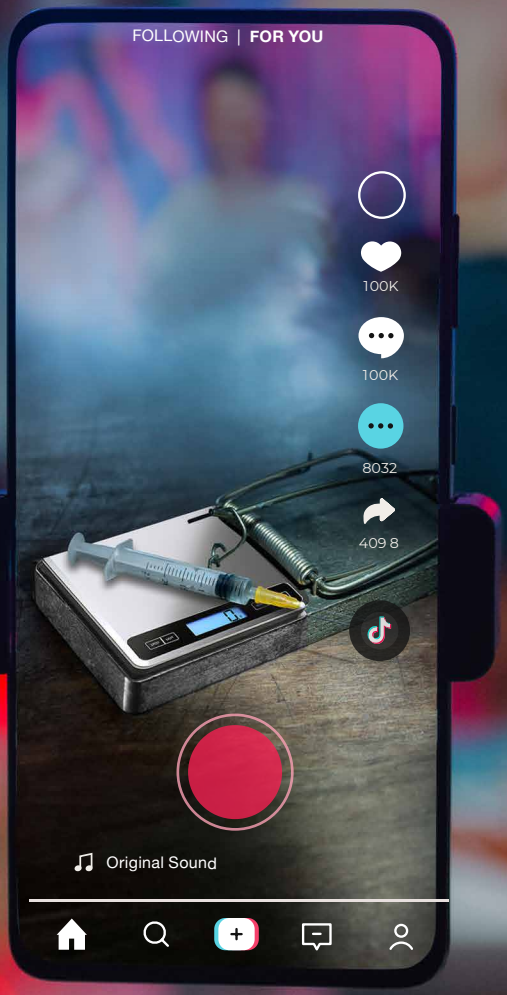
Ozempic Scams on TikTok:

The Only Thing Likely to Get Lighter is Your Wallet



digitalcitizens alliance

COALITION FOR A SAFER WEB

May 2024

Table of Contents

Executive Summary

Enticed by the prospect of effortless weight loss, Americans have turned to TikTok and other social media platforms to purchase scarce supplies of Ozempic and other prescription drugs – and by doing so have become the perfect dupe for online scammers, a joint investigation by the Digital Citizens Alliance and Coalition for a Safer Web has found.

The investigation conducted from February through April found dozens of entities – some claiming to be legitimate pharmacies – offering to ship Ozempic, Mounjaro, and Wegovy used for weight loss. They accept payments on online services such as Zelle – but never ship the drugs. During the probe, investigators engaged in numerous online chats with dozens of online personas claiming to sell the drugs. None required a prescription. Investigators transferred thousands of dollars as payment – without the drugs ever being shipped.

The moment is perfect for these weight loss scams.

Tens of millions of Americans are either using or considering using Ozempic and other drugs as a quick and easy way to shed pounds. Originally marketed to treat diabetes, the drug became popular two years ago among celebrities wishing to lose tens of pounds in mere months. By the fall of 2022, Hollywood was full of rumors of A-list celebrities relying on "skinny pens."

Millions of Americans soon followed suit. An estimated 1 in 6 have taken Ozempic or a similar drug, according to a Digital Citizens research survey. Even more alarming: among those who said they have taken Ozempic or similar drug, nearly half (46 percent) said they acquired the medication at one point even though they didn't have a prescription. Nineteen percent said they purchased it online without a prescription, while 27 percent reported receiving the medication from a friend, family member, or colleague.

Price also likely drives Americans to look for online solutions. Most insurance plans will only cover these drugs for their primary use, controlling diabetes. And with monthly costs ranging from $892 to $1,300, these drugs are pricey for Americans.

Sales of Ozempic neared $14 billion last year, while Wegovy sales were $4.5 billion. This clamor for easy weight loss has created a massive supply shortage. The makers of Wegovy and Zepbound recently warned that the drugs may be difficult to obtain through spring and summer.

Where there is a shortage, there will be bad actors and scammers to take advantage of Americans. Weight loss expert Dr. Sharon Giese estimates that online weight loss scams could end up costing Americans billions of dollars.

Social media platforms have been slow to respond to scams or the sale of counterfeit drugs. BrandShield, an Israel-based cybersecurity company, reported that it took down over 250 websites peddling counterfeit versions of weight-loss drugs last year.

TikTok recently announced a crackdown on content from so-called media influencers promoting weight loss drugs, but investigators found most of the would-be Ozempic sellers still online in late April. They had TikTok handles such as "Fatloss Pharmacy," "Trim Optifit Health," Samantha Weight Loss," and "Mounjaro Weight." Their TikTok profiles show images of stacks of boxes of weight loss pills "available" for sale.

Given that TikTok may be banned from being able to continue to operate in the United States, it's shocking that it would be so lax about scammers leveraging its platform.

It's a safe bet that ByteDance, TikTok's Chinese owner, doesn't tolerate similar scams that target users in China using its version of the social media platform called Douyin. The differences in the experiences have been compared to "opium and spinach" due to the tight restrictions that ByteDance places on content that Chinese users see.

Perhaps just as troubling is that investigators found that after they started searching for weight loss drug sellers on TikTok, TikTok eventually started suggesting connections to sellers. The investigators saw that once they, the potential buyers, demonstrated their interest by searching for the drugs, TikTok's algorithms drove the sellers their way. The algorithms make it all too easy for those pushing these drugs to find victims susceptible to the scams that investigators found.

Alas, these scams are not new. The sales pitches and post-sale follow-ups demonstrate all the hallmarks of scams that Digital Citizens and Coalition for a Safer Web have documented over the last several years: Add links to previous reports

- ***Ease of purchase.*** The sellers promise a quick and easy process that will enable a would-be buyer to get drugs such as Ozempic and Mounjaro without the prescription that would be necessary if the person went to a conventional pharmacy. The cost of the drugs ranged from $200 to $400 for a month's supply.
- ***Alternative Payments.*** The would-be sellers refuse to take traditional credit cards, instead insisting on payment services such as Zelle, Venmo, and PayPal – directing that the funds be listed as "friends and family" so they aren't eligible for refunds.
- ***A "holdup in customs."*** In a common tactic, the would-be sellers claim that an issue has arisen in getting the drugs into the country that can be solved by an additional "one-time refundable" payment to cover insurance. This is a technique to squeeze an online buyer who is already on the hook for hundreds of dollars.
- ***Payment Screenshots.*** Operators demand that buyers send proof of payment in the form of screenshots of payments through sites such as Zelle, Venmo, and PayPal. The purpose appears to be an effort to obtain sensitive banking information that may appear on the screenshots that are submitted as proof of payment.
- ***Whack a Mole.*** Another all-too-common tactic of these scammers is to utilize a social media persona or website until it attracts too much scrutiny – then discard it and resurface with a new social media account or website. In one instance, investigators discovered an operator was using at least two distinct Tik Tok accounts to lure potential victims. Investigators only discovered it was the same person when the operator used the same phone number across the two accounts to arrange payments for a shipment.

While these scams have multiple layers, the outcome is always the same: when online buyers fall for it the only thing likely to get lighter is their bank account.

In the coming weeks, perhaps TikTok will commit to ridding its platform of illicit Ozempic sales. But if it does, it's like a cop busting a popular street corner where drugs are sold. Too often, the drug peddlers just find a new venue. Unless Instagram, X (formerly Twitter), Snap, and Telegram follow suit, they will replace Tik Tok as the go-to place to peddle weight loss drugs. Already, so-called Ozempic influencers – those hailing the benefit but not selling the drugs – have signaled plans to focus on Instagram if Tik Tok bans them. And where influencers go, scammers follow.

Demand for a quick-and-easy way to lose weight only makes it easier for scammers:

- According to the Digital Citizens survey of 1,160 Americans conducted in early May, 31 percent of Americans responded they are interested in using Ozempic to lose weight.

- And those who say they are interested in using Ozempic or other similar drugs to lose weight are much more likely to look online to buy them than other Americans. According to the research survey, Americans who are interested in Ozempic are twice as likely as other Americans to consider purchasing prescription drugs online without a prescription. They are also twice as likely to view Tik Tok as a credible place to interact with medical professionals and potentially purchase prescription drugs.

That mindset makes the job of an online scammer much easier.

- While younger people are typically more associated with risky online behavior, the research survey found even older Americans are willing to skirt the rules to get the drugs. According to the survey, 22 percent of Americans age 55 and older reported that they received Ozempic or similar drugs from either a friend, family member, or colleague or by making a purchase online even though they didn't have a prescription.

Ultimately, this investigation into online Ozempic sales underscores a point DCA and CSW have made time and again: if investigators can easily find prescription drugs being illegally marketed and sold online, why can't the social media platforms that claim to be responsible actors do the same? A quick search found dozens of online peddlers of weight-loss drugs. A simple message confirmed that these "dealers" didn't require a prescription to make a deal. In these cases, they likely never intended to follow through with a shipment. But in multiple other cases, Digital Citizens has bought drugs online without a prescription – from opioids to human growth hormone – that in fact were not what they claimed to be. Perhaps the only thing worse than being scammed out of a drug delivery is getting a drug that isn't what the seller claimed it to be.

But in either instance, it's happening under the noses of large, publicly traded companies that operate the most influential social media platforms in the world. Scamming Internet users shouldn't be this easy. But in this case, TikTok has made it so.

Not Hiding. In Plain Sight

While some bad actors, such as criminals peddling stolen credit cards, rely on code words to market their services on online platforms, those offering Ozempic and other weight-loss drugs do so openly and blatantly. Take Fatloss Pharmacy (in direct messages, @fatlosspharmacy999). Its TikTok profile page features a video and images posted in April promising "fast shipping" and offering "sales of Ozempic and other weight loss medications at affordable prices."

IMAGE 1

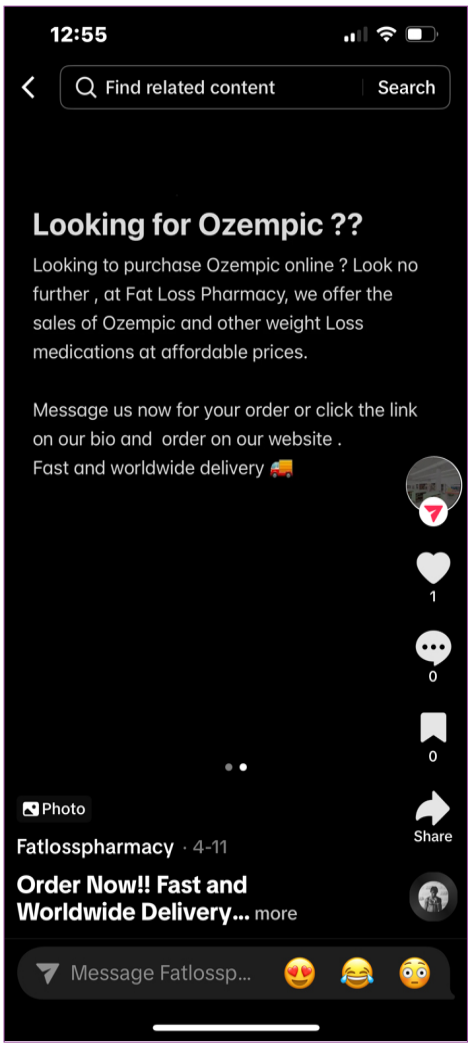


IMAGE 2

The researcher found "customer testimonials" and offers of affordable prices on the TikTok profile (see images 1 and 2). The researcher also followed the link mentioned to fatloss-pharmacy.com, which offers multiple options to purchase weight-loss drugs – no prescription required (see image 4 on the next page).

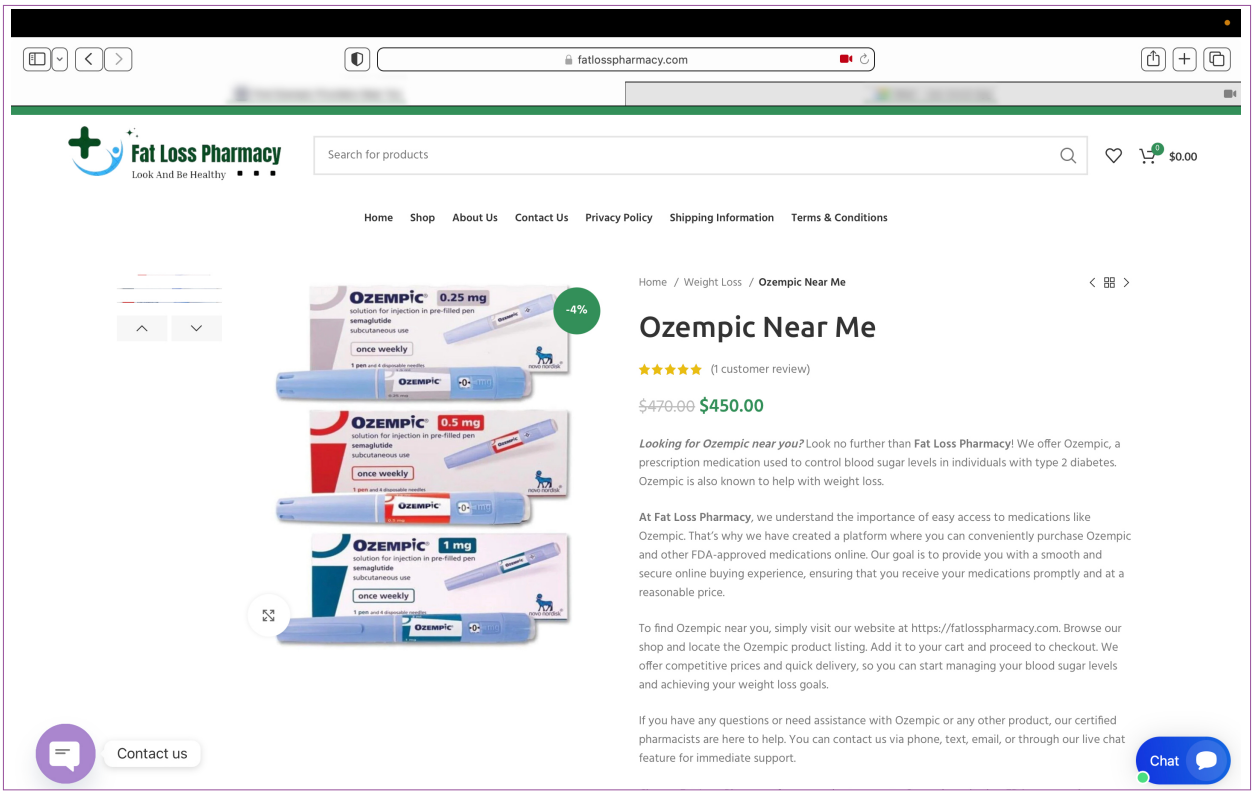


IMAGE 3

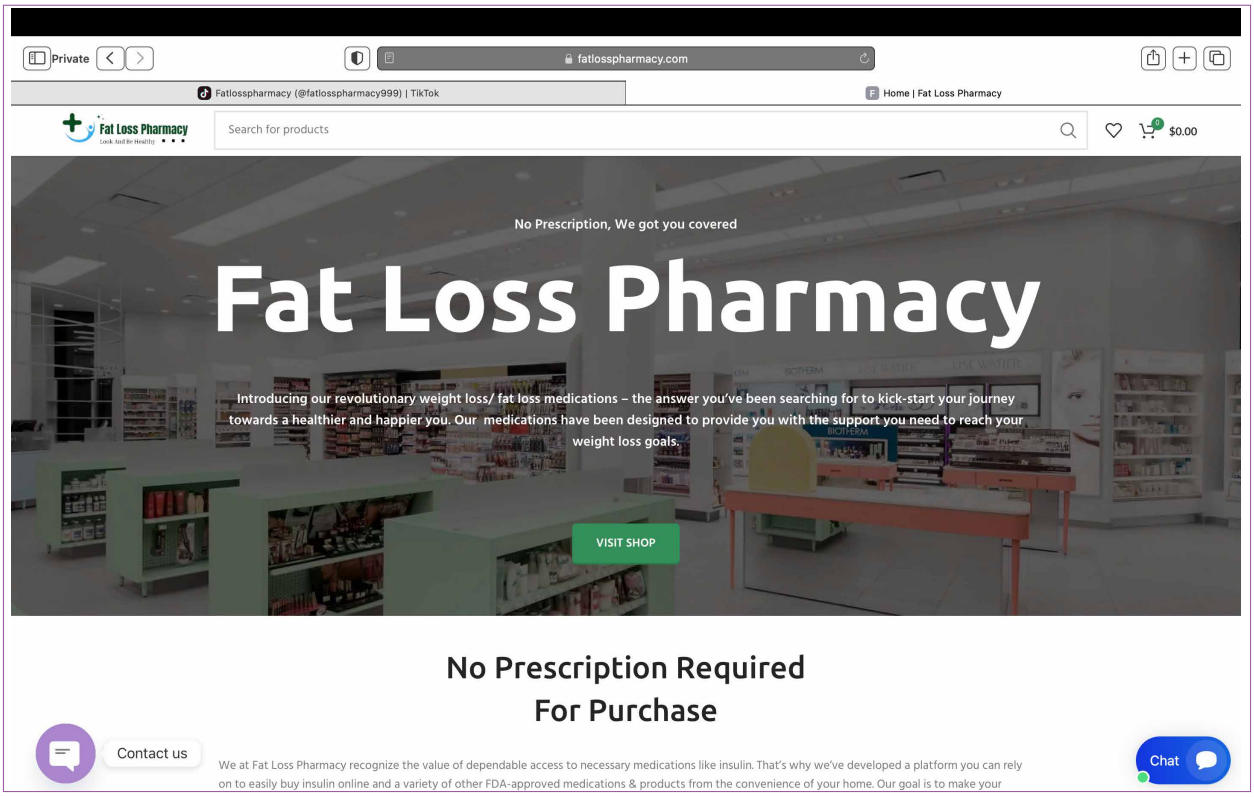


IMAGE 4

Coalition for Safer Web Investigators had multiple conversations with the person who responds to messages on Fatloss Pharmacy's TikTok page to arrange an Ozempic purchase.

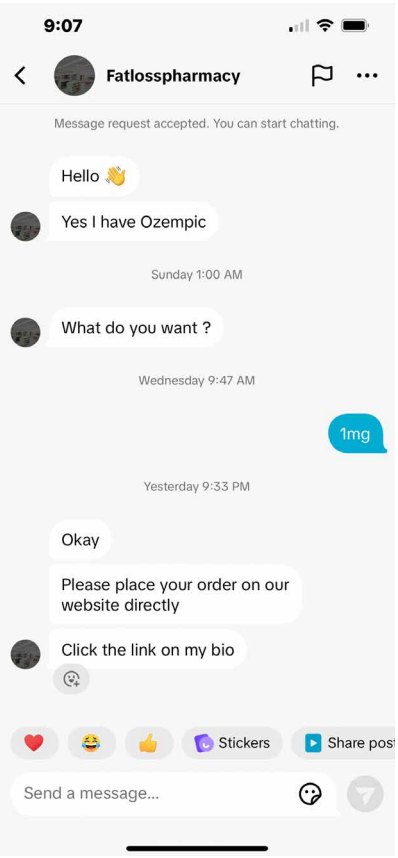


IMAGE 5

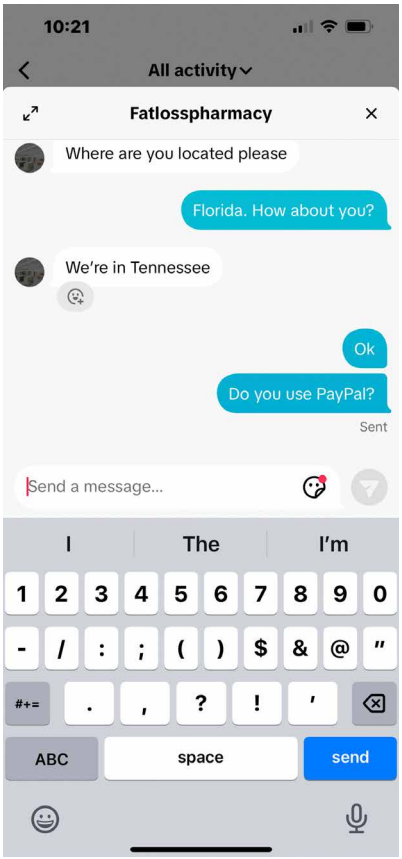


IMAGE 6

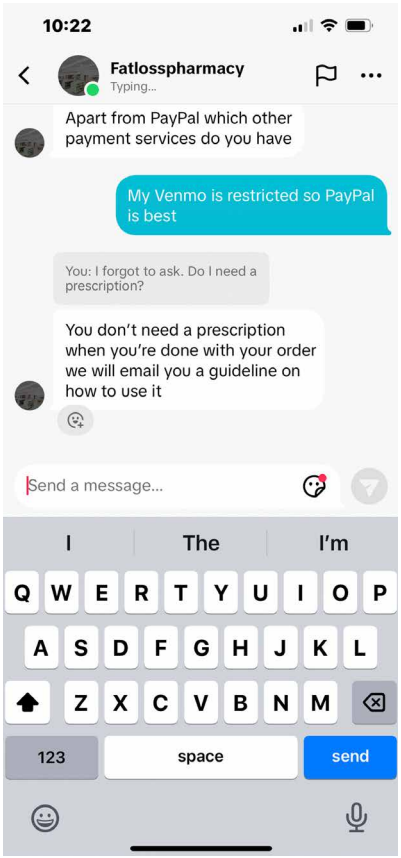


IMAGE 7

Fatloss Pharmacy's willingness to provide Ozempic and other drugs without a prescription is irresponsible. The list of potential serious side effects of Ozempic are gallbladder disease, kidney damage, and an increased risk of thyroid cancer. That is why it's meant to be taken under a doctor's supervision. Of course, if they are just scamming online users that's a different issue.

Fatloss Pharmacy is just one of dozens of accounts peddling Ozempic on TikTok. Another uses the handle jacks_opioids2, or Jack's pharmacy in direct messages.[1] The jacks_opioids2 handle reflects that its "offerings" go beyond weight loss drugs to powerful painkillers. Its TikTok profile offers prescription drugs such as Sculptra, a collagen booster that is only supposed to be injected by a trained medical professional, and Daxxify, an alternative to Botox to smooth lines in the face.

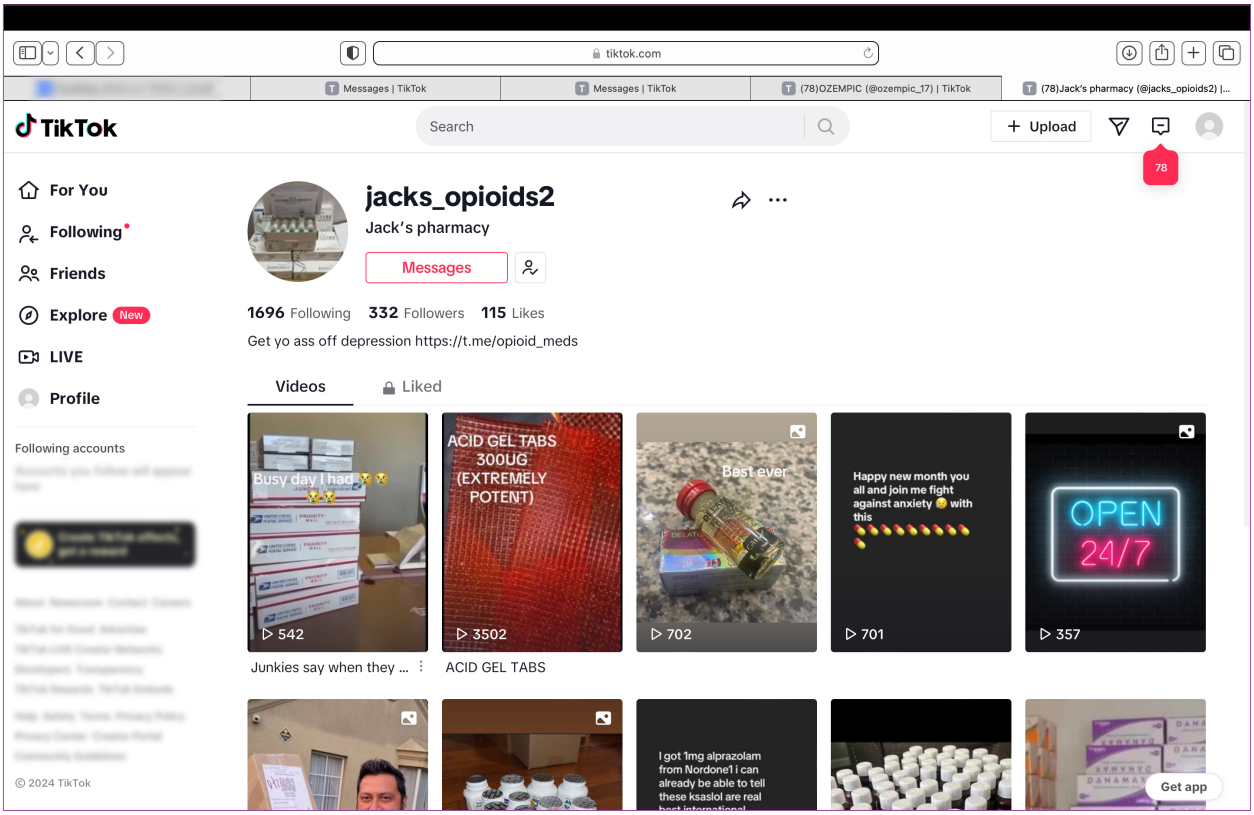


IMAGE 8

[1] There are many physical stores with the name Jack's Pharmacy across the United States. Investigators are skeptical that the TikTok account has any connection or relationship to any physical store using the name Jack's Pharmacy.

The operator of jacks_opioids2 promised to deliver Ozempic and opioids to a New Jersey address.

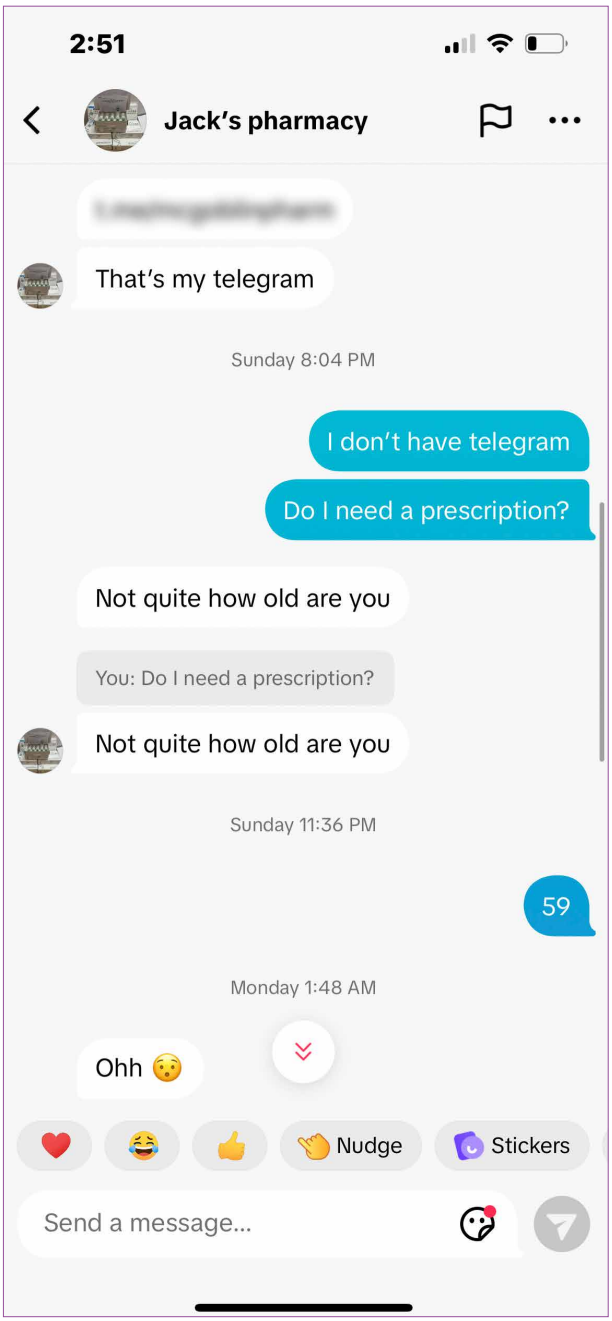


IMAGE 9

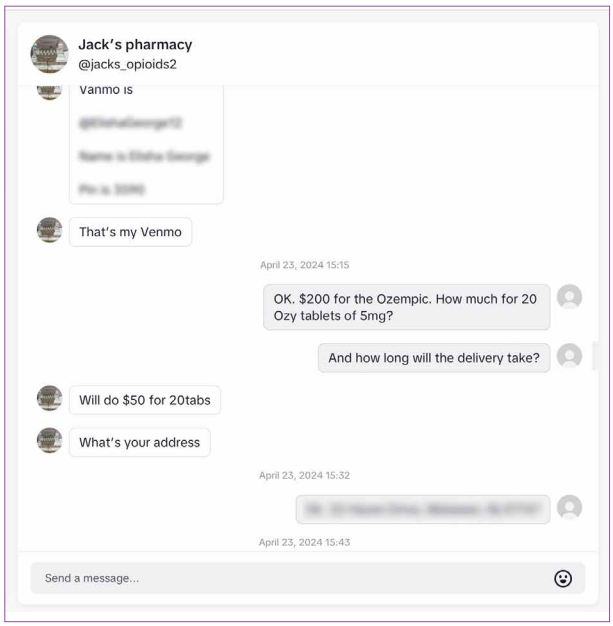


IMAGE 10

Another Ozempic dealer on TikTok is Samantha's Mounjaro (handle: @samantha_weightloss1). Its profile says it's "Taking orders. NO SCAM!!" – a tagline not bound to inspire confidence.

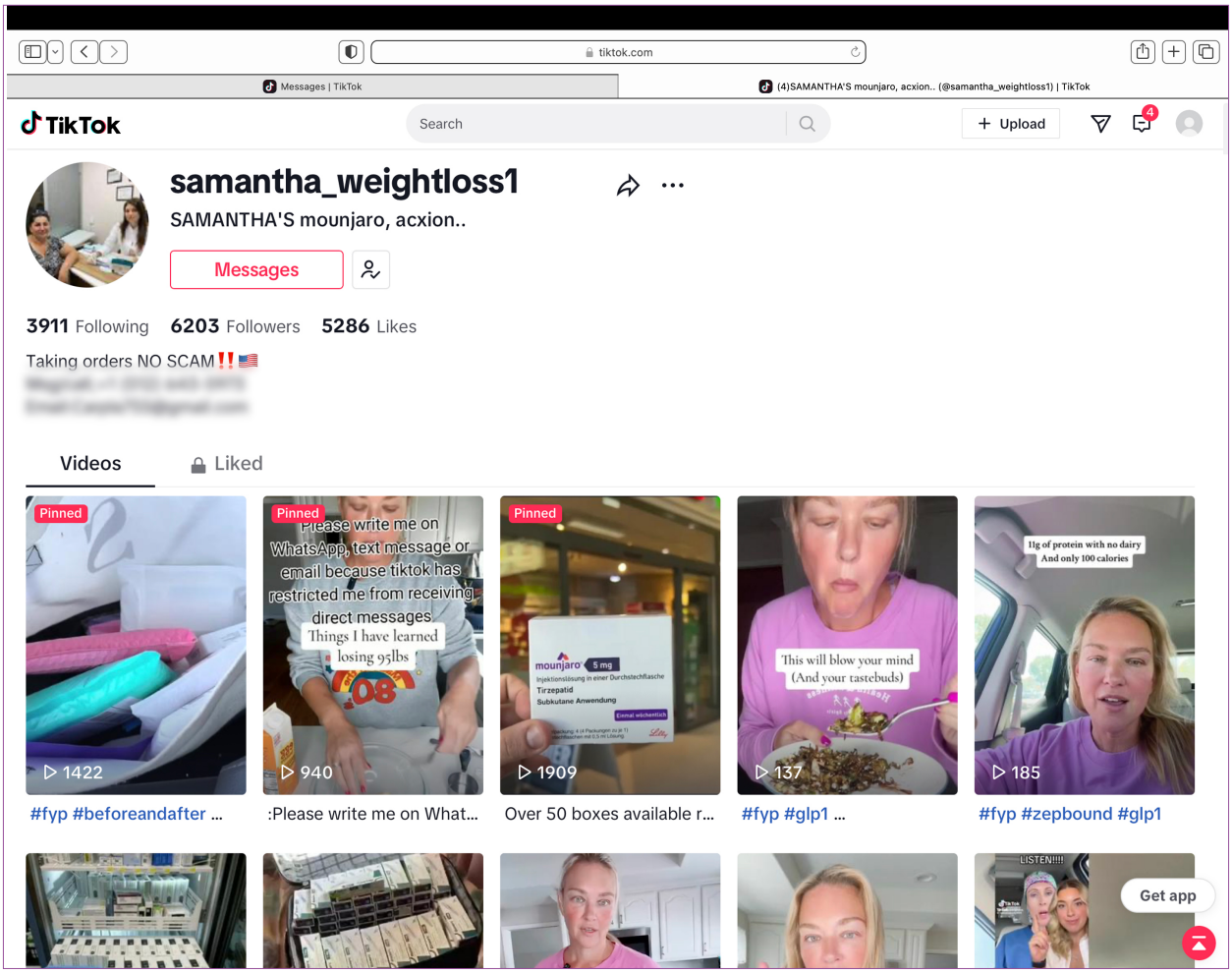


IMAGE 11

In TikTok messages, the operator of Samantha's Mounjaro promised Ozempic delivery in "24 to 72 hours maximum" once the investigator verified that he provided a screenshot of proof of payment. We'll focus on the request for a screenshot of a payment later during the "Anatomy of a Scam" section.

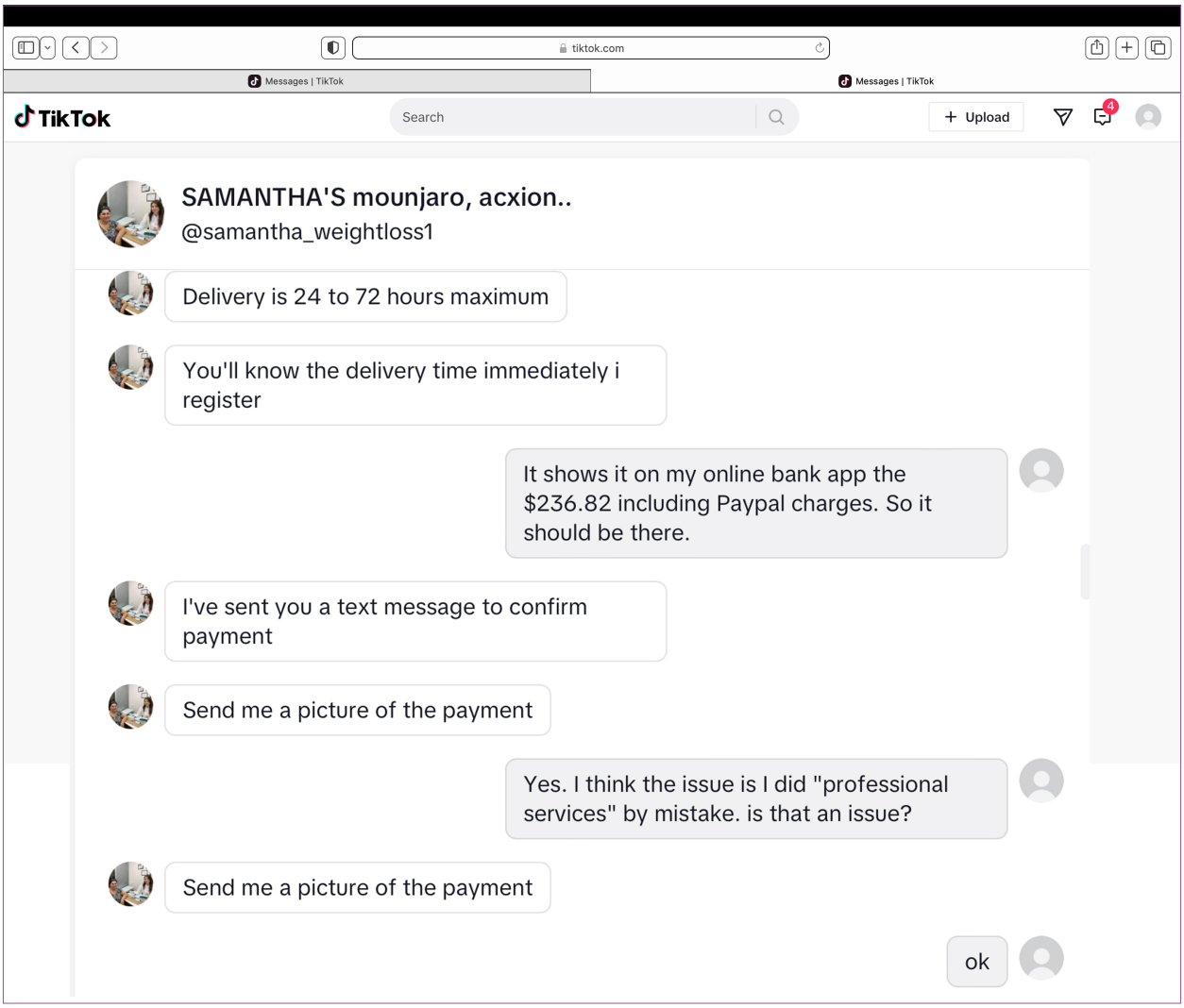


IMAGE 12

There are numerous other examples of operators using TikTok to offer Ozempic, other weight-loss drugs, and if jacks_opioids2 is to be believed, even opioids. In each instance, these are prescription drugs that if misused can have significant, even fatal, consequences.

Most, if not all, of the operators that investigators engaged with showed the telltale signs of being a scam. But that is not always the case. CBS News reported last fall on Americans hospitalized after using fake Ozempic pens that were purchased online. And whenever demand outstrips supply, there is the prospect of counterfeit weight-loss drugs. Dr. Jonathan Kaplan calls fake Ozempic "very scary." Speaking to Healthline, he said, "Sure it's convenient to order online without a prescription, but you truly don't know what's in it."

Whether scams, fakes, or actual Ozempic, the bottom line is clear: bad actors are peddling illicit weight-loss drugs right under TikTok's nose. *If investigators can find dozens of examples of Ozempic being marketed, why can't the employees responsible for policing the platform?*

That is a question only TikTok can answer. Digital Citizens reached out to the social media platform but has not heard back. If TikTok responds, we will update the report.

Anatomy of a Scam

Digital Citizens investigators shelled out just over $3,000 to purchase Ozempic. That money yielded no deliveries of the drugs. It wasn't a surprise given the telltale signs of a scam.

Once an investigator reached out, the "Fatloss" contact immediately confirmed they had the drugs requested. They tend to limit communications to TikTok or other messaging platforms such as Telegram. Once a "deal" is reached, they arrange payment – but it's never through conventional means such as a credit card. Instead, they insist on payment through cryptocurrency, Zelle, PayPal, Venmo, or other peer-to-peer payment platforms. And it must be "friends and family."

That is because if it's designated as a business transaction, there can be tax implications but more importantly it may allow the buyer to demand a refund.

Here's an example below: While finalizing the transaction, Fatloss Pharmacy insists on how to categorize the payment.

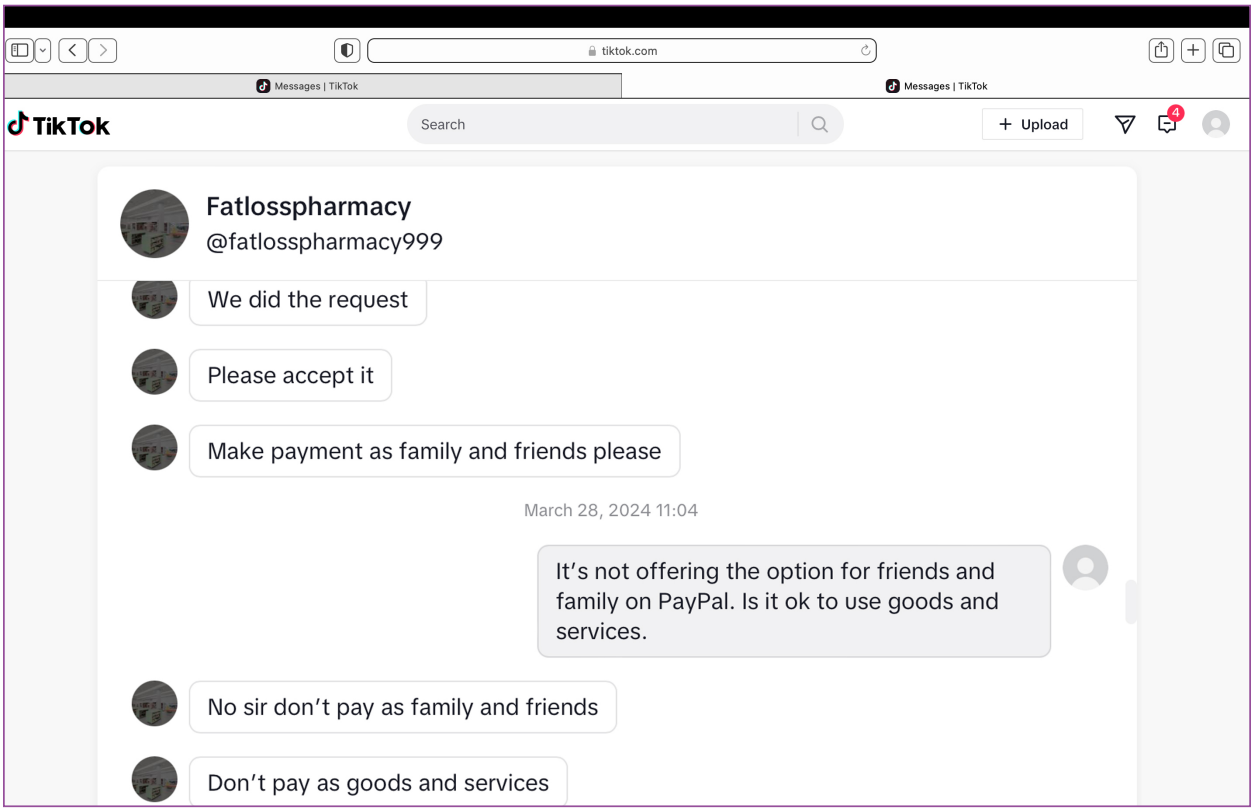


IMAGE 13

In some cases, it became clear that operators were using multiple accounts to scam would-be buyers. Operators for a TikTok account using the handle @TRIM OPTIFIT HEALTH as well as Babylovek each asked operators to send money via Zelle to a person named Jessy using the same phone number.

When asked whether the person was operating multiple sites, the operator of @TRIM OPTIFIT HEALTH got defensive and denied having multiple accounts:

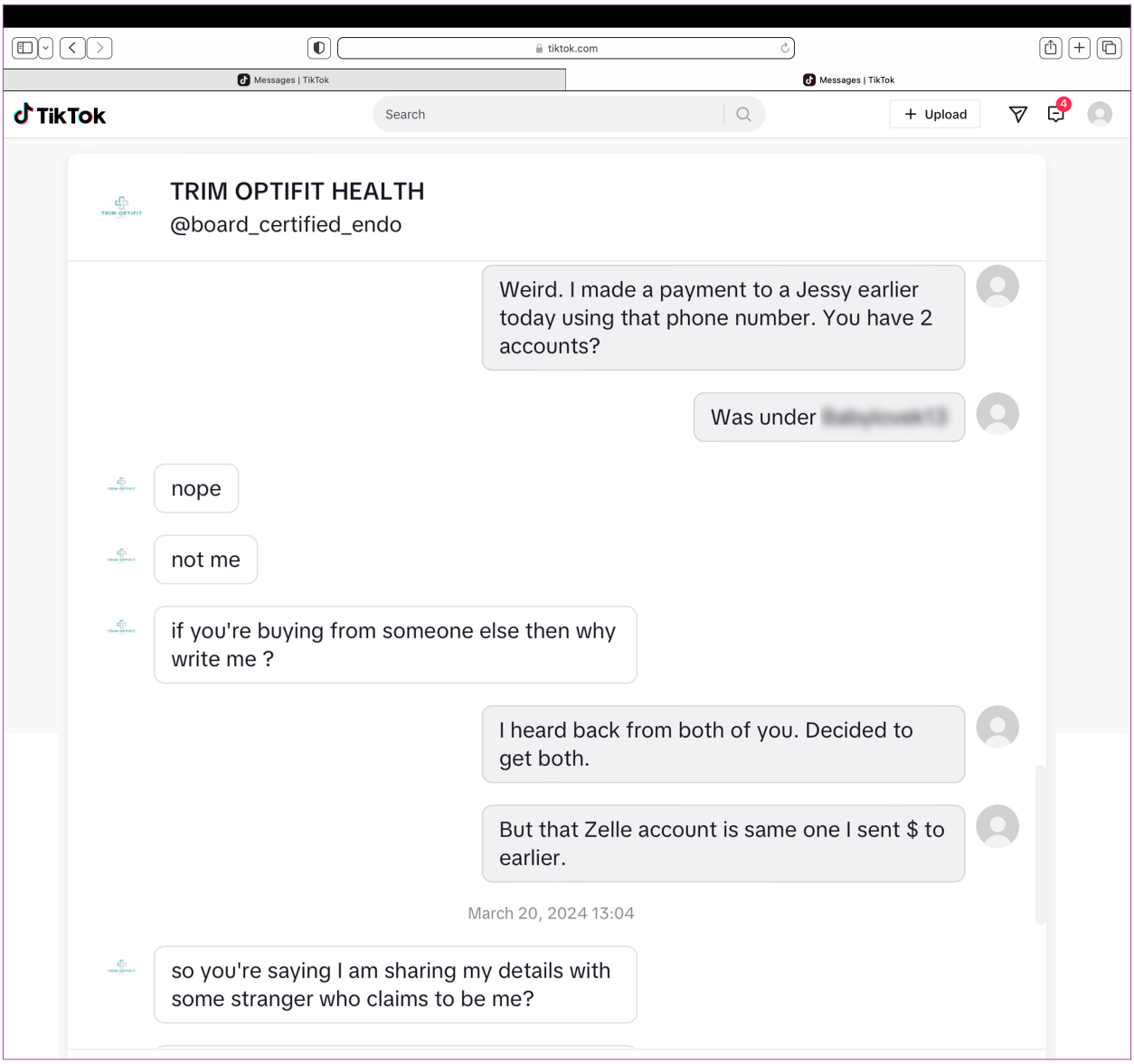


IMAGE 14

[2] Investigators did find other examples of organizations using variations of the name Trim Optifit. There is no evidence that any physical businesses using the name Trim Optifit are involved in this activity.

Nearly immediately afterwards, @TRIM OPTIFIT HEALTH stopped communicating with investigators. Several days later, the researcher could no longer access @TRIM OPTIFIT HEALTH's TikTok channel.

The next phase of the scam is sketchy or bogus delivery services. Over the years, Digital Citizens has observed in multiple instances a sophisticated tactic used by scammers: the establishment of websites that purport to be a Fed Ex-like delivery service.

In a 2021 investigation, Digital Citizens came across a bogus delivery service called Peco Transport. On the surface, it looked legitimate. The seller, in this case claiming to offer human growth hormone and other performance and appearance-enhancing drugs, sent a tracking number that confirmed a delivery date. But the delivery service didn't operate. The picture of the "CEO" of the company was a stock photo of a French actor and model. The name of the CEO on Peco Transport's website? "John Doe." Shortly afterwards, the website no longer existed.

Similarly, in the Ozempic investigation and dubious delivery services, after connecting via TikTok, investigators paid Emilia Weight Loss $310 for an order of Ozempic. The operator of Emilia Weight Loss promised the order was on its way via Global Transit Logistics shipping.

But there's a catch: a "refundable insurance fee" of $110 is needed to complete the transaction with Global Transit Logistics. This is a common tactic by scammers to squeeze more money out of their targets by claiming a customs issue is holding up the shipment.

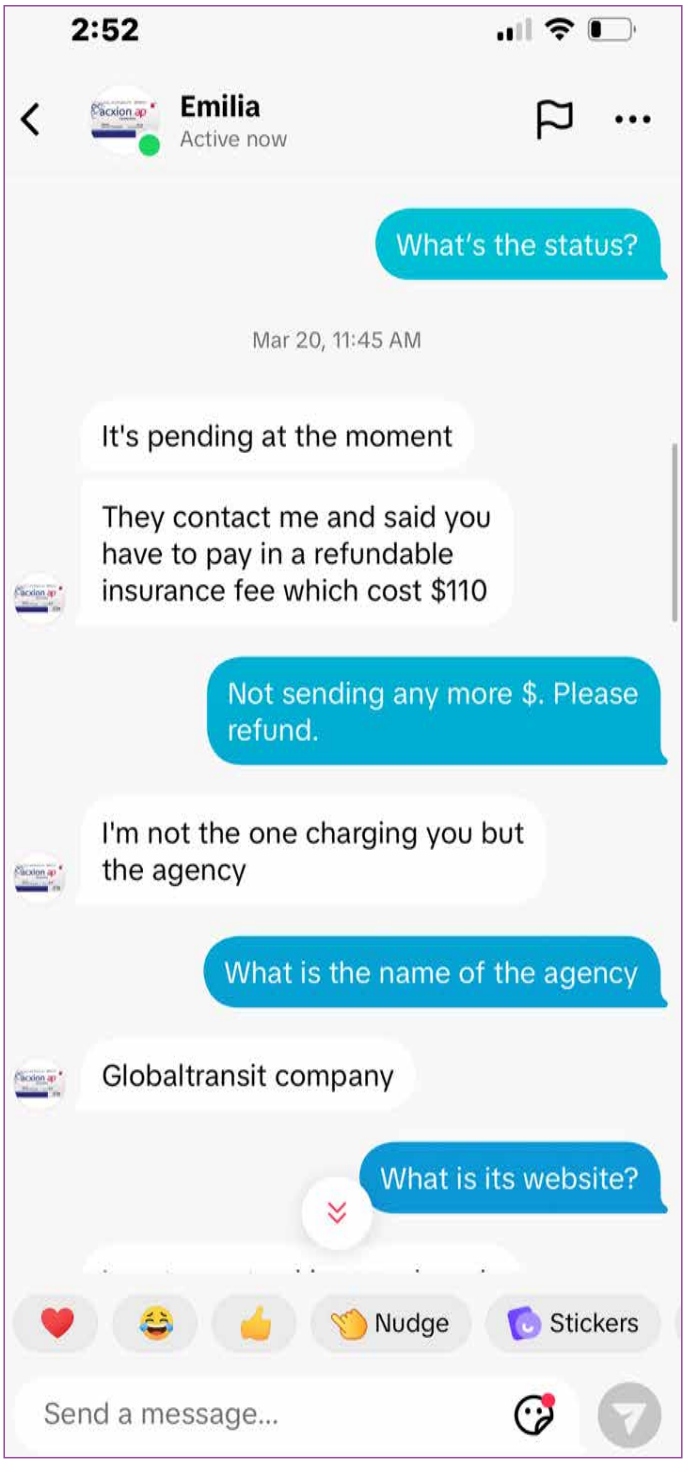


IMAGE 15

The last element of the ruse may be the most alarming. Bad actors leverage payments to obtain sensitive banking information. Nearly every would-be seller insisted that investigators send a screenshot of the Venmo, Zelle, or other payment system used to make the purchase.

Here are examples of demands for screenshots of payment confirmation:

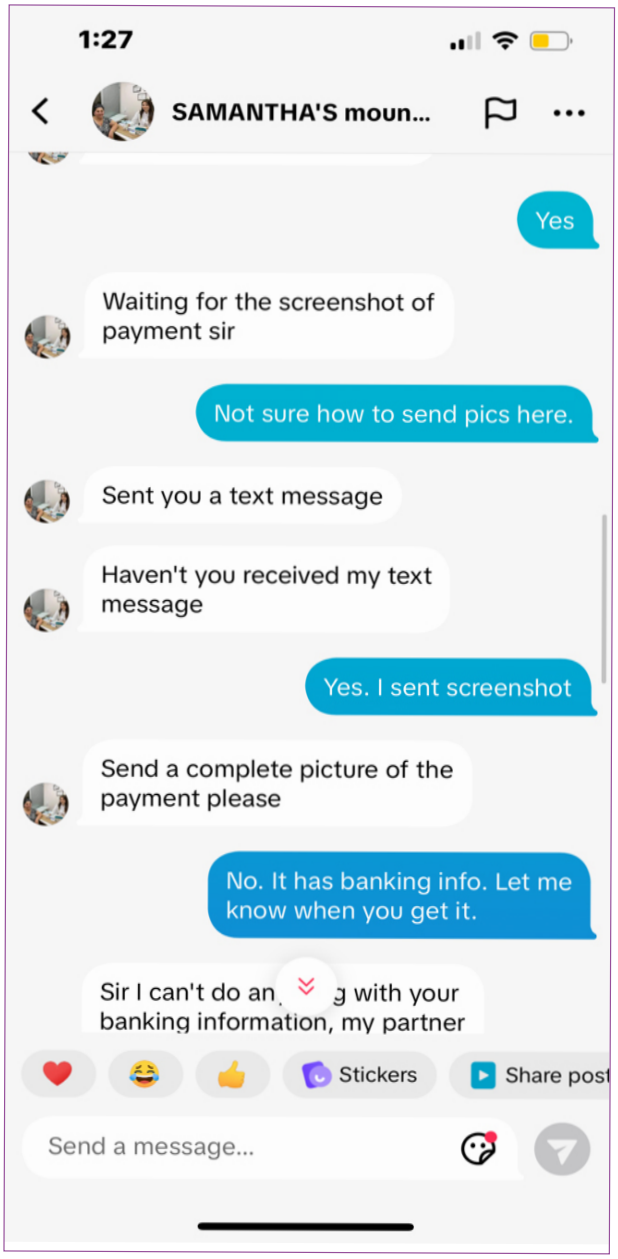


IMAGE 16

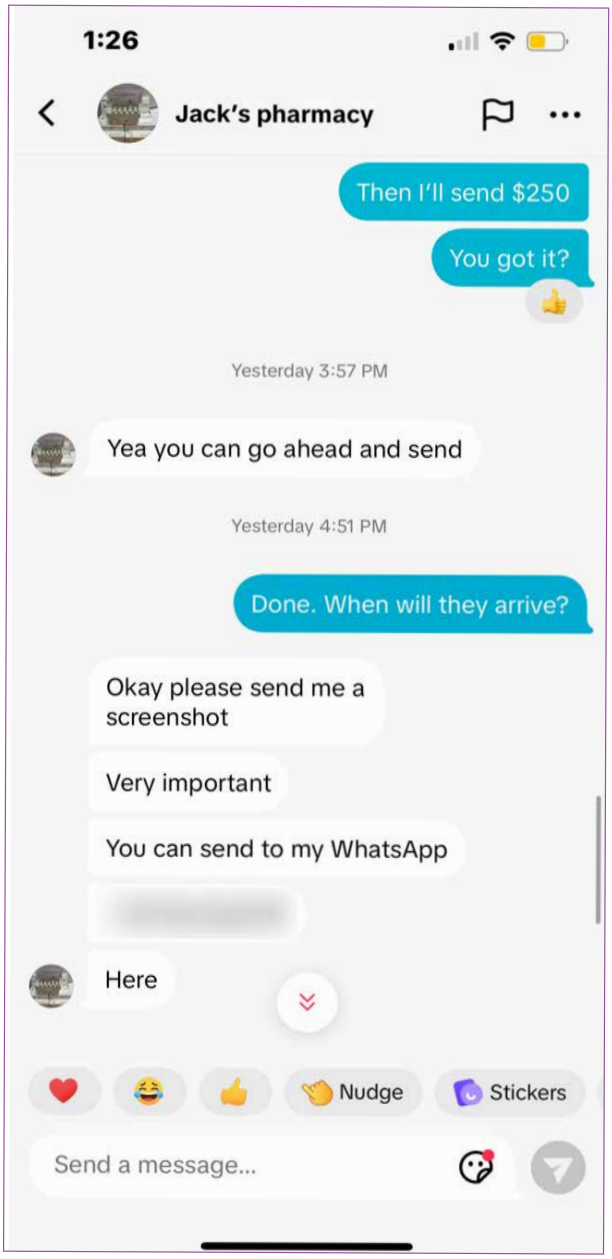


IMAGE 17

A day after making a payment to these scammers, one of the investigator's credit cards was compromised. Nearly $2,600 was charged to Hertz Rental Car. In addition, the investigator received a Zelle fraud alert within hours of a purchase.

Algorithmic Amplification – Who Is Looking for Who?

> It's easy to see why someone looking for these drugs can quickly become engulfed in a sea of drug offers. It doesn't take long for the buyer to go from the hunter to the hunted.

This research began with a CSW researcher searching for channels offering prescription drugs laced with fentanyl, opioid, and other addictive narcotics. On February 15th, the researcher came across @ TRIM OPTIFIT HEALTH because that channel was offering what's known as "Mexican Xanax." Looking at the sale items listed on the TikTok page as well as a website linked to the page, the researcher noticed @TRIM OPTIFIT HEALTH also offered weight loss drugs.

This made the investigators curious. On February 22nd, a CSW researcher began searching for TikTok accounts with brand names like Ozempic, Mounjaro, and Wegovy in channel profile handles. Additionally, there were searches for terms like "weight loss." Within the 24 hours, the CSW researcher connected with more than a dozen pages having those terms in their profiles. Several of those account holders accepted the researcher's invite and eventually engaged in conversation.

By February 24, the researcher stopped searching for sellers and just watched the sellers come to them. It started with accounts holders not included in the original search. After that, TikTok began suggesting accounts with similar names. The researcher is still getting approached by other sellers two months after the initial search.

While you may not be able to watch an algorithm work like a turbine or an assembly belt, it's not hard to create a situation in which a drug buyer is driven to dozens of drug sellers. Now just imagine what could happen with harder, even more dangerous drugs. There's no emergency off switch on these algorithms. It appears they don't just allow for harmful activities to happen, but the algorithms have the potential to accelerate the dangerous activity.

We've Seen This Before

Discovering that a social media company is allowing bad actors to operate on its platform is hardly breaking news. For over a decade, Digital Citizens and the Coalition for A Safer Web have raised alarms about criminals and other bad actors relying on these platforms to sell opioids, steroids, and fake COVID cards and vaccines. Also, researchers have found accounts peddling stolen credit cards, serving as recruiting and gathering points for international and domestic terrorism, as well as offering fake passports and other IDs.

Digital Citizens chronicled these concerns in a 2013 report that laid out how Google's subsidiary YouTube was used by bad actors. Initially, these alarms were raised about Google, which largely dismissed concerns about systemic issues on its platforms. However, shortly after Digital Citizens and Coalition for A Safer Web exposed that Islamic Jihadists were using an unmonitored Google Plus to recruit members and share videos of beheadings and other violence, the company finally completely shut down the site.

TikTok seems to have taken a page out of Google's old playbook in not taking seriously the dangers posed when it enables criminals and other bad actors to use it without consequence. That it does so as it fights for its right to remain active in the United States is stunning.

Fueled by fears that TikTok enables Chinese authorities to snoop on Americans and undermine U.S. culture, Congress appears poised to force TikTok to divest from its Chinese ownership or face a ban in the United States.

For a decade, Digital Citizens and the Coalition for A Safer Web have sounded the warning that if social media platforms don't police themselves and act more responsibly, Congress and federal regulators may step in to do it for them. That warning has proven true in the form of fines and anti-trust lawsuits.

Now it will be up to TikTok to determine what its next ten years will look like.

It can be said that it's better for Americans to be duped out of their money than to receive drugs – whether Ozempic, opioids, or steroids – that can threaten their health or even their life. But it's a sad commentary when the "lesser of two evils" is the choice offered to American consumers.

This investigation drives home that whenever Americans clamor for something – whether N95 masks during COVID or weight-loss drugs now – scammers will seize the moment.

This is just another lesson in the need for digital literacy and digital civics. When Internet users are educated about risks, they make better decisions. For that reason, Digital Citizens and Coalition for a Safer Web will develop new initiatives to raise awareness about online risks. State attorneys general have been effective messengers warning Americans about the risks of opioids, how to properly dispose of dangerous drugs, and the malware and credit card theft risks that follow when we let illicit content such as pirated content into our homes.

While online safety groups can play an effective role, it's time for Congress and state legislatures to take a more comprehensive look at how we educate school-aged children to be cybersecurity and scam savvy. These bad actors feed on ignorance; that gap must be closed.

In its failure to adequately police itself, TikTok shares that dubious distinction with American counterparts such as Google, Facebook, and X, which have all faced accusations of putting profits over user safety and, in Facebook's case, being used to manipulate elections.

Yet, TikTok appears to be missing the lesson here: When you find yourself in a hole (in this case with Congress and the White House), the best thing to do is drop the shovel. The best way to do that is to recommit to making TikTok a safer place to visit – no matter who owns it.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org.

About The Coalition for a Safer Web

The Coalition for a Safer Web is a non-partisan, 501(c)(3) demanding accountability from social media platforms, government, and corporations, and bringing together a unified voice to foster a safer digital sphere. By countering the spread of dangerous rhetoric, The Coalition For A Safer Web strives to create real-world change and address the impact of online extremism on society. To learn more about the Coalition visit the website at www.coaltionsw.org.

digitalcitizens alliance

COALITION FOR A SAFER WEB