

FILED

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

2015 AUG 28 P 12:28

UNITED STATES OF AMERICA, )  
)  
**Plaintiff,** )  
)  
v. )  
)  
ALL ASSETS IN AUSTRALIA AND )  
ELSEWHERE LISTED IN ATTACHMENT )  
A, AND ALL INTEREST, BENEFITS, )  
AND ASSETS TRACEABLE THERETO )  
)  
**Defendants in Rem.** )  
\_\_\_\_\_ )

CLERK US DISTRICT COURT  
ALEXANDRIA, VIRGINIA

Civil Action No.: 1:15-cv-1106.  
LO/MSH

**VERIFIED COMPLAINT FOR FORFEITURE IN REM**

Comes now the Plaintiff, United States of America, through its undersigned attorneys,  
and alleges as follows:

**NATURE OF THE ACTION**

1. The United States brings this action *in rem* seeking the forfeiture of all right, title, and interest in all assets listed in Attachment A, and all property traceable thereto (collectively, the “Defendant Properties”).

2. The United States’ claims arise from a scheme by the “Mega Conspiracy” — an international criminal enterprise run by Kim Dotcom, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, Bram van der Kolk, and business entities Megaupload Limited and Vestor Limited — to engage in criminal copyright infringement on a massive scale and launder the proceeds.

3. As set forth below, the Defendant Properties constitute the proceeds of the conspiracy’s criminal copyright infringement, property used or intended to be used to commit or facilitate the commission of a criminal copyright offense and property involved in the laundering

of such proceeds, and are therefore subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C), and 2323(a)(1).

### **JURISDICTION AND VENUE**

4. This Court has subject matter jurisdiction over actions commenced by the United States under 28 U.S.C. § 1345, and over forfeiture actions under 28 U.S.C. § 1355(a) and (b).

5. This Court has *in rem* jurisdiction over all of the Defendant Properties under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia. Additionally, this Court has *in rem* jurisdiction over certain of the Defendant Properties under 28 U.S.C. § 1355(b)(2) because they are located in foreign countries, or have been detained and seized pursuant to competent authority of foreign governments. This Court also has *in rem* jurisdiction over certain of the Defendant Properties under 28 U.S.C. § 1355(b)(1)(B) because they are located in the Eastern District of Virginia.

6. The location of the defendant properties is as follows:

Moneybookers account: moneybookers@megaupload.com (account #4964059) – restrained in the United Kingdom;

HSBC Bank Australia Limited bank account #11192937118 AUD (Premier account), #094491560087 AUD (Serious Saver account) and #002950681116 all in the name of Mathias Ortmann – restrained in Australia;

PayPal, Inc., account of Megaupload: paypal@megaupload.com ( account #2094224549064053152) – Eastern District of Virginia (seized in the Northern District of California);

PayPal, Inc., account of Sven Echterbach: sven@sectravel.com (account #2060399461350034133); sven@sven.com (account #1499651333470212642); and paypal@sectravel.com (account #1733378795810505763) - Eastern District of Virginia (seized in the Northern District of California);

PayPal, Inc., account of Kim Dotcom: kim@ultimaterally.com -Eastern District of Virginia (seized in the Northern District of California);

PayPal, Inc., account of Bram van der Kolk: [bramos@bramos.nl](mailto:bramos@bramos.nl) - Eastern District of Virginia (seized in the Northern District of California);

\$31,231.67 seized from Citibank, N.A. account number 3200643053 in the name of Megacard, Inc. – Eastern District of Virginia;

\$14,972.57 seized from Citibank, N.A. account number 3200643066 in the name of Megasite, Inc. – Eastern District of Virginia;

60 Servers Purchased from Leaseweb – Eastern District of Virginia (seized in the Netherlands);

The following domain names registered with GoDaddy.com, Inc.: Megaworld.com; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Megaclick.com; Mageclick.com; HDmegaporn.com; Megavkdeo.com – Eastern District of Virginia;

The following domain names registered with Dotregistrar, LLC: Megaupload.com; Megaupload.org; Megarotic.com; Megaclick.com; Megavideo.com; Megavideoclips.com – Eastern District of Virginia;

The following domain name registered with Fabulous.com PTY Ltd.: Megaporn.com – Eastern District of Virginia; and

The following domain name: Megastuff.co – Eastern District of Virginia<sup>1</sup>

7. Venue is proper within this judicial district under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia, and under 28 U.S.C. § 1355(b)(1)(B) and 18 U.S.C. § 981(h) because a criminal

---

<sup>1</sup> The registry for the domain names is as follows:

<u>Registry</u>	<u>Domain Names</u>
.CO Internet S.A.S	megastuff.co; megaclicks.co
Neustar	megaclick.us
Afilias	megaworld.mobi; metastuff.info
PIR	megaclicks.org; metastuff.org; megaupload.org
Verisign	megaclick.com; hdmegaporn.com; megavkdeo.com; megaupload.com; megarotic.com; mageclick.com; megavideo.com; megavideoclips.com; megaporn.com; megaworld.com

prosecution has been brought in this District based on the violations that are the bases for forfeiture, and 18 U.S.C. § 1395(a) because the cause of action accrued in this district and certain of the defendant property is located in this district.

## **FACTUAL ALLEGATIONS**

### **I. Relevant Persons and Entities**

8. Kim Dotcom, who has also been known as “Kim Schmitz” and “Kim Tim Jim Vestor,” is a resident of both Hong Kong and New Zealand, and a dual citizen of Finland and Germany. Dotcom is the founder of Megaupload Limited (“MUL”) and Megamedia Limited (“MMG”). Until on or about August 14, 2011, Dotcom was the Chief Executive Officer for MUL, and was, at the time of the Mega Conspiracy’s takedown on or about January 20, 2012, MUL’s Chief Innovation Officer. As the head of the Mega Conspiracy, Dotcom employed more than 30 people residing in approximately nine countries. From the onset of the Mega Conspiracy through to January 20, 2012, Dotcom supervised the development of the websites and companies utilized in the Mega Conspiracy. Dotcom directed the creation of the network infrastructure behind the Mega Conspiracy websites, negotiated contracts with Internet Service Providers and advertisers, administered the domain names used by the Mega Conspiracy, and exercised ultimate control over all decisions in the Mega Conspiracy. Dotcom has arranged millions of dollars in payments for the computer servers utilized by the MUL and MMG properties around the world, and has also distributed proceeds of the Conspiracy to his co-conspirators. Dotcom is the director and sole shareholder of both Vestor Limited and Kingdom International Ventures Limited, which have been used to hold his ownership interests in MUL– and MMG–related properties; for example, Dotcom owns approximately 68% of Megaupload.com, Megaclick.com, and Megapix.com, and 100% of the registered companies behind Megavideo.com, Megaporn.com, and Megapay.com, through Vestor Limited. Dotcom has personally distributed a

link to a copy of a copyrighted work on, and has received at least one infringing copy of a copyrighted work from, the Mega Sites. Additionally, on numerous occasions, Dotcom received copyright infringement takedown notices from third-party companies submitted pursuant to the Digital Millennium Copyright Act (“DMCA”). These copyright infringement takedown notices identify the copyrighted work that has been infringed, its location, and the owner. In calendar year 2010 alone, Dotcom received more than \$42 million from the Mega Conspiracy.

9. Megaupload Limited was the registered owner of Megaupload.com, the primary website operated by the Mega Conspiracy, and Megaclick.com, a site that offered advertising associated with Mega Conspiracy properties. MUL is a registered company in Hong Kong with a registry number of 0835149. MUL has a number of bank accounts in Hong Kong that have been used to facilitate the operations of the Mega Conspiracy. Dotcom, in addition to holding the title of Chief Executive Officer of MUL until as recently as August 2011, owned, through Vestor Limited, approximately 68% of the shares of MUL; Mathias Ortmann, through Netplus International Limited LLC, owned an additional 25%; Julius Bencko, through Basemax International Limited, owned 2.5%; Bram van der Kolk utilized Mindpoint International Limited LLC to hold 2.5% of the shares of MUL; Sven Echterbach owned approximately 1%; and the remaining 1% was owned by an investor in Hong Kong.

10. Vestor Limited is a registered company in Hong Kong with a registry number of 0994358. Vestor Limited has a DBS Bank account in Hong Kong that has been used to facilitate the operations of the Mega Conspiracy. Dotcom (under the alias Kim Tim Jim Vestor) is the sole director and shareholder of Vestor Limited, and thus is effectively the sole director and 68% owner of MUL, Megaupload.com, Megaclick.com, and Megapix.com. Dotcom is the sole director of, and Vestor Limited is the sole shareholder of, MMG, which is the parent company

and sole shareholder of the following companies: Megavideo Limited (which was the registered owner of Megavideo.com), Megarotic Limited (which was the registered owner of Megaporn.com), and Megapay Limited. Vestor Limited was also the sole owner of Megaworld.com.

11. Finn Batato is both a citizen and resident of Germany. Batato was the Chief Marketing and Sales Officer for Megaupload.com and other Mega Conspiracy properties. Specifically, Batato was in charge of selling advertising space, primarily through Megaclick.com. Batato supervised a team of approximately ten sales people around the world. The purpose of the sales team was to increase the advertising revenue in localized markets by targeting certain advertisements in certain countries. Batato handled advertising customers on the Megaclick.com website and approved advertising campaigns for Megaupload.com, Megavideo.com, and Megaporn.com. Batato personally distributed a link to at least one infringing copy of a copyrighted work to a Mega Site. Additionally, on numerous occasions, Batato received DMCA copyright infringement takedown notices from third-party companies. In calendar year 2010, Batato received more than \$400,000 from the Mega Conspiracy.

12. Julius Bencko is both a citizen and resident of Slovakia. Bencko was the Graphic Director for MUL and MMG. Bencko, as the director and sole shareholder of Basemax International Limited, was effectively a 2.5% shareholder of MUL. From the onset of the Conspiracy through to January 20, 2012, Bencko was the lead graphic designer of the Megaupload.com and other Mega Conspiracy websites. He designed the Megaupload.com logos, the layouts of advertisement space, and the integration of the Flash video player. Bencko requested and received at least one infringing copy of a copyrighted work as part of the

Mega Conspiracy. In calendar year 2010, Bencko received more than \$1 million from the Mega Conspiracy.

13. Sven Echternach is both a citizen and resident of Germany. He was the Head of Business Development for MMG and MUL. Echternach was a 1% shareholder in MUL. He led the Mega Team company, registered in the Philippines, which was tasked with removing illegal or abusive content from the Mega Conspiracy websites. The Mega Team company (the “abuse team”) was instructed not to remove infringing content, but instead to tag it in a manner that it would be more difficult for rightsholders to identify. Additionally, Echternach handled the Mega Conspiracy’s relationships with electronic payment processors, accounting firms, and law firms. His activities included traveling and approaching companies for new business ventures and services. Additionally, on numerous instances, Echternach received DMCA copyright infringement takedown notices from third-party companies. In calendar year 2010, Echternach received more than \$500,000 from the Mega Conspiracy.

14. Mathias Ortmann is a citizen of Germany and a resident of both Germany and Hong Kong. Ortmann was the Chief Technical Officer, co-founder, and a director of MUL. Ortmann, as the director and sole shareholder of Netplus International Limited LLC, effectively owned 25% of the shares of MUL. From the onset of the Conspiracy through to January 20, 2012, Ortmann oversaw software programmers that developed the Mega Conspiracy’s websites, and has handled technical issues with the ISPs. His particular areas of responsibility included setting up new servers, sending and responding to equipment service requests, and problem-solving connectivity problems with the Mega Conspiracy websites. Additionally, on numerous occasions, Ortmann received DMCA copyright infringement takedown notices from other conspirators and third-party companies. Ortmann also had authority to distribute funds from one

of the Conspiracy's main financial accounts. Ortmann received a link to a copy of a copyrighted work associated with the Mega Conspiracy. In calendar year 2010 alone, Ortmann received more than \$9 million from the Mega Conspiracy.

15. Bram van der Kolk, who has also been known as "Bramos," is a resident of both the Netherlands and New Zealand. Van der Kolk is a Dutch citizen. Van der Kolk was the "Programmer-in-Charge" for MUL and MMG. Van der Kolk, as the director and sole shareholder of Mindpoint International Limited LLC, effectively owned 2.5% of the shares of MUL. From the onset of the Conspiracy through to January 20, 2012, Van der Kolk oversaw programming on the Mega Conspiracy websites, as well as the underlying network infrastructure. Van der Kolk was also responsible for responding to DMCA copyright infringement takedown notices sent to Mega Conspiracy sites. Van der Kolk also oversaw the selection of featured videos that were posted onto Megavideo.com, and he was, at times, in charge of the rewards program. Van der Kolk personally uploaded multiple infringing copies of copyrighted works to Internet sites associated with the Mega Conspiracy and has searched servers controlled by the Mega Conspiracy for infringing copies of copyrighted works at the request of other co-conspirators, including several of the members of the Mega Conspiracy. In calendar year 2010, Van der Kolk received more than \$2 million from the Mega Conspiracy.

## **II. Factual Background**

16. On or about January 5, 2012, the United States instituted criminal proceedings against the following individuals and entities when a federal grand jury sitting in Alexandria, Virginia, issued an indictment against them: Kim Dotcom, Megaupload Limited, Vestor Limited, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, and Bram van der Kolk (Criminal Case No. 1:12-cr-3). They were charged based on their



involvement in the Mega Conspiracy, which was a worldwide criminal organization whose members engaged in criminal copyright infringement and money laundering on a massive scale with estimated harm to copyright holders well in excess of \$500 million and reported income in excess of \$175 million. At or about the same time, the United States searched the Mega Conspiracy's servers and domain names, and restrained its assets worldwide. On or about February 16, 2012, the same individuals and entities were charged in a Superseding Indictment with, in addition to the offenses charged in the original Indictment, committing wire fraud. The Superseding Indictment is incorporated herein by reference.

17. Megaupload.com was a commercial website and service operated by the Mega Conspiracy that reproduced and distributed copies of popular copyrighted content over the Internet without authorization. Between at least September 2005 and on or about January 20, 2012, Megaupload.com was used by the members of the Mega Conspiracy to willfully reproduce and distribute many millions of infringing copies of copyrighted works, including motion pictures, television programs, musical recordings, electronic books, images, video games, and other computer software. As Ortmann noted on or about September 5, 2008, if there was "a world ending nuclear war," Megaupload "could serve as a pretty complete archive of the world's intellectual property for a coming generation."

18. On its surface, the operation of Megaupload was relatively simple. Any Internet user who visited the Megaupload.com website could upload a computer file. When a user uploaded a file to Megaupload, the site reproduced the file on at least one computer server it controlled and provided the uploading user with a unique Uniform Resource Locator ("URL") link that allowed anyone with the link to download the file. For example, a link distributed on December 3, 2006 by Dotcom ([www.megaupload.com/?d=BY15XE3V](http://www.megaupload.com/?d=BY15XE3V)) linked to a musical

recording by U.S. recording artist “50 Cent.” Uploaders were incentivized to advertise the link by publishing it on one or more of thousands of “referrer” or “linking” websites—symbiotic websites that profited financially by helping users find pirated content on Megaupload, and sometimes other pirate websites.

19. A single click on a Megaupload link accessed a Megaupload.com download page that allowed any Internet user to download a copy of the file from a computer server that was controlled by the Mega Conspiracy. Millions of internet users seeking to view or download pirated content would visit these “referrer” or “linking” websites, and would click on the links to download the infringing content.

**A. The Mega Sites Were Purposefully Designed To Encourage Wide-Scale Copyright Infringement**

20. The members of the Mega Conspiracy described themselves as “modern day pirates” and virtually every aspect of the Mega Sites was carefully designed to encourage and facilitate wide-scale copyright infringement. As an initial matter, users were encouraged to upload infringing content by Megaupload’s “Uploader Rewards” program, pursuant to which uploaders were paid significant amounts depending upon the popularity of their uploads. Megaupload users who uploaded popular infringing content, such as pre-release or newly released movies, were paid thousands of dollars by the Mega Conspiracy. In total, the Mega Conspiracy directly paid uploaders millions of dollars through online payments. Some of the biggest repeat infringers were paid \$50,000 or more by the Mega Conspiracy.

21. Once a user uploaded a video file to Megavideo.com, software written by the Mega Conspiracy converted the video to a format known as Flash Video or “FLV,” which allowed for quicker and broader distribution of files because Flash videos could be streamed through most internet browsers with a high level of compression at fast download speeds.

22. The Mega Conspiracy also developed technology to allow users to stream “High Definition” (“HD”) videos. On or about May 25, 2009, NOMM noted that “[e]ven though we have lots of HD content uploaded most seems to be problematic quality or legality wise.” The HD content was “problematic” legality wise because the vast majority of it was commercial motion pictures or television shows. On or about March 3, 2009, as the conspiracy was developing their HD technology, Ortmann pondered, in a Skype conversation with Van der Kolk, “what warner bros. will say when they see crystal clear BD rips [infringing copies of Blu-ray Discs] instead of the usual blurry video?” Van der Kolk responded, “yeah will be even more pissed off :)” and he later noted, “Hollywood will curse us :)”.

23. The Mega Conspiracy also developed software to identify the most popular files on the Mega Sites and reproduce them onto Mega’s faster servers, which were those operated by Cogent Communications in Washington, D.C. An analysis of the 2,444 files on the Cogent servers showed that between 90 and 100% of the files stored on those servers were infringing. These faster servers thus facilitated the mass distribution of popular copyright-infringing works. The members of the Mega Conspiracy recognized the significance of the Cogent servers in Mega’s architecture. On August 16, 2010, Ortmann wrote to Dotcom that, “if a US-court prohibits Cogent from providing us service, we will soon lose the vast majority of our connectivity worldwide.”

24. At times, the Mega Conspiracy also limited how long non-subscription users could watch videos, in an effort to convert these users to paid subscribers. As Ortmann explained to Dotcom on or about November 23, 2008, “[m]ovies last 90 minutes” but are “most interesting in the last 20 minutes” because “movies heighten the suspense towards the end.” The Mega Conspiracy capitalized on this “sweet-spot,” as Ortmann described it, by interrupting user’s

viewing experience approximately 72 minutes into the movie. If users wanted to continue watching the movie, they were required to obtain premium membership. This technique, of course, could have only been effective if consumers were using the Mega Sites to view commercial length movies with the standard Hollywood “sweet-spot,” that is infringing movies.

25. Recognizing that their scheme was unlawful, members of the Mega Conspiracy discussed ways to restructure their infrastructure to make themselves “untouchable” by law enforcement. For example, on or about August 16, 2010, Dotcom told Ortmann via Skype, “at some point a judge will be convinced about how evil we are and then we’re in trouble. We have to make ourselves invulnerable.” To prevent this possibility, Dotcom suggested “a new hosting model” that would make Megaupload “independent from,” its server hosting facilities, “Capathia or leaseweb.” Dotcom said that Megaupload “should set up a fleet of our own servers with multiple hosters (15 or more in several countries) and make us untouchable.” Dotcom reminded Ortmann, “you should not log our chats ;-) too much shit in there.” Ortmann responded, “unfortunately Skype autologs them . . . I’m going to erase them all.”

**B. The Mega Conspiracy Purposefully Misled Copyright Holders**

26. Throughout the conspiracy, members of the conspiracy regularly told copyright holders and their representatives that they would remove infringing content that the holders and their representatives had identified on Mega Conspiracy-controlled servers, when members of the Mega Conspiracy knew they would not. In particular, they deliberately misrepresented to copyright holders that they had removed copyright infringing content from their servers, while, in fact, they only removed Mega Conspiracy-created links to the content file (which could still be illegally downloaded through numerous redundant links). For instance, in response to takedown requests, Warner Brothers, one of the rightsholders, was repeatedly sent automated messages, falsely representing that a certain number of “file[s]” and “video[s]” were “removed” from the

system (e.g., “6 files and 6 videos removed from our system”). In fact, only particular links to these infringing files and videos had been removed. Despite receiving many millions of requests to remove infringing copies of copyrighted works, the conspirators, at best, only deleted the particular URL of which the copyright holder complained, and purposefully left the actual infringing copy of the copyrighted work on the Mega Conspiracy-controlled server, allowing access to the infringing work to continue.

27. Furthermore, the members of the Mega Conspiracy either completely ignored, or purposefully delayed, their response to takedown requests from rightsholders that the conspirators believed were unlikely to pose a serious litigation risk. On April 23, 2009, Dotcom reminded the other conspirators not to respond to takedown notices from “insignificant sources” because complying with these takedown notices would result in a loss of “significant revenue” to the Mega Conspiracy. To Dotcom, “insignificant sources” apparently included sources originating from any country other than “the USA, France, Germany, UK and SPAIN.” At other times, including on or about April 24, 2009, Dotcom’s list of “significant sources” seemed to be limited only to “major organization[s] in the US.”

28. The members of the Mega Conspiracy also regularly told complaining rights holders and their representatives that the conspirators had deleted or blocked the user accounts of known and repeat copyright infringing users, when they had not. To the contrary, the conspirators knew many of the biggest repeat offenders by name, reviewed the content they uploaded before paying them, regularly praised their work, and then knowingly paid them thousands of dollars in exchange for their infringing uploads. For instance, the conspirators received 1,200 takedown requests based on URL links to the infringing content of one repeat infringer, identified here as TH. TH was important to the Mega Conspiracy because those links generated 1.2 million

downloads of copyright infringing files hosted on the Mega Sites. Therefore, despite the 1,200 takedown notices, the conspirators paid TH 26 separate reward payments for a total of more than \$50,000, exempted TH from Megaupload's storage size limitations to accommodate his 30,000 files (almost 2.5 terabytes) and repeatedly discussed and praised TH in emails. For example, on or about June 17, 2007, Ortmann told Van der Kolk that TH "is one of our most important uploaders... I don't regret any of the dollars we send him every month."

29. The members of the Mega Conspiracy also claimed to have a rigorous auditing team to prevent distribution of infringing content. In fact, auditing guidelines Van der Kolk emailed to an employee in 2007 made clear that, although auditors were to remove certain content (e.g., pornography, "real killing," and "torture"), auditors were not to remove infringing content. As Ortmann wrote Van der Kolk, "the important thing is that nobody must know that we have auditors letting this stuff through" because DMCA protection "would go away."

**C. The Mega Conspiracy Engaged In Extensive Efforts to Conceal Copyright Infringement**

30. The members of the Mega Conspiracy disguised the Mega Sites as "innocent" electronic storage lockers, purportedly existing to allow users to store electronic files on the cloud. As Ortmann told Van der Kolk on or about March 5, 2009, "now we're doing exactly what I foresaw in the beginning—innocent front end, private back end :)". Van der Kolk clearly agreed with this approach, telling Ortmann on or about October 10, 2009, "it's good to stay off the radar by making the front end look like crap while all the piracy is going through direct links" from referrer sites. In fact, when Ortmann described the Mega Conspiracy as "just a service provider" on or about January 4, 2008, Van der Kolk responded, "yeah legally, but we know better :)". In the same conversation, Van der Kolk made clear he was well aware that "we are the pirates here."

31. The members of the Mega Conspiracy went through great lengths to disguise the true function of the Mega Sites. For example, despite the fact that the conspirators, themselves, had the ability to, and did, search for particular files on Megaupload by file name, file type, file size, etc., they purposefully made it so the public could not search for content on sites. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relied on thousands of third party “linking” sites, which contained user-generated postings of links created by Megaupload.com (as well as those created by other Mega Sites, including Megavideo.com and Megaporn.com). This made it more difficult for rights owners to detect infringement, and gave the conspirators plausible deniability. As Ortmann wrote Van der Kolk on August 30, 2007, “searchability is dangerous and will kill us.” Four years later, nothing had changed. On October 24, 2011, Batato pointed out that “mak[ing] the content searchable . . . would basically mean that we can shut down Mega ;-).”

32. Similarly, the Megaupload website prominently featured a “Top 100 files” list of the files that were purportedly the most frequently downloaded files on Megaupload. In 2008, Van der Kolk explained that the “Top 100” list was an effort to make the “whole site look much more legitimate & attractive as well.” An accurate “Top 100 files” list, however, would include practically nothing but copyright infringing content. Thus, the conspirators carefully curated this list, to make sure it did not actually reflect any of the “Top 100 files,” but instead reflected a rotating list of non-infringing “harmless stuff.”

33. Unlike the Megaupload site, the Megavideo site did purport to allow users to search for video files or to browse for video files by categories such as “Entertainment,” “Comedy,” “Music,” or “Video Games.” The members of the Mega Conspiracy, however, wrote software to automatically mark all videos longer than 10 minutes (*i.e.*, all commercial movies

and television shows) as “private” to ensure that they would not be searchable or publically displayed on the front pages of Megavideo. These “private” videos could only be located through the referrer sites. The exclusion of infringing content from the Megavideo’s search engine, however, meant that the conspirators had to find non-infringing content to display publically on Megavideo. This was a significant challenge because, as Van der Kolk reminded Ortmann in 2009, “almost no harmless [i.e., non-infringing] stuff is being uploaded” to Megavideo.

34. To solve that problem, and to make Megavideo appear legitimate, the members of the Mega Conspiracy developed software to secretly copy all of the videos on YouTube to Megavideo, without the permission of YouTube or the owners of the videos. On or about October 4, 2007, Dotcom told Van der Kolk, “the day has 1440 minutes and I want to see one [YouTube] Video upload [to Megavideo] every minute.” On or about April 18, 2009, Van der Kolk explained to Ortmann that “uploading new legit videos” from YouTube “continuously” would “make the [Megavideo] site appear more legit.” Van der Kolk added that “Megavideo has quite a piracy image already.”

35. In addition, the members of the Mega Conspiracy made the conscious decision to conceal the user names of uploaders to frustrate rightsholders. On or about January 16, 2009, Van der Kolk wrote Ortmann that “for copyright issues etc.” the conspirators “should not disclose [Megaupload] usernames anywhere.” On March 13, 2009, Van der Kolk later elaborated to Ortmann that disclosing user names would “not [be] good for repeat infringement offenders.” Similarly, the conspirators also decided not to disclose how many times each file had been viewed or downloaded. As Ortmann explained to Van der Kolk on or about August 30, 2007, “as we’re displaying viewcounts, the copyright industry could be tempted to send us lost revenues based on that.” Van der Kolk responded, “that will hurt.”



36. The members of the Mega Conspiracy also made a conscious effort, in the words of Dotcom, to “stay below the radar.” When a reporter from Forbes.com asked about “Kim Schmitz” and “Tim Vestor’s” (*i.e.*, Dotcom’s) role in the company, Dotcom falsely wrote, “I can confirm that nobody by the name of Kim Schmitz is associated with our company.” Dotcom further dissembled to the reporter, telling him that “[w]e have a policy not to disclose details about our business performance. But I can tell you (off the record) that we are a small and humble business trying to earn enough to pay the bandwidth bill. Our site has grown to be popular but it is not easy to monetize the traffic in this economy.” Continuing the deceit, Dotcom added that “[t]he vast majority of users is uploading home videos, web earn captures, content they own or have the right to copy and other legitimate content.”

**D. The Mega Conspiracy Stashed Away Millions of Dollars In Criminal Proceeds**

37. The Mega Conspiracy obtained the vast majority of their criminal proceeds by selling “premium subscriptions.” Premium subscriptions for Megaupload.com were, at times, available for online purchase for as little as a few dollars per day, or as much as approximately \$260 for a lifetime. Subscription fees collected during the existence of the Mega Conspiracy from premium users totaled more than \$150 million.

38. Users would pay for premium subscriptions so that they could: (a) get paid for uploading and advertising popular (*i.e.*, infringing) content pursuant to Megaupload’s “uploaders rewards” program; (b) decrease wait and download times, which could be at least an hour for popular content (and, at times, unpaid users were ineligible to download files over a certain size); (c) upload and download files with few, if any, limitations; and (d) watch movie-length infringing videos without interruptions.

39. While it was theoretically possible for “legit [*i.e.*, non-infringing] users” to purchase premium subscriptions, there was little reason for such users, if they existed, to do so. Van der Kolk told Ortmann on March 8, 2009 that “legit users” were not a source of revenue to the Mega Conspiracy, stating “that’s not what we make \$ with :)”. Consistently, on October 7, 2007, Van der Kolk told Ortmann that if the Mega Conspiracy automatically deleted videos that were likely to contain infringing content (*i.e.*, videos that were longer than 30 minutes and had a significant number views) they would end up deleting “99.999%” of all the content on Megavideo. Similarly, on January 25, 2008, Van der Kolk told Ortmann that “more than 90%” of the Mega Conspiracy’s “profit” was specifically derived from “infringing files.” On November 21, 2009, Ortmann told Van der Kolk that Megavideo’s public [*i.e.*, non-infringing] videos “could not possibly have generated any significant payments.” Thus, the members of the Mega Conspiracy were fully aware that users purchased “premium subscriptions” to engage in copyright infringement.

40. To purchase “premium subscriptions,” users primarily made payments through PayPal.com, a U.S.-based global e-commerce business allowing payments and money transfers over the Internet. The Mega Conspiracy’s PayPal, Inc. account was utilized to receive payments from the Eastern District of Virginia and elsewhere for premium Megaupload.com subscriptions. The same PayPal, Inc. account was used by the Conspiracy to pay Carpathia Hosting in the Eastern District of Virginia and Leaseweb in the Netherlands as well as other operating expenses (including, but not limited to, direct financial rewards to uploaders of popular content in the Eastern District of Virginia and elsewhere).

41. In order to do business through PayPal, the members of the Mega Conspiracy repeatedly deceived their payment processor. Between just 2010 and 2011, PayPal sent

Megaupload more than 145 takedown notices referencing more than 3,400 infringing links. The copyrighted materials associated with these links had been downloaded more than 799,000 times. Ortmann repeatedly responded directly to PayPal, assuring PayPal that the infringing files had been removed or deleted, and 220 of the approximately 330 registered users who uploaded the files had been blocked from using the Mega Sites. For example, on or about September 17, 2011, Ortmann wrote PayPal that “[a]ll infringing uploads have been deleted and their uploader blocked.” In fact, none of the infringing files were ever deleted, and as of January 19, 2012, only approximately 18 of the 220 registered users had been blocked from using the Mega Sites for any reason.

42. The members of the Mega Conspiracy were aware that no legitimate payment processor would have worked with the Mega Conspiracy if it were aware that the Mega Conspiracy was basically ignoring their takedown requests. In fact, in 2011, Dotcom emailed PayPal to advise them “not to work with sites that are known to pay uploaders for pirated content” because these sites “pay everyone (no matter if the files are pirated or not) and have NO repeat infringer policy.” Until August 2011, however, the Mega Sites routinely paid repeat infringers for uploading pirated content.

### **III. THE DEFENDANT ACCOUNTS, SERVERS AND DOMAIN NAMES**

43. DBS BANK (HONG KONG) LIMITED ACCOUNT NUMBER 7881380320 held in the name of Megaupload Limited (the “DBS 0320 account”): On or about January 20, 2012, Hong Kong authorities, pursuant to a Mutual Legal Assistance Treaty (MLAT)

request by the United States Government, froze the assets on deposit in the DBS 0320 account.

As of that date, the balance in that account was HKD 36,880,460.<sup>2</sup>

44. The DBS 0320 account was a funnel account that received proceeds of the copyright infringements and then transferred those proceeds to various accounts in Hong Kong, New Zealand, Australia, the United Kingdom and elsewhere. The account was equipped to manage transactions in five different currencies (Hong Kong Dollars, U.S. Dollars, Euros, British Pound, and Japanese Yen).

45. Records indicate that from August 2007 through January 2012 there were 1,403 deposits into the DBS 0320 account totaling HKD 1,260,508,432.01 from the **PayPal, Inc., account of Megaupload (paypal@megaupload.com)** (the “PayPal account”). These funds represent proceeds of crime and property involved in money laundering as more fully set out herein.

46. Megaupload also used Moneybookers<sup>3</sup> to accept payment from various individuals for access to the Megaupload website. Records indicate that Moneybookers transferred USD \$280,000 and EUR 3,980,311 to the DBS 0320 account.

47. **Moneybookers account belonging to Megaupload and accessed by moneybookers@megaupload.com:** A total of EUR 3,980,311.00 was transferred from the Moneybookers Ltd., account to the DBS 0320 account between June 11, 2008, and July 28, 2011. A total of \$280,000.00 was transferred from the Moneybookers Ltd., account to the DBS 0320 account between June 12, 2008 and November 5, 2010.

---

<sup>2</sup> This account was forfeited by the United States pursuant to this Court’s order of April 7, 2015 (Dkt. #108) in case number 1:14cv969.

<sup>3</sup> Moneybookers is very similar to PayPal and allows entities and individuals to transfer money, much in the same way that PayPal operates.

48. **HSBC Bank Australia Limited (formerly Hongkongbank of Australia Limited) bank account numbers 11192937118 AUD (Premier account), 094491560087 AUD (Serious Saver account) and 002950681116 all in the name of Mathias Ortmann:** these three accounts were funded by transfers from HSBC (Hong Kong) account #813010204833, which account was funded by transfers from the DBS 0320 account in the amount of HK \$109,064,765.00 between February 10, 2009 and April 4, 2011. Between November 8, 2010, and December 7, 2011, AUD \$1,633,000.00 was transferred from the 4833 account to the 7118 account. Between November 8, 2010 and September 3, 2011, AUD \$1,033,000.00 was transferred from the 4833 account to the 1116 account. Between March 30, 2011, and June 7, 2011, AUD \$750,000.00 was transferred from the 4833 account to the 0087 account.

49. **PayPal, Inc., Account of Sven Echternach (sven@sectravel.com, paypal@sectravel.com, and sven@sven.com):** Between September 6, 2005, and October 31, 2008, EUR 53,996.00 and \$125,098.00 were transferred from Megaupload's PayPal account to Sven Echternach's PayPal account. Between April 6, 2005, and April 15, 2005, \$2,500 was transferred from Kimvestor Ltd.'s PayPal account to Sven Echternach's PayPal account.

50. **PayPal, Inc., Account of Kim Dotcom (kim@ultimaterally.com):** Between August 15, 2005, and April 24, 2009, a total of \$113,884.73 and EUR 8,000.00 were transferred from Megaupload's PayPal account to Dotcom's PayPal account.

51. **PayPal, Inc., Account of Bram van der Kolk (bramos@bramos.nl):** On July 14, 2005, EUR 2,200.00 was transferred from Megaupload's PayPal account to Bram van der Kolk's PayPal account. Between July 14, 2005, and November 13, 2007, \$12,600.00 was transferred from Megaupload's PayPal account to Bram van der Kolk's PayPal account.

Between January 18, 2008, and February 19, 2009, an additional \$150.00 was transferred to Bram van der Kolk's PayPal account from the Kimvestor Ltd PayPal account.

52. **60 Servers Purchased from Leaseweb:** Payments consisting of 45 Eurodollar transfers of EUR 8,000 each and one for EUR 113 (a total of EUR360,113) to purchase 60 servers were made from the Megaupload PayPal account on October 27, 2011. In addition, these servers are property used or intended to be used in any manner or part to commit or facilitate the commission of the copyright infringement scheme described herein.

53. **Citibank, N.A. account number 3200643053 in the name of Megacard, Inc.:** On January 11, 2008, Citibank account 3200643053 received a \$15,000 wire transfer from the DBS 0320 account. On April 27, 2009, a \$12,000 wire transfer was received from the DBS 0320 account. On January 7, 2010, another \$15,000 wire transfer was received from the DBS 0320 account. On January 19, 2012, \$31,231.67 was seized from this account pursuant to a federal seizure warrant issued from this district.

54. **Citibank, N.A. account number 3200643066 in the name of Megasite, Inc.:** On January 11, 2008, Citibank account 3200643066 received a \$15,000 wire transfer from the DBS 0320 account. On January 19, 2012, \$14,972.57 was seized from this account pursuant to a federal seizure warrant issued from this district.

55. The following domain names: **Megastuff.co; Megaworld.com; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Megaclick.com; HDmegaporn.com; Megavkdeo.com; Megaupload.com; Megaupload.org; Megarotic.com; Mageclick.com; Megavideo.com; Megavideoclips.com; Megaporn.com:** are property used or intended to be used in any manner or part to commit or facilitate the commission of the copyright infringement scheme described herein.

**FIRST CLAIM FOR RELIEF**  
**(Forfeiture under 18 U.S.C. §§ 981(a)(1)(C) and 2323(a)(1)(C))**

56. The United States incorporates by reference paragraphs 1 through 55 above as if fully set forth herein.

57. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting ‘specified unlawful activity’ (as defined in section 1956(c)(7) of this title) or a conspiracy to commit such an offense.”

58. Title 18, United States Code, Section 1956(c)(7)(D) provides that the term “specified unlawful activity” includes “an offense under . . . section 2319 (relating to copyright infringement).”

59. Title 18, United States Code, Section 2319 sets forth the penalties for willful infringement of a copyright in violation of 17 U.S.C. § 506(a).

60. Title 17, United States Code, Section 506(a) prohibits a person from willfully infringing a copyright (1) for commercial advantage or private financial gain; (2) by reproducing or distributing, including by electronic means, infringing copies of works with a total retail value of over \$1,000 over a 180-day period; or (3) by distributing a “work being prepared for commercial distribution” by making it available on a publicly accessible computer network, if the person knew or should have known that the work was intended for commercial distribution.

61. Title 18, United States Code, Section 2323(a)(1)(B) and (C) likewise subjects to forfeiture “[a]ny property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense” under 17 U.S.C. § 506 or 18 U.S.C. § 2319, as well as “[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of” such an offense.

62. As set forth above and as incorporated in the Superseding Indictment, the Mega Conspiracy wilfully infringed and conspired to wilfully infringe copyrighted works when, for purposes of commercial advantage and private financial gain, it took numerous copyrighted works, including works it knew were being prepared for commercial distribution, and made them available on a publicly accessible computer network.

63. As set forth above, the Defendant Properties constitute criminal proceeds that the Mega Conspiracy generated through its criminally infringing acts in violation of 17 U.S.C. § 506 and 18 U.S.C. § 2319, and/or property used or intended to be used to facilitate those offenses.

64. As such, the Defendant Properties are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 2323(a)(1)(B) and (C).

**SECOND CLAIM FOR RELIEF**  
**(Forfeiture under 18 U.S.C. § 981(a)(1)(A))**

65. The United States incorporates by reference paragraphs 1 through 55 above as if fully set forth herein.

66. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 [or] 1957 . . . of this title, or any property traceable to such property.”

67. Title 18, United States Code, Section 1956(a)(1) imposes a criminal penalty on any person who:

knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A) (i) with the intent to promote the carrying on of specified unlawful activity; or

\*\*\*



(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

68. Title 18, United States Code, Section 1956(a)(2) further imposes a criminal penalty on any person who:

transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—

(A) with the intent to promote the carrying on of specified unlawful activity; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

69. Title 18, United States Code, Section 1957 imposes a criminal penalty on any person who “knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity.” A “monetary transaction” includes the “deposit, withdrawal, transfer or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument . . . by, through, or to a financial institution.” 18 U.S.C. § 1957(f)(1).

70. Title 18, United States Code, Section 1956(h) imposes a criminal penalty on any person who conspires to commit any offense defined in 18 U.S.C. §§ 1956 or 1957.

71. As noted above, "specified unlawful activity" includes criminal copyright infringement.

72. As set forth above, the Defendant Properties constitute property involved in money laundering transactions and attempted money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957, and are therefore subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

**PRAYER FOR RELIEF**

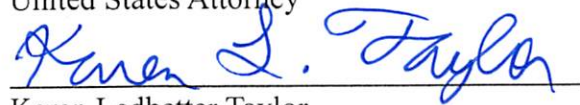
WHEREFORE, Plaintiff requests that judgment be entered in its favor against the Defendant Properties; that pursuant to law, notice be provided to all interested parties to appear and show cause why the forfeiture should not be decreed; that the Defendant Properties be forfeited to the United States of America and delivered into its custody for disposition according to law; that Plaintiff be awarded its costs and disbursements in this action; and for such and further relief as this Court may deem just and proper.

Dated: August 28, 2015

Respectfully submitted,

Dana J. Boente  
United States Attorney


By:



Karen Ledbetter Taylor  
Assistant United States Attorney  
Attorney for the United States of America  
United States Attorney's Building  
Justin W. Williams U.S. Attorney's Building  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Phone: 703-299-3700  
Fax: 703-299-3982  
Email Address: Karen.taylor2@usdoj.gov

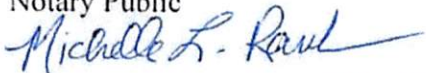
VERIFICATION

Before me, the undersigned authority, on this date personally appeared FBI Special Agent Rodney Hays, who after being duly sworn, states that he makes this verification for and on behalf of the Plaintiff, United States of America, that he has read the foregoing complaint and knows the contents thereof, that his information and knowledge about its contents was obtained by him in the course of his investigation and that of other law enforcement officers and government agents, and that the matter and things set forth in the complaint are true to the best of his knowledge, information and belief.

  
\_\_\_\_\_  
Rodney Hays  
Special Agent  
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me  
this 25 day of August 2015

Notary Public



My commission expires: 9/30/15  
Alexandria, Virginia

