Infringing Apps and Your Brand

A Guide to Developing Your Enforcement Strategy

appdetex

Protecting Your Brand Online

Contents

Important notice - In an effort to help brandholders enforce their intellectual property rights, Appdetex is providing this information for use under the guidance of legal counsel. This information is not intended as a substitute for legal advice and should not be considered as legal advice from Appdetex. Any communications with alleged infringers is at your discretion and is your responsibility.

Infringing Apps and Your Brand

A Guide to Developing Your Enforcement Strategy

Executive summary

Mobile apps have risen to become one of the most popular ways for consumers to connect with brands. While mobile apps were popular prior to 2020, the current health crisis helped drive adoption and growth at an unprecedented rate. In the recently released App Annie "**State of Mobile 2021**" report, mobile app downloads reportedly increased 7% from the same period in 2019, with 218 billion new apps downloaded in 2020. That breaks down to roughly 590 million apps downloaded every single day.

> **In our increasingly digital world, consumers connecting with brands via apps have become some of the most profitable and engaged customers.**

Stay-at-home orders and lockdowns forced consumers to turn to online shopping, helping US e-commerce sales to reach an estimated **$794.50 billion for 2020**. That figure represents an increase of over 32.4% year-over-year. With this level of growth, it's no surprise bad actors are looking to profit.

While major app platforms employ precautions to reduce uploads of nefarious apps, cybercriminals continue to find ways to bypass these security measures. With over 7,000 new apps being introduced to the major app stores every day, it's up to brandholders to be proactive when it comes to protecting their intellectual property, their consumers and their mobile commerce, or m-commerce, revenues.

The goal of this guide is to discuss how to design an app enforcement strategy that addresses the risks posed to your business by infringing mobile apps. Topics include:

- **How your mobile commerce goals impact your enforcement strategy**
- **How to carry out enforcement at scale**
- **How to build an efficient enforcement framework**

Mobile commerce goals drive your enforcement strategy

Brandholders face countless threats in the mobile app space. Just one bad app can seriously damage the reputation of even the best-known brands and impact carefully-nurtured customer relationships.

Branded apps are a critical part of the consumer/company relationship. **Approximately half of all website traffic** now comes from mobile users and **four out of five Americans shop online** with over half using a mobile device to make their purchases. With this increase in screen time comes an increase in online spending. According to eMarketer, worldwide retail e-commerce for 2020 grew over **27% for a total of $4.28 trillion**.

Just one bad app can seriously damage the reputation of even the best-known brands and impact carefully-nurtured customer relationships.

Experts report over **227.5 million US consumers**, or approximately 88% of the population, shopped online in 2020. This number is predicted to grow, climbing to an estimated 230.5 million in 2021.

Furthermore, the app economy shows no signs of slowing down. People are spending an average of 4.2 hours a day on mobile apps. In 2020, consumer spending via mobile apps grew by 20% reaching a record $218 billion dollars. Following this trajectory, it's estimated that m-commerce sales will account for more than 72% of all e-commerce sales by 2021. Financial institutions are also seeing an increase in business conducted via mobile apps with **43% of Americans** reporting they prefer mobile banking over other banking methods.

As consumers increasingly accelerated their online activities, bad actors were quick to follow, adapting their attacks to focus in on these new targets. Rogue mobile apps and brand abuse due to social media impersonation accounted for **37% of all fraudulent transactions** recorded in Q1 of 2020. Overall, global mobile app fraud **grew by 26%** in the first quarter of 2020, the highest rate of growth in nearly two years. Financial institutions were particularly hard hit, with the **FBI issuing a public service announcement in June**, warning consumers and brands alike that bad actors were actively targeting mobile banking apps.

Bad actors are using intellectual property like trademarks, logos, and copyrighted content to fool unsuspecting consumers into thinking an app is affiliated or even created by a specific brand. Lured by the appeal of well-known intellectual property, consumers load these nefarious apps onto their phones and devices, making them vulnerable to data theft, scams or other threats.

One of the drivers behind the explosion of abusive apps is how easy it has become to create apps. Gone are the days when deep programming expertise was required to design, write and distribute apps. With the emergence of inexpensive cloud hosting and the availability of rich libraries of mobile code that can be downloaded from Github and other code repositories, developers with modest technical skill sets can now write and launch apps professionally and speedily. Sadly, along with the convenience of off-the-shelf code comes the risk of developers inadvertently integrating malware and other threats directly into their apps, creating secondary risks for brands and their mobile users.

While inadvertent distribution of malware is a problem for brands defending their users' mobile experiences, intentional distribution of ill-intended mobile apps is a serious issue. Malicious actors depend on the notoriety of well-known brands to promote their wares, and while all stores offer definitive mitigation for malware, the cost of downloading, analyzing and identifying malware is an expensive undertaking.

It is far easier, faster and less expensive to identify and mitigate brand-related threats and have them removed on the basis of intellectual property abuse than the aforementioned technical process, so intellectual property rights are an excellent first line of defense. However, recidivist actors who repeatedly use brands to distribute malicious code may require escalated action against the publisher.

Bad actors are using intellectual property like trademarks, logos, and copyrighted content to fool unsuspecting consumers into thinking an app is affiliated or even created by a specific brand.

These types of problems directly impact the safety and security of your customers and your ability to maintain trusted relationships with them - and affect your ability to grow your mobile commerce business. Combating these types of infringement requires a strong and swift response. Another type of infringement, however, stems from partners, franchisees or even your fans.

Fans, for example, may wish to extend the functionality of your branded app or create an 'homage' to your app, by developing new filters, stickers or characters. Partners and franchisees are interested in serving your shared customers, but divert them from your branded app to one of their own where they can transact business directly.

While not created with malicious intent, these types of infringing apps impact your ability to form a direct relationship with your customers, causing confusion and potentially impacting customer service.

With so much business in the digital world driven by word of mouth, reviews and social shares, these misguided apps siphon off customers and potential customers from your branded apps and can negatively impact your growth potential in mobile commerce.

Effectively addressing this type of infringement may require a more nuanced approach to enforcement since the infringers are valuable members of your brand ecosystem - your fans and business partners.

Statistics indicate that 40% of users will go to a competitor after a bad mobile experience.

Given the importance of this channel, ensuring users and customers get the authentic brand experience they expect means that brands need to incorporate a comprehensive mobile apps component into their brand protection and security strategies. Statistics indicate that **40% of users** will go to a competitor after a bad mobile experience, which means regardless of the infringement category, a rapid response should be your number one priority.

Enforcement at scale

Mitigating the potential damage that may result from an infringing app requires immediate action on the part of your enforcement team. Ensuring a strong foundation for successful enforcement is vital.

Begin by using a customer mindset. Work with your marketing team to determine the search terms your customers are using to find you online, including your company brand and variations such as common misspellings or abbreviations. Be sure to include specific product brand names and any words, hashtags, phrases or marketing slogans associated with your company. These are the same terms that bad actors will use to lure your customers away. Set up a monitoring system to alert your brand protection team when those words are used in app stores and online searches.

Consider your intellectual property portfolio and how it might be leveraged or enhanced to further protect your mobile users and your business. Are you able to marshal your trademarks, copyrights, and patents to effectively identify, enforce and mitigate abuse? How do malicious actors target your users on the basis of your intellectual property assets?

Considering bad actors' historical use of your assets, as you introduce new apps, products, and services, what filings must you make to ensure safety and security for your mobile users? Will you be able to identify your intellectual property within app marketplaces so that you can take fast action on the basis of images, text, and code that malicious actors employ to confuse and abuse?

Set your enforcement team up for success with an efficient workflow. Establish a framework for action with clear guidelines that allow your enforcement team to make decisions quickly and escalate issues as needed. Whether your team is made up of internal staff or external experts, it is crucial that your legal counsel is involved in setting these guidelines.

Statistics indicate that 40% of users will go to a competitor after a bad mobile experience.

When it comes to your customers' safety or security, time is of the essence. Responses to these types of infringing apps must be swift and decisive. The longer an infringing app is live, the longer it has to lure in unsuspecting victims and wreak havoc on your brand.

If the infringement is taking place on one of the major app stores, enforcement activity needs to be taken up directly with the store in which the infringing app is located. Make sure your claim is thoroughly documented and clearly demonstrates evidence of the infringement and the legal basis for the claim, such as trademark registration information. You may also need to demonstrate how the offending app has violated any of the app store's Terms of Services policies (TOS).

Some of the major app stores list publisher contact info for apps while others require a formal report or complaint before releasing contact information for the developer who created the infringing app. This is especially true in cases when the app may have been created by an overzealous fan or misguided franchisee with whom you wish to have a dialogue rather than an immediate takedown.

Because these types of infringement are carried out by valued members of your brand's ecosystem, they require more sensitivity when handling. In fact, it is best to minimize the risk of these types of problems occurring at all by publishing clear guidelines on how third-parties can use your brand.

These guidelines should include information about copyrights and trademarks, logo usage and acceptable use guidelines, including examples of proper and improper usage. While you do not want to be in the position of advising developers on how to create apps, you do want to be sure they have a clear framework for using your trademarks or other intellectual property in a way that protects your property.

These points are especially important if a third-party ecosystem is an important growth driver to your brand or business goals.

It is crucial that your legal counsel is involved in setting these guidelines.

You may also want to consider creating co-marketing or technical partnerships with developers that include contractual terms of engagement. These terms will provide additional leverage should you need to ask the developer to resolve infringement issues.

In situations where you have a partnership with a developer, it may be possible to reach out to them directly before initiating formal processes with the app stores. Similarly, both Google Play and Amazon typically list publisher contact information, meaning it may be possible to reach a resolution with the developer before having to resort to going to the app store directly.

If your enforcement efforts with app stores are unsuccessful, outside counsel may have to become involved. Counsel may recommend continued escalation such as an attorney cease-and-desist letter filing a civil action, and/or working with law enforcement in the case of fraud or other criminal activity.

Setting Up an Efficient Mobile App Enforcement Framework

Topics to consider for your framework include:

- What kind of documentation about the infringement should be gathered, such as screenshots? In cases where an app is suspected to contain malware, you may want to consider having your forensic team download it for in-depth analysis.
- How to determine when an infringement can be dealt with in-house, with brand protection vendors, and when it must be escalated to legal counsel.
- Setting up staff training sessions to ensure familiarity with the different app store tools including reporting forms and the unique processes each store employs. App stores often delay enforcement or are unable to enforce upon abusive apps if forms are not completed correctly and completely.
- Ensuring that all applicable trademark and copyright information for your brand is available in a centralized location should that documentation be required for your claims.
- Identifying approved developers, licensees, and Application Programming Interface (API) partners on an 'allow' list to require an extra level of scrutiny that can help prevent accidental enforcements.
- Create protocols for ensuring that enforcement staff choose the broadest enforcement option possible. For example, enforcement on the basis of copyright infringement is generally global, while trademark-based enforcement is only applicable in the regions where companies hold trademarks.
- Search for the infringing apps found and enforced upon in an individual store in other primary stores, their international stores, in localized language, as well as third-party and "sideloading" sites. Publishers that are banned in one app marketplace flee to others or take other actions to avoid being banned from distributing their nefarious applications.
- Systemically deconstruct the intent of the infringing app and seek to eradicate the issue at its source. For example, if an app is seeking to distribute your copyrighted material, find the host and take down the source host via the DMCA or the European Copyright Directive.
- Look for recidivist app publishers and developers and seek escalated actions against them in app stores, and for the most egregious, through civil or criminal prosecution.

Summary

Having a comprehensive brand protection plan in place can help streamline your enforcement process and enable you to spot infringing apps before they become a threat to your m-commerce initiatives.

Understanding the types of infringement that can occur and the impact they can have on your customer relationships and business goals should be a vital component of your plan. Providing a framework for action to your staff is also key for rapid and effective enforcement, especially in the face of threats to safety and security.

One of the most effective ways to increase compliance for enforcement efforts is to partner with a brand protection company that is well-versed in the world of apps and mobile commerce. With thousands of new apps being uploaded every day in multiple app stores, maintaining vigilance can be overwhelming. A brand protection company that is familiar with the enforcement methods for each store is key to swift, streamlined, and effective enforcement. You'll enjoy peace of mind while freeing resources and attention to focus on engaging with your customers and advancing your mobile and m-commerce initiatives.

> **The longer an infringing app is live, the longer it has to lure in unsuspecting victims and wreak havoc on your brand.**

About Appdetex

Appdetex is in the business of solving business problems related to digital risks. With deep roots in intellectual property law and applying technical innovation to business challenges, Appdetex is dedicated to the success of brand protection professionals and is trusted by some of the world's largest brands, including consumer goods, gaming platforms, media, entertainment, and financial services companies.

Founded in 2012 by veterans in brand protection, the Appdetex team puts decades of experience in digital risk mitigation to work on behalf of your brand. Disrupting highly-organized, automated, and widespread systems of abuse requires technology

and expertise. The Appdetex team has extensive experience in crafting efficient enforcement strategies at scale, from traditional takedown notices to applying leverage to deactivate criminal networks at their source.

As a result, Appdetex provides comprehensive brand protection that mitigates a wide spectrum of abuse - swiftly. We balance robust brand protection with sensitivity to your customers and customer communities and deliver quantifiable benefits for your brand and your business.

appdetex

www.appdetex.com

info@appdetex.com

(855) 693-3839