Data for a whopping 26 million stolen payment cards leaked in hack of fraud bazaar

reader comments

23 with 21 posters participating

Share this story

A thriving online bazaar selling stolen payment card data has been hacked in a heist that leaked the records for more than 26 million cards, KrebsOnSecurity reported on Tuesday.

The 26 million figure isn’t significant only to the legitimate consumers and businesses who own the stolen cards or the financial institutions that issued them. Fortunately for the card owners, the database is now in the hands of affected financial institutions, who can invalidate and replace the cards.

The number, therefore, is perhaps a bigger deal because it represents a significant fraction of the world’s stolen-card inventory. Krebs said that Gemini Advisory, a company that monitors dozens of underground markets trafficking stolen card data, currently tracks a total of 87 million credit and debit card records. The haul of 26 million cards means that about a third of that supply has been taken out of circulation in a single swipe.

“With over 78% of the illicit trade of stolen cards attributed

to only a dozen Dark Web markets, a breach of this magnitude will undoubtedly disturb the underground trade in the short term," Gemini co-founder and CEO Andrei Barysevich told Krebs. "However, since the demand for stolen credit cards is on the rise, other vendors will undoubtedly attempt to capitalize on the disappearance of the top player."

BriansClub

The hacked market is called BriansClub, a site available at BriansClub[.]at that, for years, has imitated Krebs' site and likeness. The data taken in the hack shows that BriansClub acquired 1.7 million cards in 2015, 2.9 million in 2016, 4.9 million in 2017, 9.2 million in 2018, and 7.6 million in the first eight months of this year. Most of the pilfered data is composed of "dumps," the term card thieves use to describe data that's stored on the magnetic stripe of payment cards. The stolen dumps can be transferred to new cards that crooks use to buy electronics, gift cards, and other large-ticket items from big-box stores. An analysis based on how many of the cards had expiration dates in the future suggests that more than 14 million of the leaked records could still be valid.

Based on the pricing tiers listed on BriansClub, the haul represents about $414 million worth of lost sales, security intelligence firm Flashpoint told Krebs. By tracking the cards that were once available for sale and later removed, Flashpoint estimated that BriansClub has sold data for about 9.1 million cards for about $126 million. Federal prosecutors often value each stolen credit card record at $500, a sum that represents the average cost incurred from each compromised holder. Based on that estimate, the 9.1 million cards translates to about $2.27 billion in losses.

https://arstechnica.com/?p=1586127

Uber lays off another 350 workers amid ongoing losses

Enlarge / Uber CEO Dara Khosrowshahi.

reader comments

8 with 8 posters participating

Share this story

Uber is laying off another 350 workers, the company announced on Monday. Uber Eats and Uber's self-driving car team are among the divisions hit by job losses. TechCrunch obtained a copy of an email CEO Dara Khosrowshahi sent to Uber workers. It describes the layoffs as "difficult but necessary changes."

This is Uber's third round of layoffs for 2019. The company laid off 400 workers in its marketing department in July and 435 engineering and product workers in September. Some workers have also been asked to relocate.

Uber announced in August that it racked up record losses of $5 billion in the second quarter of 2019. It's important to note that the bulk of that figure represents one-time charges connected to Uber's May stock offering. Excluding those charges, Uber's ongoing burn rate has been around $1 billion in recent quarters. Third-quarter financial results are due out next month.

An Uber spokesperson told TechCrunch's Megan Rose Dickey that Monday's layoffs represented about 1% of the company's

workforce. That’s far too small to eliminate Uber’s losses. But every little bit helps.

Layoffs include Uber’s self-driving car unit, which has had a difficult time over the last 18 months. The division racked up millions of test miles before March 2018, when an Uber vehicle struck and killed pedestrian Elaine Herzberg in March 2018. Uber shut down testing for months after that death and then resumed testing on a vastly smaller scale in December 2018.

Toyota led a $1 billion investment in Uber’s self-driving unit in August 2019, but the company hasn’t indicated when it might resume large-scale testing, to say nothing of commercial deployment.

https://arstechnica.com/?p=1584805

AT&T charged customers for a corporate tax that it doesn’t have to pay

Enlarge / An AT&T store in Chicago.

reader comments

60 with 49 posters participating

Share this story

AT&T charged customers in Portland, Oregon for a corporate tax

that AT&T doesn't actually have to pay. AT&T has agreed to provide refunds to customers who were wrongly charged the tax over the past few months, but it's facing a lawsuit that seeks additional payments of at least $200 to each of those customers.

AT&T's mistake relates to Portland's new Clean Energy Surcharge, a 1% tax on retail sales in the city. AT&T has been passing this tax along to its mobile customers, even though the city law exempts utilities such as AT&T from the tax.

"The city only recently notified us that we are exempt from the tax," AT&T said a statement Friday, according to The Oregonian. "We will be issuing refunds to our customers."

The fee, listed on AT&T bills as a Portland Clean Energy Surcharge, was as low as 5¢ per month. The Oregonian wrote that one of its employees "reported being charged 23 cents in April, 7 cents in May and 5 cents every month after until September.

But AT&T's decision to charge the fee at all is concerning, especially in light of AT&T's long history of charging hidden fees that aren't disclosed in its advertised prices. There's been confusion among other entities about who actually has to pay the Portland tax. But it's possible AT&T should have realized that it didn't have to pay the tax because of the exemption for utilities.

Portland says the exemption applies to "any entity operating a utility within the City" and says that utilities include "those entities defined in the Utility License Law (ULL) definitions section of PCC 7.14.040(I) 'Utility' and those entities that provide the services listed in PCC 7.14.040 (H), 1 through 8."

Mobile service—what AT&T offers—is #7 on that list.

We asked AT&T why it started charging customers before making

certain that it actually had to pay the tax, and whether the tax applies to other AT&T services such as DirecTV. We also asked AT&T whether it actually paid any money under the new tax to Portland before realizing it was exempt. We'll update this article if we get any answers.

"The company wouldn't say how many people will be refunded, when it will occur or how much money has been collected," The Oregonian wrote.

UPDATE 2:48pm ET: AT&T responded to Ars and provided the same statement it gave to The Oregonian. The company also told us that the wrong charges happened because Portland didn't exempt mobile providers from the tax until September of this year.

Portland's website says on one page that the utility exemption and other tax changes were "adopted following their public hearing on April 3, 2019." But the page describing the utility exemption says it was adopted on September 10. Based on that, it seems that the change was made public in April and implemented in September. Businesses don't actually have to pay the taxes until April 2020.

AT&T told Ars that it will issue refunds "in the coming few months."

Original story resumes:

AT&T also charges property-tax fee

Last week, we wrote about another strange fee that AT&T charges. AT&T charges business Internet customers a "property tax" fee in multiple states to cover its own property taxes and recently raised the fee in California from 2.92% to 7%.

AT&T isn't required to pass these fees along to customers in separate line items, but doing so lets AT&T advertise lower prices than it actually charges. The practice also lets AT&T raise customer bills whenever it wants to, even when customers

are under contracts that require them to pay early termination fees if they cancel service.

Class-action lawsuit

AT&T's actions in Portland led to a class-action lawsuit being filed against it on Friday. The complaint filed in Multnomah County Circuit Court said:

> *In an effort to profit and to obtain an unfair advantage over its competitors, AT&T misled thousands of Oregon customers into paying unlawful five cent surcharges that AT&T was not permitted to collect. AT&T only said it would refund the money it wrongfully collected from Oregon customers after AT&T got caught. AT&T still has not agreed to pay its customers the $200 penalties and interest they are entitled to under Oregon law as result of AT&T's unlawful trade practices.*

The lawsuit says that AT&T "knew or should have known" that its wireless service was not subject to the clean-energy tax.

"If you steal from a bank, you can't just refund the money you stole when you get caught and call it good," plaintiffs' attorney Michael Fuller told the Willamette Week. "AT&T stole from Oregon customers, and Oregon law entitles customers who were assessed the unlawful surcharge to $200 statutory damages, and punitive damages to punish AT&T and deter other corporations from charging illegal fees."

Portland says that its clean-energy tax "is anticipated to bring $54 to 71 million in new revenue for green jobs and healthy homes for all Portlanders." The fund being paid for by the tax is expected to start issuing clean-energy grants in July 2020.

Portland voters approved the tax in November 2018, and tax payments for 2019 retail sales are due on April 15, 2020. But

businesses that make estimated quarterly payments began paying the tax in April of this year, The Oregonian wrote.

https://arstechnica.com/?p=1584591

Sikorsky makes its bid for Army’s next scout copter

Enlarge / An artist’s rendering of Sikorsky’s proposed Raider X attack-scout helicopter.

reader comments

32 with 18 posters participating, including story author

Share this story

As the Association of the US Army (AUSA) kicks off its annual Washington, DC meeting—a combination of Army conference and land-warfare trade show—Lockheed Martin’s Sikorsky unit has unveiled the company’s entry into the Army’s Future Attack Reconnaissance Aircraft (FARA) design shoot-out. As predicted, the “Raider X” is based heavily on the S-97 Raider demonstrator that Sikorsky showed off at the 2015 AUSA conference.

But there are some significant differences in the proposed design, differences that echo an earlier attempt by the Army to build a light-attack helicopter. Much like Bell’s Invictus design, the Raider X’s stealthy design bears a passing resemblance to the Boeing/Sikorsky RAH-66 Comanche.

[embedded content]
Sikorsky’s video introducing the Raider X design.
The Raider X has the same side-by-side crew configuration as the Raider demonstrator. But instead of additional crew and passenger seating, it has modular internal weapons and sensor mounts, reducing its potential radar cross-section. As with Bell’s Invictus, the design included a “Modern Open Systems Architecture”-based avionics suite, theoretically allowing for rapid and low-cost upgrades over the life of the aircraft. And as with the S-97 before it, the Raider X is designed to be “optionally manned”—meaning that it can be flown remotely or operate autonomously for missions that either don’t require an aircrew or would put aircrew at an unacceptable risk.

Like the S-97 (and Sikorsky’s X2 experimental helicopter), the Raider X design uses coaxial rigid rotors designed for better performance at high speeds and a “pusher” propeller that takes the thrust load off the rotors. The coaxial rotors help to fight the retreating blade stall effect that has previously limited helicopter airspeeds, allowing the Raider X design to reach advertised speeds in excess of 250 knots (over 287mph, or 463km/h). The reduced footprint of the coaxial rotors allows the helicopter to fly in more confined urban spaces and other environments. And the design can fly at altitudes above 9,000 feet and maneuver while banking over 60 degrees—another leap beyond traditional single-rotor helicopters.

https://arstechnica.com/?p=1584549

Visa, Mastercard, Stripe, and

eBay all quit Facebook's Libra in one day

Getty / Aurich Lawson

reader comments

44 with 38 posters participating

Share this story

Facebook's embattled Libra project suffered a major blow on Friday as four payment processors—Stripe, Visa, Mastercard, and Mercado Pago—withdrew from participation in the Libra Association, the Geneva-based group Facebook created to develop the virtual currency. eBay also announced its resignation Friday. eBay's former subsidiary, PayPal, quit the group last week.

The timing is not a coincidence. The Libra Association is scheduled to hold its first official meeting on Monday. At that meeting, members will be asked to make binding commitments to the project. So for members who weren't prepared to commit to the project, Friday was a good day to get out.

But this is an awkward development for Facebook. When the company introduced Libra earlier this year, it said it hoped to grow Libra's membership from 27 companies to more than 100 by the time the Libra network launched in 2020. Instead, the association's membership has fallen to 22 companies.

Facebook could have used help from payment companies

The even more ominous sign for Facebook is *who* bowed out. All but one of the payment-processing companies that originally signed up for Libra have now withdrawn (the one exception so far is Netherlands-based payment company PayU, which signaled its continued support on Wednesday). Their participation would have been significant because Libra faces a lot of skepticism from regulators. Companies like Visa and Mastercard have ample experience with regulations related to payments and could have helped Libra navigate those issues. But they also had the most to lose from confrontations with regulators.

One of the trickiest issues for any cryptocurrency is how to interact with the conventional financial system. Regulators often focus their enforcement efforts on intermediaries who help customers swap conventional currencies for cryptocurrencies.

Libra's official documentation is vague on exactly how this will work, stating only that the Libra Association will establish a network of "authorized resellers" to make sure customers can easily trade their dollars and euros in for facebucks.

Payment processors like Visa, Mastercard, and Stripe could have been helpful here—both with designing a system that's secure and user-friendly, and also with securing approval from regulators. Their departure means that Facebook will have to figure out many of these issues on its own.

Libra already faced an uphill fight

The Libra project has been met with skepticism or even outright hostility by regulators in the United States and overseas. The Libra Association has yet to clearly explain how

it’s going to comply with the broad range of regulations that govern financial networks. The project faces skepticism from policymakers who aren’t sure Facebook can be trusted to handle peoples’ money responsibly, regardless of how the network is designed.

At the same time, Libra has not been popular in the conventional blockchain world. Many supporters of Bitcoin and Ethereum were attracted by these networks’ decentralized architecture. They like the idea of a financial system that’s outside the control of any single organization.

The Libra network, in contrast, will be completely under the control of a single private group—the Libra Association. For many cryptocurrency enthusiasts, that represents a step backwards. It’s not clear if it’s even possible to marry the technical advantages of an open blockchain with the heavy regulatory burden the law imposes on conventional payment networks.

https://arstechnica.com/?p=1584207

Activists’ phones targeted by one of the world’s most advanced spyware apps

reader comments

12 with 10 posters participating

Share this story

Mobile phones of two prominent human rights activists were repeatedly targeted with Pegasus, the highly advanced spyware made by Israel-based NSO, researchers from Amnesty International reported this week.

The Moroccan human rights defenders received SMS text messages containing links to malicious sites. If clicked, the sites would attempt to install Pegasus, which as reported here and here, is one of the most advanced and full-featured pieces of spyware ever to come to light. One of the activists was also repeatedly subjected to attacks that redirected visits intended for Yahoo to malicious sites. Amnesty International identified the targets as activist Maâti Monjib and human rights lawyer Abdessadak El Bouchattaoui.

Serial pwner

It’s not the first time NSO spyware has been used to surveil activists or dissidents. In 2016, United Arab Emirates dissident Ahmed Mansoor received text messages that tried to lure him to a site that would install Pegasus on his fully patched iPhone. The site relied on three separate zeroday vulnerabilities in iOS. According to previous reports from Univision, Amnesty International, and University of Toronto-based Citizen Lab, NSO spyware has also targeted:

- 150 people, including US citizens and opposition critics chosen by an ex-president of Panama
- 22 journalists and activists researching corruption in the Mexican government
- Two people—one an Amnesty International researcher and the other a dissident—in Saudi Arabia

A potent attack exploiting a vulnerability in both the iOS and Android versions of WhatsApp was used to install Pegasus, researchers said five months ago. Last week, Google also

uncovered evidence NSO was tied to an actively exploited Android zeroday that gave attackers the ability to compromise millions of devices. It’s not known who the targets were in either of those attacks.

This week’s report said that the targeting of the two Morrocan human rights defenders began no later than November 2017 and likely lasted until at least July of this year. In 2017 and 2018, the men received text messages that contained links to sites including stopsms[.]biz and infospress[.]com, which Amnesty International previously said was part of NSO’s exploit infrastructure. Other domains included revolution-news[.]co (which Citizen Lab has identified as tied to NSO) and the previously unknown hmizat[.]co (which appears to impersonate Moroccan ecommerce company Hmizate).

Suspicious redirects

Then, starting this year, Monjib’s iPhone started being suspiciously redirected to malicious sites. An analysis of logs Safari stores of each visited link and the origin and destination of each visit showed the redirects happened after Monjib entered “yahoo.fr” in the address bar of his Safari browser. Under normal conditions, Safari would quickly be redirected to the encrypted link https://fr.yahoo.com/. But on at least four occasions, from March of this year to July, the activist was instead diverted to links including

hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz

and

hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz#048634787343287485982474853012724998054718494423286

.

These redirections were possible only because the initial

connection to Yahoo wasn't protected by an encrypted HTTPS connection. In the redirection from July, Monjib again tried to access Yahoo, but instead of typing an address in the browser, he searched for "yahoo.fr mail" on Google. When he clicked the result, he landed on the correct site. Authors of this week's report wrote:

> *We believe this is a symptom of a network injection attack generally called "man-in-the-middle" attack. Through this, an attacker with privileged access to a target's network connection can monitor and opportunistically hijack traffic, such as Web requests. This allows them to change the behavior of a targeted device and, such as in this case, to re-route it to malicious downloads or exploit pages without requiring any extra interaction from the victim.*
>
> *Such a network vantage point could be any network hop as close as possible to the targeted device. In this case, because the targeted device is an iPhone, connecting through a mobile line only, a potential vantage point could be a rogue cellular tower placed in the proximity of the target or other core network infrastructure the mobile operator might have been requested to reconfigure to enable this type of attack.*
>
> *Because this attack is executed "invisibly" through the network instead of with malicious SMS messages and social engineering, it has the advantages of avoiding any user interaction and leaving virtually no trace visible to the victim.*
>
> ***We believe this is what happened with Maâti Monjib's phone. As he visited yahoo.fr, his phone was being monitored and hijacked, and Safari was automatically directed to an exploitation server which then attempted to silently install spyware.***

Amnesty International

Amnesty International researchers said they believe at least one of the injections “was successful and resulted in the compromise of Maâti Monjib’s iPhone.” The researchers continued:

> *Whenever an application crashes, iPhones store a log file keeping traces of what precisely caused the crash. These crash logs are stored on the phone indefinitely, at least until the phone is synced with iTunes. They can be found in Settings > Privacy > Analytics > Analytics Data. Our analysis of Maâti Monjib’s phone showed that, on one occasion, all these crash files were wiped a few seconds after one of these Safari redirections happened. We believe it was a deliberate clean-up executed by the spyware in order to remove traces that could lead to the identification of the vulnerabilities actively exploited. This was followed by the execution of a suspicious process and by a forced reboot of the phone.*

A preponderance of evidence

The researchers said they can't prove the redirections were the work of NSO products or services, but they say evidence strongly suggests a link. The evidence includes similarities between the known NSO URLs contained in the SMS messages—such as

hxxps://videosdownload[.]co/nBBJBIP

and the URLs used in the redirects —such as

hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz

. Both are composed of generic domain names followed by a pseudorandom alphanumeric string of seven to nine characters.

The researchers also found a similar network injection capability described in a document titled Pegasus—Product Description that was found in the 2015 hack of NSO competitor Hacking Team. The NSO document calls the redirect capability a "Tactical Network Element" and describes how a rogue cell tower could be used to identify a targeted phone and remotely inject and install Pegasus.

Amid growing criticism, NSO Group—which earlier this year was valued at $1 billion in a leveraged buyout by UK-based private equity firm Novalpina Capital—promised in September to follow a human rights policy based on these guiding principles. A key aspect of the policy was to "investigate whenever the company becomes aware of alleged unlawful digital surveillance and communication interception of NSO products."

In a response to this week's report, NSO officials wrote:

> *As per our policy, we investigate reports of alleged misuse of our products. If an investigation identifies actual or potential adverse impacts on human rights, we are proactive and quick to take the appropriate action to address them.*

> *This may include suspending or immediately terminating a customer's use of the product, as we have done in the past.*
>
> *While there are significant legal and contractual constraints concerning our ability to comment on whether a particular government agency has licensed our products, we are taking these allegations seriously and will investigate this matter in keeping with our policy. Our products are developed to help the intelligence and law enforcement community save lives. They are not tools to surveil dissidents or human rights activists. That's why contracts with all of our customers enable the use of our products solely for the legitimate purposes of preventing and investigating crime and terrorism. If we ever discover that our products were misused in breach of such a contract, we will take appropriate action.*

In an email, an NSO representative said appropriate action could include shutting down a customer's access to the NSO system, which the company has done three times in the past.

Amnesty International, for its part, remains skeptical.

"In the absence of adequate transparency on investigations of misuse by NSO Group and due diligence mechanisms, Amnesty International has long found these claims spurious," this week's report said. "With the revelations detailed in this report, it has become increasingly obvious that NSO Group's claims and its human rights policy are an attempt to whitewash rights violations caused by the use of its products."

https://arstechnica.com/?p=1584181

AT&T raises prices 7% by making its customers pay AT&T’s property taxes

Getty Images | Aurich

reader comments

205 with 134 posters participating

Share this story

Telecom companies like AT&T *love* creating new fees to tack on customer bills, and they *really love* raising those fees after customers sign contracts that are supposed to lock in a consistent price.

It’s a win-win for the company, but not the customer: AT&T gets to advertise a lower price than it actually charges and has a mechanism for raising customer bills whenever it wants to. Customers who are angry enough to cancel service would have to pay early termination fees.

This story about AT&T thus isn’t likely to surprise anyone, but it’s possible you haven’t heard about the particular fee we’ve been looking into this week. AT&T has been charging business Internet customers a “property tax” fee, claiming it needs to charge this to recover AT&T’s own property taxes. AT&T has been charging the fee for at least a couple of years and just hit customers in California with an increase that more doubled the fee.

A first-bill surprise

Scott Phillips, owner of a small business called Valley View Media in Santa Clarita, California, signed up for AT&T fiber Internet service and a block of static IP addresses, agreeing to an all-in price of $95 a month. His order summary, which he shared with us, specifically says that the $95 ongoing monthly price includes taxes and fees. The document makes no mention of property taxes.

But when Phillips got his first bill on July 1, which he also shared with Ars, it contained this notice:

> *Effective October 1, 2019, there will be an increase in the AT&T Cost Assessment Charge used to recover AT&T property taxes. The monthly rate will change from 2.92% to 7.00% of your total AT&T Business Internet, Phone and/or U-verse TV monthly charges. This charge is not a tax or fee that the government requires AT&T to collect from its customers.*

That first bill included exactly $95 in recurring charges, consisting of $60 for 100Mbps download Internet and $35 for the static IP addresses, just as AT&T promised. (There was also a one-time installation fee of $99.) While the property-tax fee notice on that first bill suggested he was already paying a 2.92% charge on top of the $95, the first few bills didn't actually include a separate property-tax fee.

But when Phillips' October bill came, AT&T imposed the 7% property-tax fee, adding $6.65 to the $95 base price. The actual billing increase was thus for the full 7%, not just for the difference between 2.92% and 7%.

"Don't you wish you could pass on the cost of *your* property taxes to your clients?" Phillips asked rhetorically. "I sure wish I could. But we both know that's really not ethical."

Phillips had switched from Charter Spectrum Internet to AT&T

after a price dispute. He said that Charter started offering much lower prices to new customers, charging $50 less for the same service, but the company refused Phillips' request for a similar discount. Phillips told us that ditching AT&T to go back to Charter now would result in a $225 early termination fee, consisting of $25 for each month left in his deal.

"What gets me the most about paying AT&T's CAC [Cost Assessment Charge] is that it's basically paying their taxes for them and they are so blatant about it, like 'What are you gonna do about it, huh?' They know they have a stronghold on the market in our area," Phillips said.

Phillips' order summary links to AT&T's Internet terms of service, but the specific page it links to makes no mention of property taxes. From there, you have to follow two more links to get to the AT&T Internet Business Fee Schedule, which lists the property-tax charge. The document says that as of October 1, the charge varies between 2.76% and 7% depending on the state, and it's not applied in all states or to certain customers.

- Scott Phillips' AT&T order summary: $95 in monthly costs and a one-time installation fee of $99.
- Scott Phillips' first AT&T bill warns of an impending price increase.
- The property-tax line item from Scott Phillips' October bill is rather vague.

"I pay my own property tax"

AT&T has been charging the property-tax fee to business customers since at least mid-2017. An AT&T business DSL customer in Oklahoma complained about it on Reddit at the time, saying the then-new fee was 1.08% of the monthly bill.

In January 2019, an AT&T customer complained in a DSLReports

forum that the property-tax fee was raised from 2% to 6.69%. “So I gotta ask—did their ‘property taxes’ increase by 335%?” the customer wrote, noting the greater-than-three-fold increase.

Most companies would consider property taxes one of the costs of doing business, and they’d simply factor the taxes into their advertised prices instead of deceiving customers by listing one price in an order and then charging a higher one. At the risk of giving AT&T’s billing department more ideas, why stop at property taxes? Why not charge customers separate fees for AT&T’s water and electricity bills, too?

“I pay my own property tax, don’t want to pay theirs!” one customer wrote in an AT&T support forum in July 2017. “Can a doctor add a property tax to their bill for services, or a bank? Why not just raise the rates if it is part of their business?”

Aside from the property-tax fee, Phillips’ cost could go up a lot after his one-year contract is up. His order form said the $95 monthly price is a promotional rate after a $140 discount. The form indicated that his Internet service would normally cost $200 a month instead of $60, not including the $35 charge for static IP addresses.

https://arstechnica.com/?p=1583657

How self-driving shuttles could enable car-free living

in the suburbs

Timothy B. Lee / Ars Technica

reader comments

59 with 33 posters participating, including story author

Share this story

RESTON, VIRGINIA—A Boston-based startup called Optimus Ride has launched a new self-driving vehicle service in the Washington, DC suburb of Reston, Virginia. On Monday, I traveled to the site, a 45-minute drive from my home in the nation's capital, to see it first-hand.

Since August, the company has been ferrying passengers between a Fannie Mae office building at the site and an overflow parking lot a few minutes' walk away. But Optimus Ride has much larger ambitions for the site.

The 36-acre property is directly adjacent to a new stop ("Reston Town Center") on the DC Metro system's Silver Line. The site's owner, Brookfield Properties, is planning a massive mixed-use development here it has dubbed Halley Rise. There will be new homes, office space, and retail stores—including a Wegmans grocery store.

Optimus Ride is betting that self-driving vehicles can transform the way projects like this are designed—making it much easier to build pedestrian-friendly, high-density developments far out in the suburbs.

Why walkable suburban neighborhoods are hard to create

Enlarge / A rendering shows a street scene from the planned Halley Rise development in Reston, Virginia.
Brookfield Properties

There are fundamentally two kinds of neighborhoods: high-density neighborhoods oriented around walking and transit, and low-density neighborhoods oriented around cars.

High-density urban neighborhoods have enough foot traffic that stores and restaurants can thrive without parking lots. The lack of parking lots allows stores and homes to be closer together, which improves walkability.

Transit plays a key role here. High-density neighborhoods have a lot of people within walking distance, including many without cars, which means there's a lot of demand for transit. That allows buses and trains to run frequently, further improving the appeal of a car-free urban lifestyle.

The opposite dynamic is at work in the suburbs. Most people drive, so stores, restaurants, and apartment buildings need large parking lots. All that parking spreads things out, so walking isn't practical for most trips. With widespread car ownership, demand for transit is low, so buses run infrequently.

In large metropolitan areas, there's still significant demand for rapid transit from the suburbs into the urban core. Lines like the DC Metro's new Silver Line cater to this demand. But parking is a major challenge. Few people live within walking distance of a suburban train station, so the station needs to offer parking. But the parking lots fill up quickly, and during rush hour you wind up with traffic jams around the subway station.

Urban planners sometimes try to address this by encouraging high-density development right around suburban subway stops—essentially creating an island of urban living around the subway stop. But it's not easy. A family within walking distance of a subway stop can take the subway for some trips, but if the area around the subway stop is all car-oriented suburbs, the family is still going to need a car to travel anywhere else. That means you need a parking space—and probably two—for every housing unit. That limits how many people can live within walking distance of the station.

This problem is illustrated by the subway stop's namesake, Reston Town Center, which is on the north side of the subway line (Halley Rise is to the south). I had lunch at Reston Town Center prior to my Optimus Ride visit.

Reston Town Center is a high-density mixed-use development much like Brookfield is planning for the Halley Rise site. The site pre-dates the subway line, so developers were forced to build several massive parking garages to accommodate people who drive to the area's shops and restaurants. That drives up the cost of a development like this while making it less

appealing for people living in the area—since no one wants to live next door to a parking garage.

Self-driving shuttles could help

Enlarge / The current Optimus Ride shuttle has four Velodyne lidars. There's one on top, two on the front corners, and one on the back right. It also has a number of cameras.
Timothy B. Lee / Ars Technica

Optimus Ride CEO Ryan Chin argues that self-driving shuttles can play a role here.

"When the metro opens, we expect that there's gonna be some modal shifts," Chin said in a Monday interview at the Halley Rise construction site. "People that normally would have driven here because there was no other way. Now the metro opens, they can take this system."

And that works the other way, too—people who live at Halley

Rise can take an Optimus Rise shuttle to the metro stop, then take the metro to their jobs downtown.

In either case, there's a big payoff for developers: they don't need to build as many parking spots. Building parking spots is expensive—especially if they're in parking garages. And developers can use the extra land to build more housing, office, and retail space. That means extra profits for Brookfield, giving Brookfield an incentive to subsidize the shuttles, making them free to riders.

And that, in turn, sets up a virtuous circle: the more residents the neighborhood has, the more retail stores it can support. The more retail stores there are, the easier it is for residents to do their shopping on foot (or in Optimus Ride shuttles) and the less reliant they are on their cars. So driverless shuttles could make it much easier to create islands of car-free urbanism in a sea of suburban sprawl.

Obviously, shuttles like this aren't a new concept. Airports have had them for decades. But self-driving technology could make them both cheaper and better. With no driver and an efficient all-electric design, these shuttles will be cheap to operate. Having no driver also means it's viable for each shuttle to be much smaller—Optimus Ride's shuttles have room for four to six people—and to have a larger number of shuttles instead. That should reduce the waiting time to near zero, since there can almost always be a shuttle waiting for people.

In the long run, this could work on a much larger scale than Brookfield's current 36-acre site. Optimus Ride shuttles could make it feasible for people a mile or two from the subway stop to commute to work without a car. Optimus Rise could eventually sign deals with other real estate developers in the area to use the shuttle service, expanding the range of people who can get to the Silver Line—as well as the shops and restaurants at Halley Rise—without a car. People who live in Halley Rise could take a free shuttle to Reston Town Center,

and vice versa.

And Optimus Ride is hoping Halley Rise will be a model for other similar developments around the country. Chin says Brookfield operates dozens of large sites like Halley Rise. Optimus Rise hopes that success here will lay the groundwork for deployments like it across America and around the world.

Optimus Ride hopes to begin driverless operation in 2020

Enlarge / An Optimus Ride employee monitors the vehicle’s progress.
Timothy B. Lee / Ars Technica

To be sure, none of this has happened yet. Brookfield is still in the early stages of developing the property. The subway station is expected to begin operations next year, and the development’s anchor Wegmans grocery store isn’t scheduled to

open until 2022.

Most importantly, Optimus Ride hasn’t demonstrated a capability to operate its vehicles autonomously. Right now, the company still has two people in every vehicle—a safety driver behind the wheel and a second employee monitoring the vehicle’s behavior from the passenger seat.

Chin told me that the company hopes to begin commercial driverless operations next year. This, of course, is a promise we’ve heard before. Google’s self-driving company, Waymo, was planning to launch a driverless commercial service last year but failed to do so. GM’s Cruise scrapped its own plans for a 2019 driverless launch earlier this year.

But there are some reasons to think a small company like Optimus Ride might succeed where its larger rivals so far have not. Waymo is trying to build a service that will operate in more than 100 square miles, including at freeway speeds. Cruise is trying to master the complex driving dynamics of downtown San Francisco. In contrast, Optimus Ride is only trying to master the 36-acre Halley Rise site, and initially, the cars won’t go faster than 20 miles per hour (32km/h).

Self-driving at 20mph is a much easier problem than self-driving at 60mph (96km/h). If anything goes wrong, a vehicle doing 20mph can safely slam on the brakes. Optimus Rise can also work with Brookfield to make sure the roads are as friendly as possible for autonomous vehicles, with clearly marked lanes and no weird intersections.

But even this simplified version of the self-driving problem might prove too difficult to solve in the next year. We’ll have to wait and see.

https://arstechnica.com/?p=1582533

Feds hit GirlsDoPorn owners with criminal sex trafficking charges

reader comments

221 with 80 posters participating, including story author

Share this story

Federal prosecutors have charged three men and a woman with sex trafficking charges for operating the popular porn site GirlsDoPorn. At least 22 women featured on the site have sued the site's owners, charging that the pornographers used lies and coercion to gain their participation.

The 22 women said they responded to ads for clothed modeling gigs. When they were asked to shoot porn instead, they initially resisted. But they went along with it after the company assured them that their videos would only be sold on DVD to customers outside the United States and would not be posted online. That turned out to be a lie, as their videos wound up on GirlsDoPorn, a website with plenty of American viewers.

"I was in a state of panic when I first found out," one of the alleged victims testified in court. "I couldn't believe it. I still can't believe it."

"I kept asking if it would be shared with anyone here and they

said ‘No, it would be in Australia only,'” she said.

One of the site’s owners, 36-year-old Michael Pratt, fled the United States last month. Co-owner Matthew Wolfe, 37, was arrested on Tuesday. Ruben Garcia, 31, the male performer in many of the site’s videos, was arrested on Wednesday.

The only woman defendant, 37-year-old Valorie Moser, was an administrative assistant for the porn company for more than three years. She recently testified in civil court about her involvement in the company—perhaps unaware that she was about to be criminally indicted. She described picking up women from the airport, taking nude photos of them, and managing many of the financial and logistical details of the shooting process.

The Daily Beast reports that “girls begged Moser to remove their videos, offering to return their earnings, or pay extra. For the first year at Girls Do Porn, Moser would forward these messages to Pratt. He often told her to block their numbers. She did.”

Prosecutors say that the defendants reaped more than $17 million in revenue from the site—much of it obtained under false pretenses. In their lawsuit, the 22 women are seeking $1 million each. The civil trial is expected to wrap up later this month. The criminal trial likely won’t get started for months.

“Some of the women were pressured into signing documents without reviewing them and then threatened with legal action or outing if they failed to perform,” prosecutors allege. “Some were not permitted to leave the shooting locations until the videos were made. Some were forced to perform certain sex acts they had declined to do, or they would not be paid or allowed to leave.”

Prosecutors say the charges carry a maximum penalty of life in prison.

“I need to take you for a test drive”

Courthouse News reporter Bianca Bruno posted a copy of the criminal indictment in the case. It accuses Garcia, the male performer in many of the videos, of raping two of the women.

After one woman flew to San Diego, Garcia allegedly picked her up and took her to a hotel room. There he “began groping” her and forced her to kiss him. Garcia then allegedly said “I need to take you for a test drive before tomorrow,” pushed her down onto her back, and raped her.

The next day, she was allegedly rushed through signing a contract. She had sex with Garcia, which “was frequently painful because he was aggressive and indifferent.” According to the indictment, she woman remembers being told “stop being a whiny little bitch” when she asked to take breaks due to the pain.

After the video appeared online, the woman’s parents kicked her out of the house, “told her not to come back and disowned her.”

A second woman reported that she was forced to perform oral sex on Garcia even though she had not agreed to do that. She wanted to stop and leave. However, the indictment said, “she did not know how to extricate herself” because there was lighting equipment blocking the exit door. Moreover, she said, she felt that “based on their body language, demeanor, and tone of voice,” Garcia and Wolfe “were in control and they might hurt her if she did not comply.”

After a five-hour photo shoot, Garcia allegedly offered to take this second woman back to her car. Instead, he drove her to a nearby parking lot, locked the doors, and “tried to kiss her and make physical advances toward her.” She “attempted to evade Garcia by climbing into the back seat and telling him

that she was not interested and wanted to leave.”

According to the indictment, he followed her into the backseat and raped her.

https://arstechnica.com/?p=1583425

Adobe backtracks, will refund customers after canceling their accounts

Getty Images | SOPA Images

reader comments

4 with 4 posters participating

Share this story

Adobe has reversed itself on a curious decision that would have denied refunds to customers in Venezuela whose accounts are being canceled through no fault of their own.

Adobe announced Monday that it is deactivating all user accounts in Venezuela in order to comply with an executive order issued by President Donald Trump. Adobe interpreted the executive order much more broadly than other companies, claiming that it was “unable to issue refunds” because the order required cessation of all business activity.

This was strange in part because the executive order doesn’t

actually require cessation of all business activity between US companies and Venezuelan people, as it was targeted at the Venezuelan government and people who provide material support to the regime.

Additionally, Adobe was giving customers in Venezuela until October 28 to download any content they have stored in their Adobe accounts. The company didn't explain why it could continue providing that service for a few more weeks while simultaneously being unable to issue refunds to customers who won't keep getting what they paid for.

Adobe reversed the no-refund part of its decision in an update to the support document yesterday. "If you purchased directly from Adobe, we will refund you by the end of the month for any paid, but unused services. We are working with our partners on the same," Adobe said in the update.

Adobe also reversed itself on one other portion of the mass account deletion. Adobe originally said it would have to stop providing both fee-based and free services to people in Venezuela. But now, Adobe says its free Behance social media platform will continue to be available in Venezuela after the cutoff date for other services.

"In order to remain compliant, Adobe will be deactivating all accounts in Venezuela, with the exception of Behance, on October 29, 2019," Adobe said.

Trump's executive order, titled "Blocking Property of the Government of Venezuela," was a response to Venezuela's ongoing presidential crisis following a disputed election held in May 2018. The US supports Juan Guaidó's claim to the presidency and describes President Nicolás Maduro as a usurper, saying the US is trying to "isolate Maduro's illegitimate regime from the global financial system and the international community."

https://arstechnica.com/?p=1582803