



# Shielding the Brand: Taking Measures to Protect Intellectual Property Assets on Social Media

Having a robust social media presence is a must for modern businesses. It is a fast and easy way to reach hundreds or thousands of people just with the click of a button. This day and age, most organizations seemingly have at least a Facebook® and a Twitter® account, keeping the public up-to-date on everything from new product releases to details about upcoming events.

Yet, as important as it is to have multiple social media accounts, it is arguably just as crucial to protect these marketing and communication assets, shielding the company's brand from possible damage. To meet this goal, organizations can take a range of reactive and proactive measures. From preemptively registering usernames to utilizing online takedown tools, companies have the ability to take vital steps in order to protect their business.

## A preemptive approach to protection

As a company prepares to launch social media accounts, here are some steps they can take to begin to immediately protect their business.

### Registration

One of the most important first steps that a business can take with its social media strategy is registering multiple accounts. It is a similar concept to signing up for website domains. Companies will not only register a domain name in order to operate a website, but many also register additional similar sounding domain names in order to prevent others from creating confusingly similar or intentionally misleading websites. That is why you often see businesses or individuals or political campaigns registering multiple domain names, from using different Uniform Resource Locator ("URL") suffixes (such as .net, .org, or .biz) to creating variations on the URL itself, such as adding "the" before a restaurant's name. This prevents others from signing up those domain names, providing an organization's brand with a level of protection.

The same logic applies to social media. Companies should register accounts on nearly every type of social media they can think of—even if they do not intend to use that social media. For instance, a business can sign up for an Instagram® handle even if they do not want to use the platform just to prevent someone else from trying to open one up with their company's name. Also, like with putting variations on URLs for domain name registration, it can also be helpful for a business to take that same approach with social media usernames/handles. There is really no harm in doing this, given that social media accounts are usually free.

So, if you are a company that is building a social media presence, why not register for not only the Twitter handle you intend to use, but also some logical variations of that name? Adding "the" or "the real" or "official" before a Twitter handle and also registering those accounts prevents others from doing so. This simple step can be done in minutes and shields a business down the line in case someone elects to try to injure their brand name by registering a similar sounding account and causing problems online.

### Authenticating accounts

As social media grew in popularity, so did the presence of fake accounts. Countless Facebook and Twitter accounts have been made to impersonate celebrities and businesses in an effort to deceive the public. To

combat this, social media companies began utilizing an account authorization process, placing icons such as blue checkmarks on accounts to show the public that an indicated profile is authentic.

Verifying an account is an important step for the modern business to take. Since anyone can create a social media account, the door remains open for individuals to create accounts claiming they are a business in order to try and dupe the public. In general, it is a rather simple process—and one that can prevent unnecessary headaches down the line. For instance, consider Facebook's verification process for business pages. First, the individual applying for the verification needs to upload a form of accepted government ID, or two official documents if they do not have a photo ID. Once Facebook has reviewed and made the decision to proceed, then the individual provides requested business details, including a phone number. Then Facebook will send a verification code either by text, call, or email, and once that is submitted by the applicant—*voilà*, the page is verified.

From Instagram to Twitter, many social media companies provide a way for individuals to authenticate their accounts. It is a smart way to shield individuals and companies from being impersonated, and taking advantage of this protection is considered a must for businesses.

### Being vigilant about account security

You hear about these stories all the time—whether it involves a business or a celebrity or an everyday citizen—where lax security measures were in place that allowed nefarious actors to hack into a social media account. Once something like this happens, the hacker can access information associated with the account or put out statements purporting to be from the account's profile. Even though the hacked company was the victim of the attack, a security breach can do long-lasting damage to a business's brand. In addition to the hit they might take based on the content of the hacker's posts, the organization also loses public trust as they were shown to be vulnerable to a cyber-attack.

There is a relatively easy fix for companies. Though businesses are often targeted by hackers—especially more well-known brands—why not make it as difficult as possible for the attacker to gain access? For starters, passwords should be frequently changed. Keeping the same password—and using the same password across multiple accounts—may lead to potential exposure. On the same note, passwords should not be easy to guess. Too often, businesses try to make their passwords something easy to remember. According to a survey published in 2019 by the UK's National Cyber Security Centre, the five most common passwords were 123456, 123456789, qwerty, password, and 111111. Instead of making a password easy to remember, companies should create complex and hard to guess passwords that utilize combinations of uppercase and lowercase letters, numbers, and special characters.

Beyond password vigilance, there are other steps a company can take to protect the security of their accounts. One of the best ways to provide an additional layer of protection is to turn on two-step authentication. When this is activated, an account holder is sent a message via email or text message when they try to log in, providing them with an additional unique code that they need to enter. Another option provided by a number of social media companies is unrecognized login alerts. By turning this option on, social media companies like Facebook will reach out immediately if there is a login to your account that appears unusual.

### Creating IP notices for social media pages

Another step companies can take to protect what they post on their social media accounts is through providing IP notices. This is a relatively simple measure to take, and can help strengthen a potential case for infringement if an individual violates a company's IP rights.

For instance, if a business wants to prevent someone from reusing its copyrighted material, they can take the simple step of adding a copyright symbol to their social media page or putting it on a specific social media post. Now, since March 1, 1989, the laws have significantly changed in regard to copyright notice. An individual or

organization owns the copyright once they create a legally copyrightable work, eliminating the need to apply for a copyright registration. This means that giving notice is not necessary in order to retain rights in a written work. However, by making a simple statement that includes the copyright symbol (©), the year the work was created, and the copyright owner's name, notice is given that this work is subject to copyright protections. Then, if a work is later infringed upon, this notice can help protect against an innocent infringement defense and potentially allow for greater damages—though it needs to be noted that registering for a copyright with the U.S. Copyright Office is needed before a suit can be filed. Delaying in filing for a copyright registration can also adversely affect the ability to collect damages for past infringement.

Like with copyrighted material, a company can also protect its trademarks by giving notice—though in many cases a federal trademark registration as opposed to simply relying on common law rights is required to seek assistance from a social media company. To protect a registered trademark granted by the United States Patent and Trademark Office, a company can provide notice on a social media page or post by either placing a trademark symbol (®) next to the trademark, or by writing “Registered in United States Patent and Trademark Office” or a shortened version of that statement (“Reg. U.S. Pat. & Tm. Off.”). A business can also note that a trademark has been applied for by placing notice such as “trademark applied for.” This alerts the public that they intend to utilize a trademark as a source differentiator. Like with copyright, it is not required to include an explicit trademark identifier. However, it is highly recommended, as it provides strong evidence that potential infringers were made aware that the material is legally protected and allows for the recovery of a greater range of damages such as lost profits.

## Reactive measures

Unfortunately, misuse of IP and attacks on social media accounts are events that occur far too often. However, there are a range of steps that companies can take if they ever need to, such as the following.

### Using takedown forms

In an effort to combat the misuse of trademarks and copyrights, a number of social media companies offer the ability for the infringed party to request the removal of the offending content.

For instance, if someone discovers that their trademark has been misused on Facebook, they can begin to fill out a takedown form. First, the individual needs to show that they are the trademark's registered owner and provide details regarding the trademark's registration. Then they need to show where the trademark is being infringed upon. If Facebook finds that there is indeed an infringement, it will take down the violative post—though there remains the ability for the offending party to appeal the decision, meaning they will need to prove that the post does not actually infringe on any trademark rights.

Likewise, many social media sites provide a simple way for users to report copyright infringement. With copyright, it is always important to note if there was a fair use of the material, as that means it is unlikely a post will be removed. This includes parody, commentary, usage for criticism, and utilization for teaching purposes, among other uses. If there is no fair usage and a copyrighted work was posted without authorization, then an infringement notification can be filed and ultimately lead to the infringing material being removed from the social media site.

### Vigilantly monitoring for misuse

Once posts have been made on social media, a company should do what it can to monitor how that material is treated.

It is difficult to identify misuse when the infringing party has made their social media account and associated profile private. However, social media sites like Facebook and Twitter have built-in search functions that allow individuals to look for content within specific posts. These searches can also be focused on a specific timeframe, allowing the company to hone in on what they are looking for. By searching the business's name or specific content related to a company's protected intellectual property, a company may be able to sift through all material that is written about them and potentially find infringing posts.

Another key way to monitor against misuse is through specific tools such as Google Alerts. This provides a way for someone to be notified when certain terms, such as the name of a business, are mentioned online. In addition to being a great way to be on the lookout for what people are saying about your business, companies can utilize this tool in order to see if their protected IP is being misused in any way.

### Taking action

Ultimately, a business cannot control what an individual decides to post online, whether they are infringing on their intellectual property rights, misusing material, or harassing a business. However, that does not mean that they can't take steps to stop this misconduct.

If a company is facing misuse and wants to put an end to that conduct—and there are no other options left on the table, such as asking the offending party to take down an infringing post—they can take legal action. For starters, a business can have a cease and desist letter or a takedown notice sent, asking the individual responsible to remove the material that infringes on their IP rights or to stop with their harassing behavior.

Yet this does not always work. In that case, a company can take things further and pursue either a court injunction or a lawsuit. Now, this should be considered a last resort, as litigation is often expensive and time consuming. However, depending on what is at stake, this may be the best course of action. 🍷

DISCLAIMER: This paper provides background information of potential interest to facilitate and inform a reader's specific inquiry to be made with legal advisers of their choosing. It does not constitute legal advice. This paper is neither a guide nor an explanation of all relevant issues under consideration. Moreover, the law is ever evolving; observations made today may be inapplicable tomorrow. Fishman Stewart PLLC assumes no responsibility for any use of, or reliance on, this paper.