludes and more concrete information is disseminated.

Louisiana’s declaration of a state of emergency follows a model established by Colorado in the wake of a ransomware attack there in March 2018. In Colorado, the declaration of emergency only came after a week the Colorado Office of Information Technology’s overwhelmed and short-staffed IT department spent trying to disinfect more than 2,000 infected machines. Declaring a state of emergency allows the National Guard’s resources and personnel to be brought in.

Edwards’ emergency declaration also freezes the prices of services and goods in the designated emergency area to those “ordinarily charged… in the same market area at or immediately before the state of emergency.” This is likely a pre-emptive

measure to prevent local IT consulting services the schools may contract from hiking their rates while the schools are desperate.

This declaration is the first activation of the emergency support functions of Louisiana's Cybersecurity Commission, which was first established by Governor Edwards in 2017. Edwards declared then that Louisiana is "an international leader in regards to cybersecurity capabilities." How well the state responds to these attacks—including discovering the actors behind them, and establishing and truthfully disclosing the actual nature and extent of data both lost and exfiltrated during them—will do much toward outlining the veracity of that statement.

https://arstechnica.com/?p=1542303

You can go claim at least $125 from the Equifax settlement right now

Bloomberg | Getty Images

reader comments

86 with 64 posters participating

Share this story

There is at long last a silver lining for the 144 million of

us who had our personal data leaked in the gigantic 2017 Equifax data breach: cash money.

Under the terms of its settlement with the Federal Trade Commission, Equifax established a fund of at least $300 million to compensate individuals who had their data compromised.

You, the individual, get to choose which claim to file: up to 10 free years of credit monitoring service, or a $125 check.

Additionally, you may also be eligible to claim up to $500 in compensation for time you spent dealing with the fallout of the breach, and up to another $20,000 if you suffered identity theft you can tie back to it.

How to choose?

Ars is by no means a financial advisory site. But if you can, claim the cash. Credit monitoring can be a useful service, but it generally has major limits and doesn’t really protect you from fraud.

Here’s the catch for this Equifax offer: You can only claim the cash in the settlement *if* you certify you already have a credit monitoring service. Luckily, there’s a very good chance that you do, or you easily could without much trouble.

Many banks, credit unions, and credit card companies offer free credit monitoring services to customers through a partnership with one of the three major credit bureaus (Equifax, Experian, and TransUnion). Services like AAA, professional organizations, and alumni organizations also frequently offer low- or no-cost credit monitoring programs through similar partnerships.

If you dig around in your wallet and your inbox, there are decent odds you’ll find you already have an affiliation with some entity that can hook you up,

You may even already have free credit monitoring services as the result of a previous data breach (including even this one), as it has become standard practice for everybody and their grandmother to offer it to consumers following a "cybersecurity incident."

How to apply

Filing a claim, at least, is reasonably straightforward.

Step 1: Check your eligibility. Use the eligibility lookup tool to see if you were among the 144 million US residents who was affected by the breach.

If the answer is no, congratulations! Your data is doubtless still included in dozens of other breaches, of course, but not this one. Lucky you. If the answer is yes, proceed to…

Step 2: File a claim. You can use an online form or, if you prefer, send in a paper claims form.

On the first page of the online claim form, fill in your personal information and click next. The second page will ask you to choose what you want to claim: cash or credit monitoring. Selecting either option will bring up an explanation of your choice. If you select credit monitoring, you will also have the option to add an additional six years of service, provided by Equifax, to the initial four years provided by Experian.

Once you've chosen between credit monitoring or the $125 check, the next page gives you the option to claim compensation for up to 20 hours of time spent dealing with the breach at $25 per hour. If you don't want to claim any hourly compensation, just hit "next." If you do elect to claim time, and specify more than 10 hours of work, you must upload supporting documentation showing what you did.

Finally, the form will ask if you lost or spent money as a

result of trying to prevent or recover from identity theft linked to the incident. If you select “yes,” you will be presented with a form asking you to provide detailed information and to upload documents supporting your claim. Funds spent freezing your credit or paying for credit monitoring in the wake of the breach *are* eligible for recompense in this section.

Finally, you select how you want to be paid any compensation (in cash or on a prepaid debit card), review your answers, and sign to submit. Take a screenshot or save a PDF of your claim confirmation number after you submit just in case.

For more information, the Equifax Breach Settlement site has a detailed FAQ, or you can read about it on the FTC’s website.

https://arstechnica.com/?p=1542257

People forged judges' signatures to trick Google into changing results

Enlarge / Google CEO Sundar Pichai.

reader comments

78 with 63 posters participating

Share this story

It's not easy to convince Google to remove unflattering information about you from its search results. One of the few reasons Google will remove search listings if it gets a court order to do so. But getting a court order isn't easy, either. Courts have held that the First Amendment gives publications broad discretion to decide what kind of information to publish—especially if it's accurate.

As a result, some unscrupulous parties have taken an unethical—and likely criminal—shortcut: they sent Google fake court orders, complete with forged signatures from a judge. An investigation by CBS News uncovered more than 60 cases where someone used this tactic.

"CBS News sorted through thousands of these court orders and spotted small businesses from all across America trying to clean up their reputations," two CBS reporters write. "But we also spotted a problem: Dozens of the court documents were fakes."

CBS says that some are obviously fake, like one document with a case number of "1-2-3-4-5-6-7-8-9." Others appear to be more

subtle forgeries. The most recent fake document they found was filed in April. CBS reports that two of the documents were submitted by convicted sex offenders who hoped to scrub Google of references to their crimes.

Google says it works hard to catch this kind of fraud.

“We are always vigilant to protect our legal removals process from bad actors,” a company spokesman told Ars by email. “We have processes in place to verify the veracity of court orders, and if we are alerted to removals made in error, we will reinstate that content as appropriate.”

Forging a judge’s signature is a serious crime. In October, a New York man was sentenced to nine months in prison for “conspiring to forge a federal judge’s signature on counterfeit court orders that he submitted to Google to get negative reviews about his business removed from Google search results.” Between 2014 and 2017, the man created more than 10 fake court documents purporting to find negative reviews of his business to be defamatory and ordering them removed from search results.

https://arstechnica.com/?p=1542243

It’s official: US government approves T-Mobile/Sprint merger

Getty Images | alexsl

reader comments

71 with 53 posters participating

Share this story

The Justice Department today announced its approval of the T-Mobile/Sprint merger as part of a settlement that requires the merging companies to spin off several assets to Dish Network.

The DOJ decided against filing a lawsuit to block the T-Mobile US purchase of Sprint, even though it reduces the number of major mobile network providers from four to three. In exchange for its approval, the DOJ convinced the companies to sell Dish spectrum licenses, wholesale network access, and Sprint's prepaid business including subsidiaries Boost Mobile and Virgin Mobile. Boost and Virgin both resell Sprint network access instead of operating their own networks.

Dish would use its newfound assets to resell T-Mobile/Sprint service and to build its own network. The building-its-own-network part is far more crucial for Dish to effectively replace the competition eliminated by the merger, but this is expected to take several years.

The DOJ's approval is not the last one T-Mobile and Sprint need, because 13 states and the District of Columbia sued the companies to block the merger.

Dish "a faux competitor, not a real one"

Consumer advocates are rooting for the states in their lawsuit.

"This deal [with the DOJ] creates a faux competitor, not a real one, which is why I would bet on the states in their forthcoming court challenge," attorney Andrew Schwartzman of

the Benton Foundation told media outlets in a statement. Schwartzman led the Media Access Project, a public interest telecommunications law firm, from 1978 to 2012.

Schwartzman continued:

> *Dish is buying Boost, a brand which sells prepaid service to low-end consumers. Dish will start with none of the lucrative postpaid customers, no brand name and no retail network. Even if Dish successfully builds out its own network, that could not happen for several years, during which time the three big wireless companies will be able to lock in their customer and introduce their 5G technologies. In other words, rather than having Sprint as a weak fourth competitor, the combined companies will now face an extremely weak fourth competitor.*

The DOJ convinced five states to sign on to the settlement, namely Nebraska, Kansas, Ohio, Oklahoma, and South Dakota. But none of these are among the 13 states suing to block the deal.

Terms of the settlement as announced by the DOJ are as follows:

> *T-Mobile and Sprint must divest Sprint's prepaid business, including Boost Mobile, Virgin Mobile, and Sprint prepaid, to Dish Network Corp., a Colorado-based satellite television provider. The proposed settlement also provides for the divestiture of certain spectrum assets to Dish. Additionally, T-Mobile and Sprint must make available to Dish at least 20,000 cell sites and hundreds of retail locations. T-Mobile must also provide Dish with robust access to the T-Mobile network for a period of seven years while Dish builds out its own 5G network.*

New York Attorney General Letitia James vowed to continue the states' lawsuit against the merger. "The promises made by Dish and T-Mobile in this deal are the kinds of promises only

robust competition can guarantee," James said in a statement. "We have serious concerns that cobbling together this new fourth mobile player, with the government picking winners and losers, will not address the merger's harm to consumers, workers, and innovation."

DOJ defends settlement

DOJ antitrust chief Makan Delrahim said that the "settlement will provide Dish with the assets and transitional services required to become a facilities-based mobile network operator that can provide a full range of mobile wireless services nationwide."

The DOJ acknowledged that the "combination of T-Mobile and Sprint would eliminate head-to-head competition between the companies and threaten the benefits that customers have realized from that competition in the form of lower prices and better service." But the department argued that the required divestitures will allow Dish to replace the lost competition, ensuring that Americans will still have four facilities-based choices nationwide.

Federal Communications Commission Chairman Ajit Pai announced his support of the T-Mobile/Sprint merger in May. The FCC approval, which still needs a commission vote, is contingent on the divestiture of Boost Mobile and a guarantee that Boost will have access to the T-Mobile/Sprint network. Transferring licenses to Dish would likely require a further FCC approval, however.

Today, Pai said he's ready to move forward with a final FCC approval. "I plan to present my colleagues soon with a draft order, consistent with the [Justice] Department's filings, favorably resolving the FCC's review of the transaction," Pai said in a statement. He said that the merger will result in T-Mobile and Sprint "deploy[ing] a 5G network that would cover 99 percent of the American people."

But many critics of the merger are not convinced by the DOJ and FCC arguments. “If the merger goes forward, it would leave the United States with only three viable nationwide wireless-service providers even with these divestitures,” advocacy group Free Press said. “Approving the merger would crush competition, raise prices and eliminate thousands of jobs, according to union estimates. It would disproportionately harm low-income people and communities of color, who rely on robust competition among T-Mobile and Sprint and their subsidiaries to keep access affordable.”

The Rural Wireless Association, an industry group that represents small, rural carriers, also criticized the DOJ action.

“The conditions imposed on New T-Mobile by the consent decree are drastically insufficient to protect against the clear harms this market-consolidating merger would bring,” the RWA said. “Expecting Dish, a startup mobile carrier in its infancy, to be able to compete as a fourth nationwide network, with divested wireless assets from Sprint and T-Mobile and Boost’s MVNO customers, and subject only to a handful of requirements that will expire, spells disaster for American consumers.”

https://arstechnica.com/?p=1542227