QUINN EMANUEL URQUHART & SULLIVAN LLP
Rachel Herrick Kassabian (SBN 191060)
rachelkassabian@quinnemanuel.com
Yury Kapgan (SBN 218366)
yurykapgan@quinnemanuel.com
Margret M. Caruso (SBN 243473)
margretcaruso@quinnemanuel.com
555 Twin Dolphin Dr., 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Brian Mack (SBN 275086)
brianmack@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6400
Facsimile: (415) 875-6700

Attorneys for Plaintiff WPEngine, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

WPENGINE, INC., a Delaware corporation,

Plaintiff,

vs.

AUTOMATTIC INC., a Delaware corporation; and MATTHEW CHARLES MULLENWEG, an individual,

Defendants.

Case No.: 3:24-cv-06917-AMO

DECLARATION OF RAMADASS PRABHAKAR IN SUPPORT OF PLAINTIFF WPENGINE, INC.'S REPLY IN SUPPORT OF ITS MOTION FOR PRELIMINARY INJUNCTION

Judge: Honorable Araceli Martínez-Olguín
Courtroom: 3, Oakland Courthouse
Hearing Date: November 26, 2024
Hearing Time: 10:30 a.m.

I, Ramadass Prabhakar, declare as follows:

1. I am Senior Vice President and Chief Technology Officer at WPEngine, Inc. (“WPE”). I have personal knowledge of all the facts set forth in this declaration, and if called upon to do so by the Court, I could and would testify competently thereto.

Inaccuracies Regarding Defendants’ Blocking of WPE Customers

From wordpress.org

2. As stated in my October 18, 2024 declaration, on September 25, 2024, I became aware that Matt Mullenweg, CEO of our competitor Automattic, had banned WPE customers who host their WordPress installations on WPE servers from accessing wordpress.org resources through the WordPress administration panel, which includes downloading community developed themes and plugins, including themes and plugins developed by WPE. This means that WPE customers and users would no longer be able to install new plugins and themes from wordpress.org. This also means that WPE’s customers and users would no longer be able to update from the administrative panel their existing plugins (whether WPE plugins, or any other of the more than 50,000 plugins hosted at the wordpress.org repository) and themes to address bugs and security vulnerabilities, or add new functionality.

3. In their opposition to WPE’s motion for preliminary injunction, Mr. Mullenweg and Automattic state that “at no time was WP Engine or any third party prevented from accessing, updating or downloading any WordPress software, themes or plugins.” Opp. at 8 (citing Abrahamson Decl. ¶¶ 10, 14). That statement is misleading. On September 26, 2024, and for part of September 27, 2024, WPE customers and users were in fact blocked from accessing wordpress.org resources through the WordPress administrative panel, including themes and plugins. Although access was briefly restored on September 27, 2024, WPE customers and users were blocked again on October 1, 2024, as described in more detail below. As Mr. Mullenweg himself acknowledged in a September 27, 2024 blog post on wordpress.org, due to his actions, he has “heard from WP Engine customers that they are frustrated that WP Engine hasn’t been able to make updates, plugin directory, theme directory, and Openverse work on their sites.” This of course was Mr. Mullenweg’s doing. Attached hereto as Exhibit E is a true and correct copy of a webpage I

caused to be printed out containing this post, located at https://wordpress.org/news/2024/09/wp-engine-reprieve/, dated September 27, 2024 and titled "WP Engine Reprieve."

4. In their opposition to WPE's motion for preliminary injunction, Mr. Mullenweg and Automattic state that WPE customers and users could still have manually downloaded each of their plugins/themes from wordpress.org and then manually uploaded those plugins to their websites. Opp. at 9 (citing Abrahamson Decl. ¶¶ 10-11, 14). While technically not impossible, this "workaround" is impractical for many reasons. ***First***, without access to wordpress.org—which supplies that data needed to notify users that a later version of a plugin is available—WPE users would not know that their plugins require updating. As a result, Defendants' suggestion is not in fact a workaround for practical purposes, and does not alleviate the harm WPE has suffered and continues to suffer. ***Second***, many WordPress users (including WPE users) are not aware that it is possible to update a plugin in the manual way articulated by Mr. Mullenweg and Automattic because almost all users have always relied on single-button-click updates through the administrative panel which download plugins directly from wordpress.org and install them automatically, or automatic updates which regularly download and install plugins from wordpress.org without any action by the user. It is not surprising that most WordPress users install plugins in this automated way given that this functionality is hardcoded into the WordPress core software and is recommended on the "Updating WordPress" documentation page at wordpress.org:

> <u>Automatic Background Updates</u>
>
> For WordPress 3.7+, you don't have to lift a finger to apply minor and security updates. Most sites are now able to automatically apply these updates in the background. If your site is capable of one-click updates without entering FTP credentials, then your site should be able to update from 3.7 to 3.7.1, 3.7.2, etc. (You'll still need to click "Update Now" for major feature releases.)
>
> <u>One-click Update</u>
>
> WordPress lets you update with the click of a button. You can launch the update by clicking the link in the new version banner (if it's there) or by going to the Dashboard > Updates screen. Once you are on the "Update WordPress" page, click the button "Update Now" to

> start the process off. You shouldn't need to do anything else and, once it's finished, you will be up-to-date.
>
> One-click updates work on most servers. If you have any problems, it is probably related to permissions issues on the filesystem.

Attached hereto as Exhibit F is a true and correct copy of a webpage I caused to be printed out, located at https://wordpress.org/documentation/article/updating-wordpress/, which is a post on wordpress.org titled "Updating WordPress" described above. Nowhere on the wordpress.org website does it recommend using the manual uploading mechanism. The "Plugin and themes auto-updates" documentation page states that: "If you are running WordPress 5.5 or more and those [update] controls are still unavailable, it probably means the feature was partially or completely deactivated by your hosting company or by a plugin." Attached hereto as Exhibit O is a true and correct copy of a webpage I caused to be printed out, located at https://wordpress.org/documentation/article/plugins-themes-auto-updates/, which is a post on wordpress.org titled "Plugin and themes auto-updates." Nowhere does the wordpress.org website state that this functionality may be compromised by Mr. Mullenweg blocking access to wordpress.org.

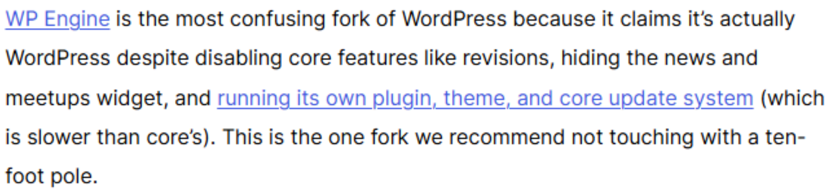
5. ***Third***, many WPE users manage many websites, each of which may use several dozen plugins and themes, making this manual update process so onerous and time consuming that it's not a true workaround to the blocking of wordpress.org. It is like saying that a person can walk from San Francisco to Los Angeles, rather than fly or drive. While it is technically correct, it is impractical if not impossible to do so.

<u>WPE's Mirror Does Not Redress the Harm to WPE and Its Customers</u>

6. As explained in my prior declaration, on September 27, 2024, in reaction to public outcry, Mullenweg announced that he was temporarily restoring WPE's access to wordpress.org, but not permanently. Instead, he stated that he would block access again on October 1, 2024. He blocked WPE's access to wordpress.org again on October 1, 2024. In anticipation of that event, WPE created a partial "mirror" of the plugin and theme repositories at the wordpress.org website to help alleviate the disruptions that WPE users and customers would face by Mullenweg's renewed

blocking. WPE's partial mirror has only focused on making the latest version of plugins and themes from wordpress.org available to its customers.

7. In their opposition to WPE's motion for preliminary injunction, Automattic and Mr. Mullenweg state that WPE users and customers are not being harmed because WPE has deployed a "solution that fully restored its regular workflow practices," by creating this mirror of wordpress.org. Opp. at 8 (citing Xu Decl. ¶ 7). This too is incorrect. Among other things, the "solution" only applies to WPE customers and not WPE itself. WPE remains forced to operate a dramatically irregular workflow in order to provide a limited workaround to Defendants' harmful actions blocking updates to plugins from the administrative panel, and WPE also remains unable to support and maintain its owned plugins and themes hosted at wordpress.org. Regarding the workflow for WPE customers, Defendants' argument is contradicted by Mr. Mullenweg's own statements, as he represented on his blog that WPE's mirror is "slower than core's" and shouldn't be touched "with a ten-foot pole," meaning that Mr. Mullenweg himself believes WPE's mirror is an inferior workaround to the plugin, theme, and core update directories hosted on wordpress.org.



WP Engine is the most confusing fork of WordPress because it claims it's actually WordPress despite disabling core features like revisions, hiding the news and meetups widget, and running its own plugin, theme, and core update system (which is slower than core's). This is the one fork we recommend not touching with a ten-foot pole.

Attached hereto as Exhibit G is a true and correct copy of a webpage I caused to be printed out, located at https://wordpress.org/news/2024/10/spoon/, which contains the blog post discussed above on the wordpress.org website. Defendants have also sent solicitations to our customers stating that "WP Engine's access to WordPress.org has been restricted, which could impact sites, especially regarding plugin and theme installations or updates that are sourced directly from the WordPress.org repository." Dkt. No. 20 ¶ 29 (Teichman Decl.).

8. Furthermore, WPE's mirror of wordpress.org has several significant limitations, by design and as dictated by wordpress.org's own procedures. ***First***, wordpress.org throttles the rate at which third parties can download its content. As a result, creating and updating a mirror can often take several days. ***Second***, wordpress.org limits the data that it makes available to WPE. For

example, while WPE is able to download the source code for WordPress plugins and themes hosted on wordpress.org, it does not make available to WPE critical information about plugins, such as ratings, reviews, and download and installation counts, which is often important information for WordPress users to assess the trust and reliability of a WordPress plugin. ***Third***, if Mr. Mullenweg decides to make any minor changes to the function or content of wordpress.org, it could break WPE's process in creating and updating its mirror. Given that Mr. Mullenweg has promised further attacks on WPE, it is not out of the question that Defendants may—among other things—make changes to the function or content of wordpress.org to intentionally harm WPE. ***Fourth***, wordpress.org does not notify WPE when plugins and themes on wordpress.org are updated, and thus need to be downloaded to WPE's mirror. As a result, it is possible that WPE's mirror could go out of sync with wordpress.org, leaving WPE customers without critical security patches, or otherwise access to updates. ***Fifth***, wordpress.org explains that "[t]he latest version of WordPress is always available from the main WordPress website at https://wordpress.org. Official releases are not available from other sites — **never** download or install WordPress from any website other than https://wordpress.org" (emphasis in original). Attached hereto as Exhibit H is a true and correct copy of a webpage I caused to be printed out, located at https://developer.wordpress.org/advanced-administration/security/hardening/, which is an article on the developer portal of the wordpress.org website. This admonition on wordpress.org about "official" releases and updates may dissuade users from relying on a mirror not maintained by and available on wordpress.org. In summary, wordpress.org has not been built in a way to allow third-parties to reliably create a mirror of it, making the process of creating a mirror tedious, risky and unreliable.

Inaccuracies Regarding Defendants' Blocking of WPE From Accessing Plugin Listings And Developer Resources On wordpress.org

9. As described in my opening declaration, in addition to blocking WPE customer access to wordpress.org from their administrative panel, Defendants also blocked WPE software developers from the plugins that they have developed and host on wordpress.org. In their opposition to WPE's motion for preliminary injunction, Automattic and Mr. Mullenweg state that WPE "has full control of its own repository of its own plugins." Opp. at 10 (citing Abrahamson Decl. ¶¶ 14-

15). This is misleading and incorrect. As noted above, Mr. Mullenweg and Automattic have blocked WPE's access to wordpress.org, cutting off its ability to update those plugins in any way, including fixing the description and code.

10. Mr. Mullenweg and Automattic also state that WPE can host all of its plugins on its own website at https://wpengine.com/solution-center/plugins/. However, this makes no sense. The WordPress software is hardcoded to download plugins from wordpress.org using the administrative panel. This means that that the WordPress core software code contains instructions to the user's computer such that the WordPress administrative panel can only download plugins from wordpress.org. The WordPress administrative panel is also hardcoded to interact with wordpress.org for the purpose of detecting updates to plugins and installing updates. Overall, wordpress.org is referenced over 1,500 times in the core WordPress code. Attached hereto as Exhibit P is a true and correct copy of a post on X located at https://x.com/joeydi/status/1849070363335864732 that I caused to be printed out. This instruction to download plugins from wordpress.org (and only wordpress.org) cannot be changed without modifying the core WordPress code, something that a typical WordPress user that is not hosted by WPE is unable to easily do. Plugin users who are not paying WPE hosting customers, and therefore not protected by WPE's partial mirror solution, would have no idea to look to WPE's website to download updates to the plugins. And WPE would have no way to notify these plugin users of the availability of updates because WPE does not know the identity of users who have previously downloaded its plugin for free from wordpress.org.

11. Finally, by being blocked from wordpress.org, WPE does not have access to the software developer community, including community-based support forums, that use wordpress.org to communicate. Defendants do not appear to dispute this or suggest there is a viable workaround for WPE. By being blocked from the developer community, WPE cannot communicate with WordPress developers to notify them of bugs or security issues with WPE plugins, provide support, respond to requests for feature updates, or discuss future updates. This materially impacts WPE's ability to provide the best WordPress experience possible for the users of its plugins.

Inaccuracies Regarding Defendants' Claims Concerning WPE's ACF Plugin

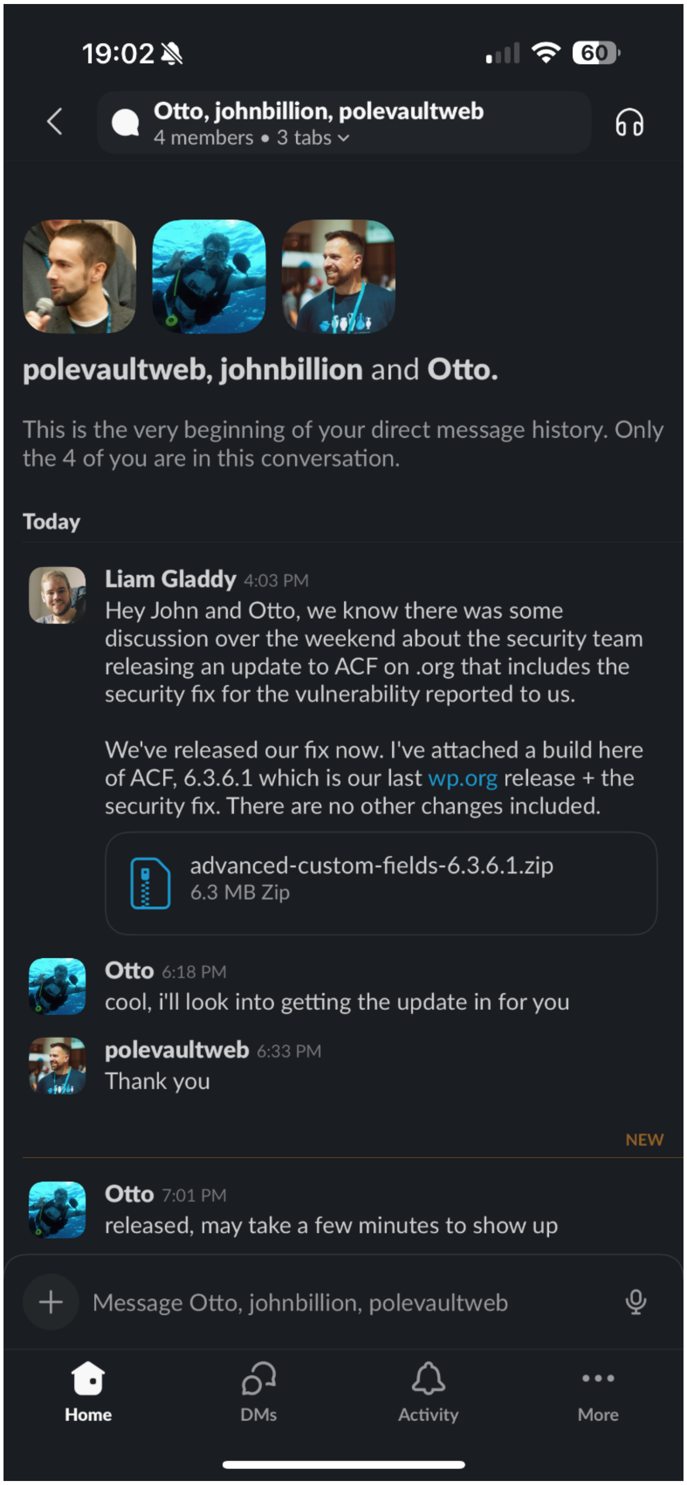
12. As stated in my October 18, 2024 declaration, WPE is the developer of one of the most popular WordPress plugins called Advanced Custom Fields (ACF). When installed on a website built using WordPress, this plugin extends the functionality of WordPress to allow WordPress to collect and store additional types of information and essentially function as a fully-featured content management system, a major enhancement of functionality. As explained in the Brunner Declaration of October 18, 2024, WPE acquired the ACF plugin and its developer team through the acquisition of another company. Dkt. No. 21 ¶ 63 (Brunner Decl.). For many years the ACF plugin was hosted at the webpage https://wordpress.org/plugins/advanced-custom-fields/, and maintained and updated by WPE and its team of ACF developers.

13. On October 12, 2024, without WPE's consent, Defendants effectively took over WPE's ACF plugin by editing the ACF plugin code and listing page in several ways. For example, Mr. Mullenweg changed the name of the plugin from "Advanced Custom Fields" to "Secure Custom Fields" ("SCF"). Mr. Mullenweg also changed the name of the author of the plugin from "WP Engine" to "WordPress.org." Because Mr. Mullenweg blocked WPE from wordpress.org, WPE has no ability to fix these issues, or to upload new versions of the ACF plugin to wordpress.org.

14. Defendants publicly stated that they took over the ACF plugin hosting page because of an alleged security vulnerability in the plugin. This is not credible. As explained in the Brunner Declaration, on October 4, 2024, Automattic sent an email notification about a minor security vulnerability with the ACF plugin to WPE and copied Mr. Mullenweg and WPE's CEO, Heather Brunner. *See* Dkt. No. 21 (Brunner Decl.), Ex. H at 1. Mr. Mullenweg states that it was the "Wordpress security team" who notified WPE of this security vulnerability. *See* Opp. at 6 (citing Mullenweg Decl. ¶¶ 45-46). This too is false. It was Mr. Mulllenweg's for-profit company, the "Automattic Security Team," who emailed WPE about the alleged security vulnerability. *See* Dkt. No. 21-8 (email from "Automattic Security Team" (security@automattic.com) to acf-security@wpengine.com)). The email also indicated that "[i]f we don't receive a response from you within the next 5 business days, we may need to reach out to the Marketplace where your extension is published for further assistance in fixing the issues we have found." *Id*. The next 5 business days

from October 4, 2024 would have been October 11, 2024. The supposed vulnerability was minor and WPE released a security update on October 7, 2024, within 72 hours of receiving the security notification – well before the arbitrary deadline Automattic imposed.

15. In their opposition to WPE's preliminary injunction motion, Mr. Mullenweg and Automattic claim that "WP Engine never responded to that [security vulnerability] disclosure." Opp. at 6 (citing Mullenweg Decl. ¶ 45). That is incorrect. WPE promptly responded on October 7 via Slack with a security patch within 72 hours of the notice.



polevaultweb, johnbillion and **Otto.**

This is the very beginning of your direct message history. Only the 4 of you are in this conversation.

Today

Liam Gladdy 4:03 PM
Hey John and Otto, we know there was some discussion over the weekend about the security team releasing an update to ACF on .org that includes the security fix for the vulnerability reported to us.

We've released our fix now. I've attached a build here of ACF, 6.3.6.1 which is our last wp.org release + the security fix. There are no other changes included.

advanced-custom-fields-6.3.6.1.zip
6.3 MB Zip

Otto 6:18 PM
cool, i'll look into getting the update in for you

polevaultweb 6:33 PM
Thank you

NEW

Otto 7:01 PM
released, may take a few minutes to show up

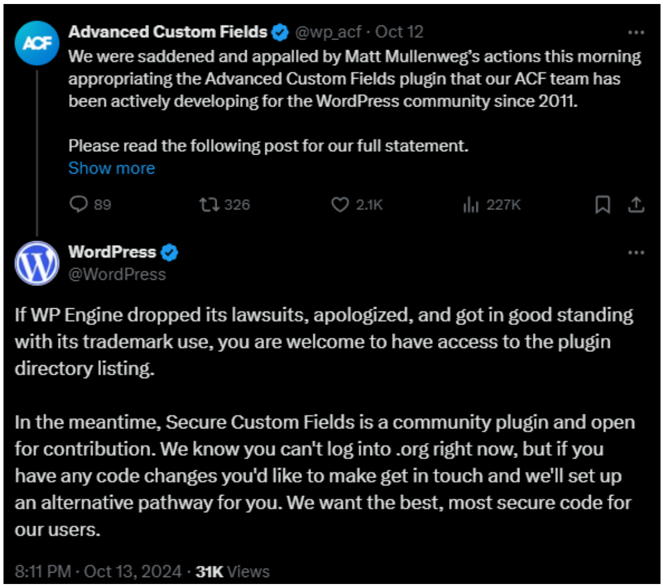
Attached hereto as Exhibit I is a true and correct copy of a series of Slack messages between WPE employee Liam Gladdy and Samuel Wood I caused to be printed out. The "Otto" referred to in this chat is Samuel Wood, who works with Mr. Mullenweg at his venture capital firm Audrey Capital. Attached hereto as Exhibit J is a true and correct printout of Mr. Wood's profile on wordpress.org (https://profiles.wordpress.org/otto42/), showing that his username on Slack is @otto. Attached hereto as Exhibit K is a true and correct printout of Mr. Wood's LinkedIn profile (https://www.linkedin.com/in/samwood/), which lists Mr. Wood as "Tech Ninja" for Audrey Capital.

16. WPE could not submit a security patch for ACF directly to wordpress.org because Mr. Mullenweg had blocked WPE's access to wordpress.org. So WPE sent the security patch to Mr. Wood, who uploaded the security patch to wordpress.org as a new release. After submitting this security patch, we never heard from Automattic or Mr. Mullenweg again about this security vulnerability.

17. On October 5, 2024, just one day after Automattic's security team sent the vulnerability notification, Mr. Mullenweg wrote a post on the X social media website stating: "What are the best alternatives to Advanced Custom Fields @wp_acf for people who want to switch away? Is there an easy way to migrate? I suspect there are going to be millions of sites moving away from it in the coming weeks." *See* Dkt. No. 18-11 (Jenkins Decl. Ex. 11). (https://x.com/photomatt/status/1842500184825090060). No where in that post did Mr. Mullenweg state that there were security issues with the ACF plugin.

18. Mr. Mullenweg also now states that "[w]hile WP Engine did update the version of ACF hosted on the WP Engine website to patch the disclosed vulnerability, a review of that patch by the WordPress security team indicated that the patch was incomplete." Opp. at 6 (*citing* Mullenweg Decl. ¶ 45). This is also false. The vulnerability that Automattic disclosed to WPE was fixed in its entirety.

19. As for the true reason Defendants took the ACF plugin from WPE, what we know is that Mr. Mullenweg publicly stated on October 13, 2024, in response to a post about the ACF plugin being misappropriated by Defendants, that WPE would be "welcome to have access to the plugin directory listing" back "[i]f WP Engine dropped its lawsuits, apologized, and got in good standing with its trademark use." *See* Dkt. No. 18-25 (Jenkins Decl. Ex. 26). Mr. Mullenweg's statement did not mention anything about supposed security vulnerabilities in ACF or an incomplete patch.



Advanced Custom Fields @wp_acf · Oct 12

We were saddened and appalled by Matt Mullenweg's actions this morning appropriating the Advanced Custom Fields plugin that our ACF team has been actively developing for the WordPress community since 2011.

Please read the following post for our full statement.

Show more

89 326 2.1K 227K

WordPress @WordPress

If WP Engine dropped its lawsuits, apologized, and got in good standing with its trademark use, you are welcome to have access to the plugin directory listing.

In the meantime, Secure Custom Fields is a community plugin and open for contribution. We know you can't log into .org right now, but if you have any code changes you'd like to make get in touch and we'll set up an alternative pathway for you. We want the best, most secure code for our users.

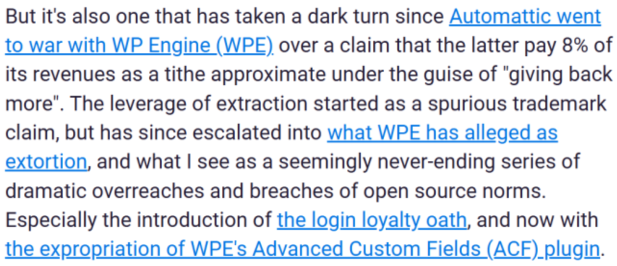
8:11 PM · Oct 13, 2024 · 31K Views

Dkt. No. 18-25 (Jenkins Decl. Ex. 26). (https://x.com/WordPress/status/1845663751342883195).

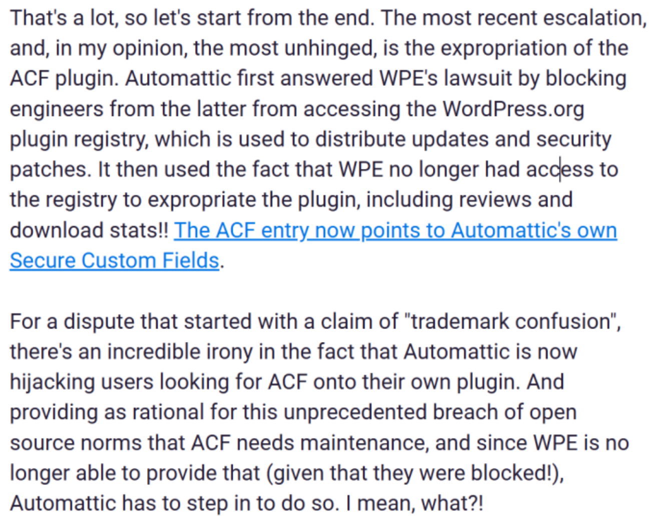
20. Mr. Mullenweg claims that the "WordPress security team forked [the ACF plugin], and named that fork SCF." Opposition at 6 (citing Mullenweg Decl. ¶ 46). Mr. Mullenweg further states "[f]orking—where a developer creates a separate and independently developed version of an existing open-source project—is a common practice in the open-source software community and is how the WordPress software originated." Opposition at 6 (citing Mullenweg Decl. ¶ 47). As I explained in my prior declaration, Defendants' taking of WPE's ACF plugin was not a true fork. Based on my experience in the software industry, "forks" of open source software are common. But in a "fork," a software developer will create a new copy of the code and host that code on a new website or URL so there is no confusion between the original software and the new "forked" software. The newly forked software would initially have no reviews, ratings, or download history. This is not what happened here, where Mr. Mullenweg co-opted the ACF listing page (*i.e.*, its URL "slug"), and its users and reviews, and caused many ACF users' websites to download the SCF software without their knowledge or consent. The WordPress community has expressed shock and condemnation of what Defendants did in taking ACF from WPE, including ACF's download counts and customer reviews and ratings. Attached are some of the public comments from WordPress community members and open source leaders expressing their outrage:

- “The most recent escalation, and, in my opinion, the most unhinged, is the expropriation of the ACF plugin. Automattic first answered WPE's lawsuit by blocking engineers from the latter from accessing the WordPress.org plugin registry, which is used to distribute updates and security patches. It then used the fact that WPE no longer had access to the registry to expropriate the plugin, including reviews and download stats!! The ACF entry now points to Automattic’s own Secure Custom Fields . . . For a dispute that started with a claim of "trademark confusion", there’s an incredible irony in the fact that Automattic is now hijacking users looking for ACF onto their own plugin. And providing as rational for this unprecedented breach of open source norms that ACF needs maintenance, and since WPE is no longer able to provide that (given that they were blocked!), Automattic has to step in to do so. I mean, what?! . . . Weaponizing open source code registries is something we simply cannot allow to form precedence. They must remain neutral territory. Little Switzerlands in a world of constant commercial skirmishes.”

Attached hereto as Exhibit L is a true and correct copy of a webpage I caused to be printed out, located at https://world.hey.com/dhh/open-source-royalty-and-mad-kings-a8f79d16, which is dated October 13, 2024 and is a blog post titled “Open source royalty and mad kings.”

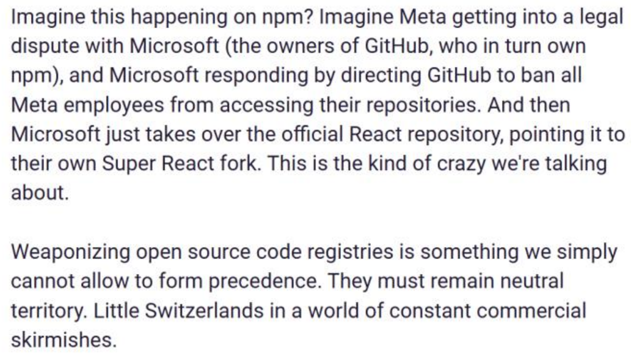


But it's also one that has taken a dark turn since Automattic went to war with WP Engine (WPE) over a claim that the latter pay 8% of its revenues as a tithe approximate under the guise of "giving back more". The leverage of extraction started as a spurious trademark claim, but has since escalated into what WPE has alleged as extortion, and what I see as a seemingly never-ending series of dramatic overreaches and breaches of open source norms. Especially the introduction of the login loyalty oath, and now with the expropriation of WPE's Advanced Custom Fields (ACF) plugin.



That's a lot, so let's start from the end. The most recent escalation, and, in my opinion, the most unhinged, is the expropriation of the ACF plugin. Automattic first answered WPE's lawsuit by blocking engineers from the latter from accessing the WordPress.org plugin registry, which is used to distribute updates and security patches. It then used the fact that WPE no longer had access to the registry to expropriate the plugin, including reviews and download stats!! The ACF entry now points to Automattic's own Secure Custom Fields.

For a dispute that started with a claim of "trademark confusion", there's an incredible irony in the fact that Automattic is now hijacking users looking for ACF onto their own plugin. And providing as rational for this unprecedented breach of open source norms that ACF needs maintenance, and since WPE is no longer able to provide that (given that they were blocked!), Automattic has to step in to do so. I mean, what?!



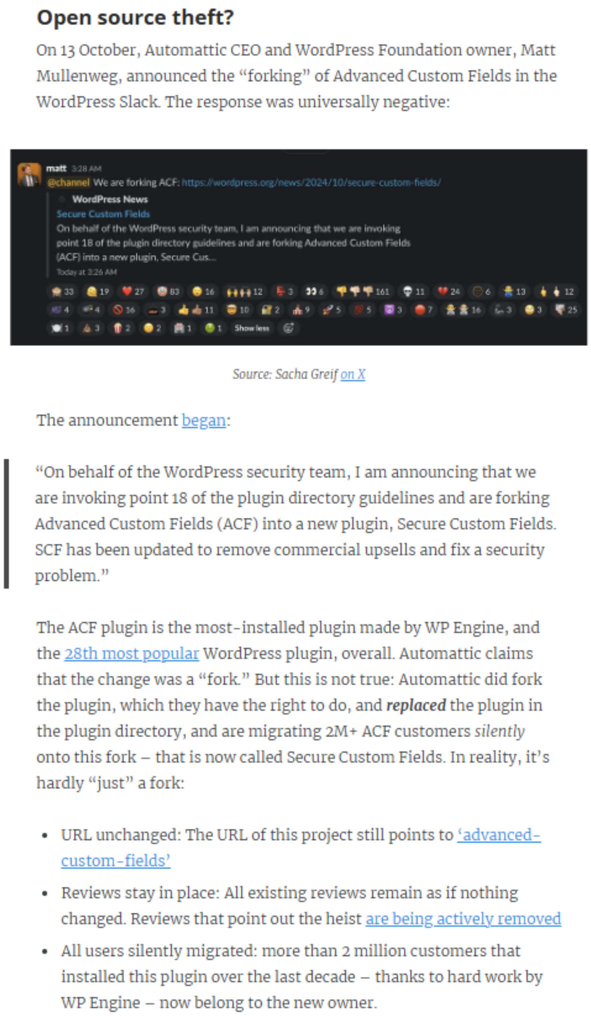
Imagine this happening on npm? Imagine Meta getting into a legal dispute with Microsoft (the owners of GitHub, who in turn own npm), and Microsoft responding by directing GitHub to ban all Meta employees from accessing their repositories. And then Microsoft just takes over the official React repository, pointing it to their own Super React fork. This is the kind of crazy we're talking about.

Weaponizing open source code registries is something we simply cannot allow to form precedence. They must remain neutral territory. Little Switzerlands in a world of constant commercial skirmishes.

- "Open source theft? On 13 October, Automattic CEO and WordPress Foundation owner, Matt Mullenweg, announced the 'forking' of Advanced Custom Fields in the WordPress Slack. The response was universally negative. . . . But this is not true: Automattic did fork the plugin, which they have the right to do, and replaced the plugin in the plugin directory, and are migrating 2M+ ACF customers silently onto this fork – that is now called Secure Custom Fields. . . . Sadly, it seems that Automattic has thrown away unwritten but valuable ethics in an effort to hit WP Engine where it hurts. But leveraging a supposedly neutral platform (the WordPress plugin manager) should not be the way to win in business – at least not in open source. . . . Automattic will forever be associated with being the first in crossing an

> ethical red line in open source web software: commandeering another team's actively maintained plugin, using a nonprofit foundation to orchestrate a pre-meditated attack, and ignoring ethics of open source. All in the name of trying to harm their biggest competitor. Automattic: it's time to play fair."

Attached hereto as Exhibit M is a true and correct copy of a webpage I caused to be printed out, located at https://blog.pragmaticengineer.com/did-automattic-commit-open-source-theft/, which is a blog post on a website titled "Did Automattic commit open source theft?"



Open source theft?

On 13 October, Automattic CEO and WordPress Foundation owner, Matt Mullenweg, announced the "forking" of Advanced Custom Fields in the WordPress Slack. The response was universally negative:

matt 3:28 AM
@channel We are forking ACF: https://wordpress.org/news/2024/10/secure-custom-fields/
WordPress News
Secure Custom Fields
On behalf of the WordPress security team, I am announcing that we are invoking point 18 of the plugin directory guidelines and are forking Advanced Custom Fields (ACF) into a new plugin, Secure Cus...
Today at 3:26 AM

Source: Sacha Greif on X

The announcement began:

> "On behalf of the WordPress security team, I am announcing that we are invoking point 18 of the plugin directory guidelines and are forking Advanced Custom Fields (ACF) into a new plugin, Secure Custom Fields. SCF has been updated to remove commercial upsells and fix a security problem."

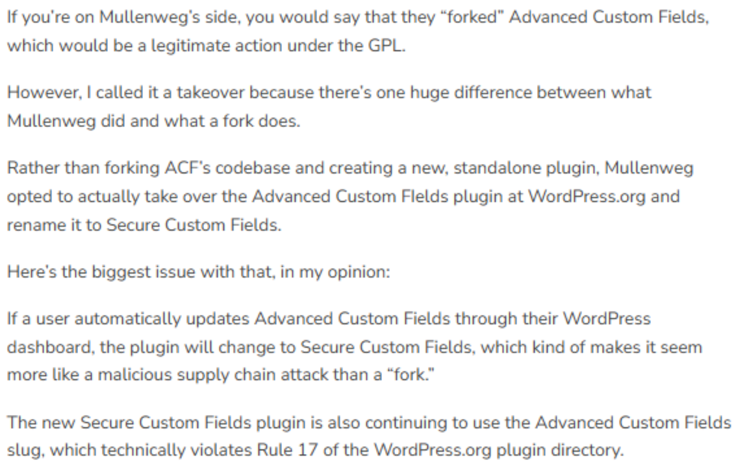
The ACF plugin is the most-installed plugin made by WP Engine, and the 28th most popular WordPress plugin, overall. Automattic claims that the change was a "fork." But this is not true: Automattic did fork the plugin, which they have the right to do, and ***replaced*** the plugin in the plugin directory, and are migrating 2M+ ACF customers *silently* onto this fork – that is now called Secure Custom Fields. In reality, it's hardly "just" a fork:

- URL unchanged: The URL of this project still points to 'advanced-custom-fields'
- Reviews stay in place: All existing reviews remain as if nothing changed. Reviews that point out the heist are being actively removed
- All users silently migrated: more than 2 million customers that installed this plugin over the last decade – thanks to hard work by WP Engine – now belong to the new owner.

- "If you're on Mullenweg's side, you would say that they 'forked' Advanced Custom Fields, which would be a legitimate action under the GPL. However, I called it a

> takeover because there's one huge difference between what Mullenweg did and what a fork does. Rather than forking ACF's codebase and creating a new, standalone plugin, Mullenweg opted to actually take over the Advanced Custom Fields plugin at WordPress.org and rename it to Secure Custom Fields. Here's the biggest issue with that, in my opinion: If a user automatically updates Advanced Custom Fields through their WordPress dashboard, the plugin will change to Secure Custom Fields, which kind of makes it seem more like a malicious supply chain attack than a 'fork.' The new Secure Custom Fields plugin is also continuing to use the Advanced Custom Fields slug, which technically violates Rule 17 of the WordPress.org plugin directory."

Attached hereto as Exhibit N is a true and correct copy of an article on a webpage that I caused to be printed out, located at https://wpshout.com/mullenweg-takes-over-advanced-custom-fields, which is a blog post on a website which is dated October 15, 2024 and titled "Mullenweg and Co. Take Over the Advanced Custom Fields Plugin."



If you're on Mullenweg's side, you would say that they "forked" Advanced Custom Fields, which would be a legitimate action under the GPL.

However, I called it a takeover because there's one huge difference between what Mullenweg did and what a fork does.

Rather than forking ACF's codebase and creating a new, standalone plugin, Mullenweg opted to actually take over the Advanced Custom Fields plugin at WordPress.org and rename it to Secure Custom Fields.

Here's the biggest issue with that, in my opinion:

If a user automatically updates Advanced Custom Fields through their WordPress dashboard, the plugin will change to Secure Custom Fields, which kind of makes it seem more like a malicious supply chain attack than a "fork."

The new Secure Custom Fields plugin is also continuing to use the Advanced Custom Fields slug, which technically violates Rule 17 of the WordPress.org plugin directory.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 4, 2024, in Sofia, Bulgaria.

P. Ramadass

Ramadass Prabhakar

ATTESTATION

I, Rachel Herrick Kassabian, am the ECF user whose ID and password are being used to file the above Declaration. In compliance with Civil L.R. 5-1(i)(3), I hereby attest that Ramadass Prabhakar has concurred in the aforementioned filing.

By */s/ Rachel Herrick Kassabian*
Rachel Herrick Kassabian