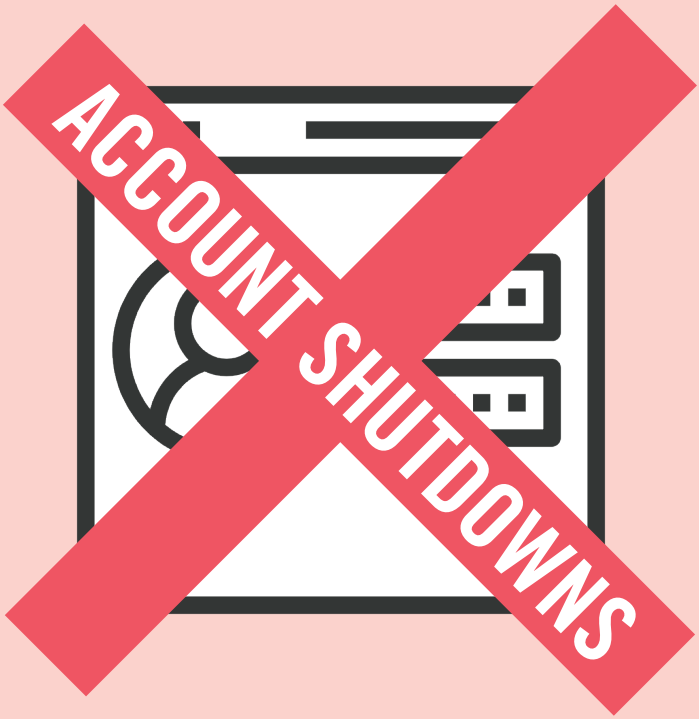


WHY THEY HAPPEN, MITIGATION STRATEGIES, AND WHAT YOU CAN DO IF IT HAPPENS TO YOU

NOVEMBER 2019

THESE ARE ONLY SUGGESTIONS, NOT GUARANTEES

If you're unable to get your account back after trying all of the options listed in this guide, **it's not your fault**. The platfrorms and payment processors' decision making processes are incredibly opaque, and tactics that worked with one platform might not work for another, and probably none of them will work every time forever. A lot of this guide focuses on fintech, but many of the strategies apply to social media as well.

WHY THIS HAPPENS

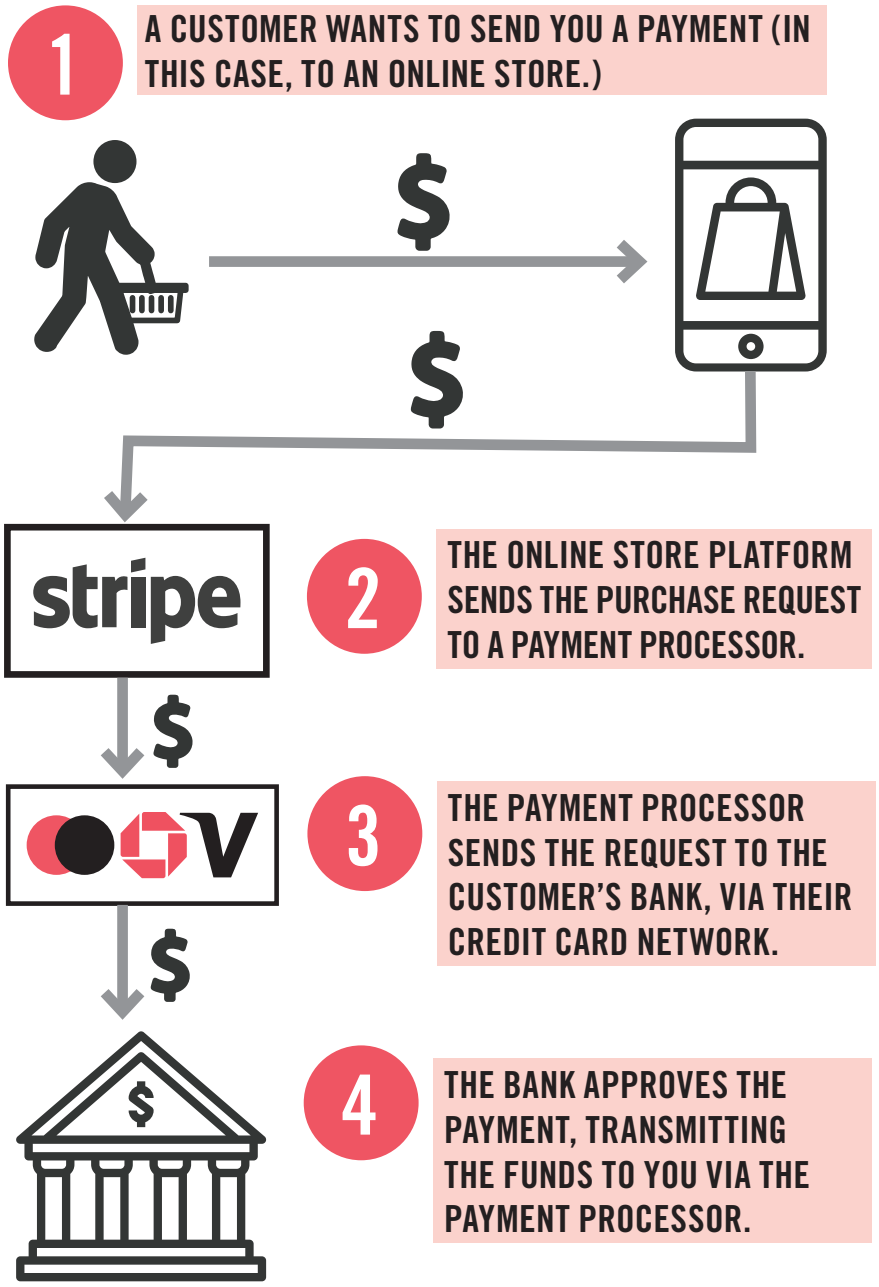
Payment processors are services that let you accept payments online. For example, if you set up a Shopify account to sell physical photo sets, you can choose to use Stripe, QuickBooks Payments, BitPay, or a number of other services to accept payments on your site.

The payments industry is very heavily regulated and subject to **Know Your Customer (KYC)** laws. As part of the KYC regulation and in order to manage risk, payment processors are required to monitor all transactions and investigate them to the best of their abilities if they think they're associated with activities that could be high risk to the processor. Unfortunately, sex work is often classified as being high risk to the processor, despite there being no empirical evidence that this is true.

Additionally, payment processors are subject to constraints put on them by other companies they work with to facilitate transactions (e.g. banks, credit card companies, and so on). These companies have a lot of power and influence when it comes to whether or not they are willing to cooperate with payment processors in accepting certain types of transactions.

For example, a bank can decide that they don't want to accept transactions related to sex toys, and then the payment processor can't process transactions related to that. The bank's justification will be something like "this increases the risk too much," (though again, these policies are often more founded in their conservative biases and overt hostilities towards people not like them than reality).

HOW TRANSACTIONS SHOULD WORK



Payment processors deal with a huge number of transactions per second and mainly rely on automated techniques (e.g. keyword triggers and machine learning algorithms) to flag transactions for manual review.

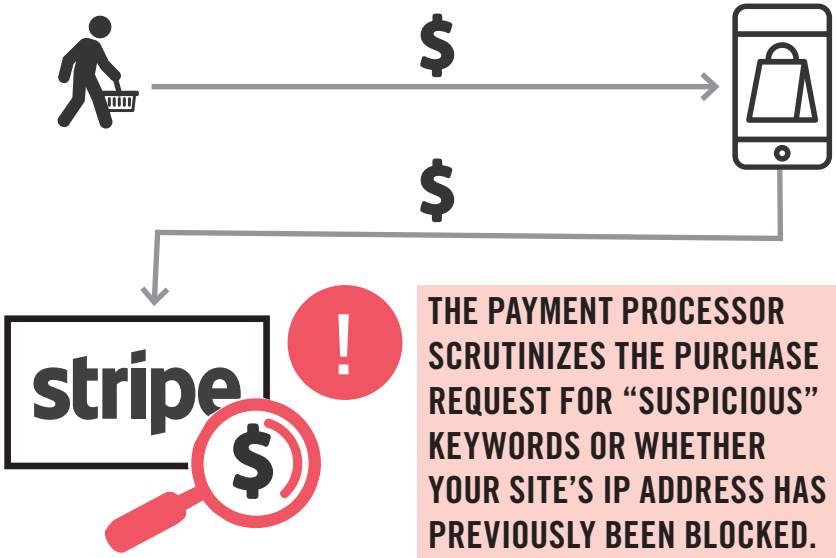
Things these algorithms are likely to flag:

- Has someone from your IP address had their account shut down before (e.g. created from or accessed from)? Companies keep very detailed logs of every IP address you've ever used and can easily view every account that's ever used one of those addresses.
- Has a previous account with your email address been shut down before? Or with the same SSN? Same mailing address?
- Has someone with a similar browser configuration to yours been shut down before?
- What words are used in the payment message? ask clients to stick to things like "vacation" "congratulations" or "drinks", or just leave it blank.

The people doing these manual reviews spend very little time on each individual case. They'll look at your website and often decide under a few minutes whether or not to allow something, and will often heavily err on the side of caution. Once they've decided to shut down one account, they'll regularly then shut down or freeze every account potentially associated with it (e.g. same IP address, same email address).

The next thing they do is notify all other platforms associated with your account to alert them that they believe you've engaged in "high risk" behaviour (e.g. if you were using Stripe through your Shopify account, Stripe would notify Shopify). **This is how cross-platform shutdowns come about so quickly,** and why it's so important to have different accounts separated as much as possible. Not just between different payment sites, but also between ad sites and social media. **Use different info for every site!**

HOW ACCOUNT SHUTDOWNS HAPPEN



THE PAYMENT PROCESSOR SCRUTINIZES THE PURCHASE REQUEST FOR "SUSPICIOUS" KEYWORDS OR WHETHER YOUR SITE'S IP ADDRESS HAS PREVIOUSLY BEEN BLOCKED.

!

THE BANK FLAGS THE PAYMENT REQUEST AS "SUSPICIOUS" OR "HIGH RISK" AND REFUSES TO ALLOW THE REQUEST TO BE PROCESSED.

!

THE PAYMENT PROCESSOR'S REFUSAL TO PROCESS YOUR PAYMENT REQUEST WILL LEAD TO THE SERVICE RUNNING YOUR ONLINE STORE TO SHUT DOWN YOUR ACCOUNT AND BAN YOUR IP ADDRESS.

MITIGATION STRATEGIES

- **Seriously consider using a VPN!**
  - VPNs are services that hide your IP address from sites you visit. You can use them both on your computer and your phone.
  - The way it works is that when the VPN is on, all traffic from your computer and phone first go to the VPN provider's servers, and then get passed on to the site you are visiting. Likewise, when the site you're accessing responds, the data gets passed to the VPN's servers, which are then forwarded back to you.
  - This means that you're shifting a lot of trust to the VPN provider. It's important to read a VPN provider's policies about whether or not they keep logs, under what circumstances they turn logs to law enforcement (e.g. do they explicitly say they require a warrant?), and so on. Some even have transparency reports about the number of times they've received requests for information from law enforcement and how they've responded.
  - Picking a VPN can be overwhelming, as there are many detailed (and kind of overwhelming) guides and comparison charts online (such as https://thatoneprivacysite.net/#detailed-vpn-comparison).
  - It's important to note that there are some sites that are known to block many IP addresses associated with VPNs (e.g. Netflix blocks all of Private Internet Access's IP addresses for video playback). Make sure you test this out and do some research before signing up for a long term plan with a VPN, or before the trial period ends.
  - VPN Terms of Service change regularly. Always research a VPN before picking it, even if it was recommended to you!
  - Avoid free VPNs! If they're free, it's because they're selling your data.
- **Never use the same email address twice** when signing up for these services. The more different your information across separate accounts is, the better.
  - You can make as many ProtonMail email accounts as needed!
  - Reminder: use different emails for ad sites and social media as well!
- **Use different phone numbers (and if possible, devices) for accounts**. It's easy and cheap to get multiple virtual phone numbers.
- **Use different names** when you can.
- You can get around the SSN issue by **filing an LLC and using the EIN associated with it to protect your privacy**. Credit Cards can be attached to your LLC (though not all payment processors will accept cards attached to business accounts).
- **Try to pick your payment processor based on your needs** to make contesting an account shut down later easier. For example, Stripe explicitly doesn't process payments involving the sales of sex toys. (Though honestly, they're all not that great when it comes to this.) **liaraslist.org** maintains a list of payment processors and the parts of their Terms of Service where they discriminate against sex workers.
- **Don't keep money in your payment processor account.** Payment processors have a history of seizing funds during account closures. To prevent this, transfer your payments as quickly as possible to a bank account.

WHAT TO DO IF IT HAPPENS

- Contacting the company and point out that you don't have a ToS violation or ask them to show you where the ToS violation is.
- See the last point from the previous section about choosing a payment processor. You can always start over.
- Finding executives/leaders from the organization and publicly shaming them on social media can sometimes be effective. Financial discrimination against sex workers means disproportionately discriminating against trans people, POC, women, and other minorities. They deserve all the public criticism and shaming when they do it.
- Reach out to tech journalists who have a history of covering sex work or anyone you know who might have connections to the platform.
- Sending a legal (or legal-sounding) letter helps.
- If using a form provided by the platform, sending it as often as you like might help. It won't get sent to the same content moderator, and one might be more sympathetic so you might as well try as many as possible.

SAMPLE LETTER

INSTRUCTIONS FOR FILLING OUT LETTER TO PLATFORMS

1. Insert the name of the platform. Fill in the name of the platform in all the other spaces that say “platform” in the letter.
2. Fill in your account ID/user name/handle (e.g. on Twitter, @ ghjsk12)
3. Insert “use” or “service”. Some platforms have a “terms of use” and others have “terms of service”, select the word that corresponds with the platform you are using. Fill in “terms of use/service” in all other spaces that say “ToS” in the letter.
4. Here you will go to the platform’s terms of use/service. In the terms of use/service, the platform will describe or list types of content that it prohibits.
    a. If there is a short list you can list the types of banned content that you have not posted. For example: “I have not: 1) Posted threatening or harassing content; 2) Shared child porn…etc.
    b If the description of what is prohibited is longer, you can summarize. For example: I have not posted content that is harmful to the community or prohibited in any other way.
5. Here say what the platform allows. The guidelines for acceptable content may be described in the terms of use/service or they might be in the platform’s menu under some other name like “community standards” or “community guidelines”. Some examples of content that is acceptable would be:
    a. Adult content (for example on twitter)
    b. Partially nude photos so long as…
    c. Content that meets community standards
6. If necessary, add some explanation of the content that is allowed. For example, on Twitter 18+ Accounts may have adult content. If there is nothing to add, delete the bracket.
7. Find a quote from the terms of use/service or community standards/guidelines. This quote could be something similar to: “to give everyone the power to create and share ideas and information instantly without barriers.”

[Date]
[Address of letter’s recipient]

To whom it may concern:

I write to you regarding the recent suspension of my account on your platform. Although [1:platform] is within its legal rights to remove content from its platform, this removal does not seem in line with any of the reasons why [platform] has stated it will removal accounts. Given that, I respectfully ask that you reinstate the account as soon as possible.

My account, [2], has not violated the terms of [3] of [Platform]. I have not: [4]. These are the reasons that are listed in [Platform]’s [ToS] as reasons for account suspension.

[Platform] allows the content that I have shared on my account. [Platform] permits [5]. [6]. My account is in conformity with these guidelines. I would ask that you point clearly to the specific guideline in the [ToS] that you believe my account is violating.

[Platform]’s [ToS] reflect a history of supportiveness to voices from a wide variety of communities and perspectives. Denying access to select groups of users silences their voices and makes it harder to build community. This runs directly counter to [Platform]’s stated goal [7]. I respectfully ask that [Platform] reinstate my account in accordance with that goal.

Sincerely,

[Name]
[Contact Information]
[Account Name]

MORE RESOURCES

HACKINGHUSTLING.COM
SURVIVORSAGAINSTSESTA.ORG
CODINGRIGHTS.ORG/4
SSD.EFF.ORG
HOLISTIC-SECURITY.TACTICALTECH.ORG

PRODUCED IN COLLABORATION WITH
HACKING//HUSTLING
FOR THE NOVEMBER 7 CONVENING AT THE
CYBERLAW CENTER AT THE BERKMAN KLEIN
CENTER FOR INTERNET & SOCIETY

Graphic design: Ingrid Burrington