KILPATRICK TOWNSEND & STOCKTON LLP
JAMES G. GILLILAND, JR. (State Bar No. 107988)
TIMOTHY R. CAHN (State Bar No. 162136)
MEHRNAZ BOROUMAND SMITH (State Bar No. 197271)
HOLLY GAUDREAU (State Bar No. 209114)
RYAN BRICKER (State Bar No. 269100)
Two Embarcadero Center, 8th Floor
San Francisco, California 94111
Telephone: (415) 576-0200
Facsimile: (415) 576-0300
Email: jgilliland@kilpatricktownsend.com
tcahn@kilpatricktownsend.com
mboroumand@kilpatricktownsend.com
hgaudreau@kilpatricktownsend.com
rbricker@kilpatricktownsend.com

Attorneys for Plaintiff
SONY COMPUTER ENTERTAINMENT AMERICA LLC

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SONY COMPUTER ENTERTAINMENT AMERICA LLC, a Delaware limited liability company,

Plaintiff,

v.

GEORGE HOTZ; HECTOR MARTIN CANTERO; SVEN PETER; and DOES 1 through 100,

Defendants.

Case No._____

PLAINTIFF'S *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER, ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION, AND ORDER OF IMPOUNDMENT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

Date: January 12, 2011
Time: 9:00 a.m., or as soon as can be heard
Courtroom: 3, 17th Floor
Judge: Hon. Richard Seeborg

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

I. INTRODUCTION

Defendants George Hotz, "Bushing," Hector Cantero, Sven Peter and "Segher" (collectively, "Defendants") are computer hackers.[1] Working individually and in concert with one another, Defendants recently bypassed effective technological protection measures ("TPMs") employed by plaintiff Sony Computer Entertainment America LLP ("SCEA") in its proprietary PlayStation®3 computer entertainment system ("PS3 System"). Through the Internet, Defendants are distributing software, tools and instructions (collectively, "Circumvention Devices") that circumvent the TPMs in the PS3 System and facilitate the counterfeiting of video games. Already, pirated video games are being packaged and distributed with these circumvention devices. Declaration of Ryan T. Bricker In Support of *Ex Parte* Motion for Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction; Order for Impoundment ("Bricker Decl.") ¶2, Exh. A. Pursuant to Federal Rule of Civil Procedure 65 and Local Rules 65-1 and 7-10, SCEA moves *ex parte* to put an immediate halt to the ongoing distribution of these illegal Circumvention Devices and avoid irreparable harm to SCEA and to other video game software developers stemming from video game piracy.

Defendants' Circumvention Devices allow users to circumvent multiple TPMs in the PS3 System – including access control, encryption and digital signature protections – to enable use or playing of illegal copies of PlayStation®3 video games on the PS3 System.

---

[1] Defendant Hotz, against whom this motion initially is being brought, has established considerable contacts with the District in connection with his unlawful conduct. Upon information and belief, Defendant George Hotz is bound by the "Playstation Network Terms of Service and User Agreement" (the "PSN User Agreement"), ¶14 of which states in relevant part that "both parties submit to personal jurisdiction in California and further agree that any dispute arising from or relating to this Agreement shall be brought in a court within San Mateo County, California." Further, upon information and believe, in connection with his unlawful conduct, Hotz has utilized an account via PayPal, a company located in San Jose, California, and therefore derives a financial benefit through his unlawful conduct in this district. Bricker Decl. at ¶31, Exh. DD. Mr. Hotz is also unlawfully demonstrating and distributing a circumvention device or component thereof through YouTube, a widely used and interactive website located in Mountain View, California. *Id.* ¶25, Exh. W. Mr. Hotz has also discussed his unlawful conduct through Twitter, a widely used and interactive website located in San Francisco, California.

These Circumvention Devices violate federal copyright law, including the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 *et seq*. This Court previously has recognized the illegality of similar devices and enjoined their sale and distribution. *See, e.g., Sony Computer Entertainment America v. Zoomba et al.*, 2010 U.S. Dist. Lexis 113228, 2010 WL 4512835 (N.D. Cal. October 13, 2010); *Sony Computer Entertainment America v. Divineo, Inc.*, 457 F. Supp. 2d 957 (N.D. Cal. 2006). Defendants' intentional hacking of the PS3 System without authorization, and their obtaining and transmission of SCEA's proprietary information (including but not limited to digital signature keys) also violates the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.* If Defendants are not immediately enjoined from accessing the PS3 System, circumventing its TPMs and trafficking in illegal Circumvention Devices, Defendants will continue to do so, thereby facilitating and proliferating the unlawful copying of PlayStation3 games and causing immediate and irreparable harm to SCEA and others.

Indeed, the Defendants' enabling of software piracy through their activities over the last several days has been widely reported. Yesterday, for example, an article trumpeted that "PS3 Software Piracy Begins as First Game is Played on an Unmodded Playstation 3." Bricker Decl. at ¶2, Exh. A. The article proceeds to explain:

> That didn't take long, did it? The rootkey crack that was uncovered by Geohot [i.e., Defendant George Hotz] and other modders has ***the door wide open for rampant PlayStation 3 piracy***, and the first pirated game on an unmodded PS3 has been done.

See also, Bricker Decl. at ¶30, Exh. CC. This motion seeks to close the door for rampant piracy that Defendants have illegally pried open in violation of federal and California law.

Though SCEA need only show "likely" success to obtain a Temporary Restraining Order ("TRO"), SCEA's evidence demonstrates a compelling case of DMCA violations and computer fraud and abuse warranting preliminary relief and an order for impoundment. Accordingly, SCEA respectfully requests that the Court issue: (1) a TRO immediately barring Defendant Hotz from (a) circumventing the TPMs in the PS3 System; (b) offering to the public, marketing, distributing, or trafficking in the Circumvention Devices; and (c) accessing

SCEA's protected PS3 System, obtaining and transmitting SCEA's proprietary information or code, and impairing the confidentiality of information obtained from the PS3 System until a preliminary injunction can be issued; (2) an Order for Impoundment; and (3) an Order to Show Cause why a preliminary injunction should not issue enjoining Defendants from continued circumvention, distribution of the Circumvention Devices and accessing and transmitting SCEA's proprietary information.

II. BACKGROUND

A. SCEA's PlayStation®3 Computer Entertainment System And Its Technological Protection Measures

SCEA markets and sells the PS3 System, a computer entertainment system featuring hardware and firmware designed for the playing of video games. Declaration of Riley R. Russell In Support of *Ex Parte* Motion for Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction; Order for Impoundment ("Russell Decl."), ¶3, Exh. A. The PS3 System is a highly sophisticated apparatus that usually connects to a television or monitor for use in playing video game software simulating three-dimensional action. *Id.* The PS3 System also features PlayStation Network ("PSN"), an entertainment network that supports multiplayer online gameplay, access to the PlayStation Store to purchase video games as well as rent or buy feature films and PS3 System connectivity. *Id*.

The PS3 System has enjoyed wide success throughout the United States and the world. Over 41 million PS3 Systems have been sold worldwide since the product release in November 2006. Russell Decl. at ¶4. There are hundreds of different video game titles currently available for the PS3 System in the United States, which typically sell for retail prices between $40.00 and $70.00. *Id.*

All genuine PS3 Systems are manufactured with technological protection measures that effectively control access to the PS3 System and prevent unlicensed or copied software from playing on the PS3 System. *See* Declaration of Bret Mogilefsky In Support of *Ex Parte* Motion for Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction; Order for Impoundment ("Mogilefsky Decl."), ¶4. The PS3 System is designed to

run multiple levels of authorized, encrypted code in one or more sequences. *Id.* at ¶5. Each level features TPMs, which control access, encrypt and decrypt code, and authenticate signatures to enable access to the files within the code. *Id.*

One purpose of the PS3 System's TPMs is to prevent users from playing illegally copied, pirated games. *Id*. at ¶14. To that end, every file authorized to run on the PS3 System contains an authentic digital signature. *Id.* at ¶9. SCEA generates each digital signature using a pair of electronic keys ("Keys"). *Id.* at ¶10. The PS3 System verifies each signature using one of those Keys, which is encrypted and embedded in the system. *Id.* The other Key is held by SCEA; it is not distributed and cannot be located anywhere in the PS3 System's code or hardware, or the code of any authorized video game. *Id*. The PS3 System will not execute a file unless that file contains an authentic digital signature. *Id.* Unauthorized or unlicensed video game discs (such as those burned from genuine game discs) do not have an authorized signature code. *Id.* at ¶11. Accordingly, a normally-functioning PS3 System will not run those pirated video games.

The PS3 System also utilizes access control and encryption TPMs. *Id*. at ¶8. Those TPMs prevent, restrict or otherwise limit access to certain sections of the PS3 System software and hardware. *Id*. at ¶5. As a result, the TPMs ensure that the PS3 System functions in a safe and reliable manner. *Id*. at ¶13. They also protect the encrypted firmware, encrypted digital signature Keys and other encrypted Keys that are stored within the PS3 System. *Id*. at ¶10. Because the PS3 System and its code are protected by these TPMs, users can neither access nor read the signatures or the Keys, and therefore cannot use those elements to gain access to the System to run a pirated video game. *Id.* at ¶13.

Using the types of TPMs discussed above, the PS3 System allows only the operation of legitimate, authorized and approved software that is licensed for distribution in the region or geographical territory of the console's sale. *Id*. at ¶6. By taking these precautions, SCEA has been able to protect its exclusive rights to copy, sell, distribute and manufacture video games. In addition, SCEA has been able to protect its substantial investment – and the investment of third-party videogame companies – in the development, creation, and

distribution of the PS3 System and compatible video games.

B. SCEA's Copyrights And Copyright Licenses

SCEA develops and publishes its own interactive entertainment software video games for the PS3 System. Russell Decl. at ¶6. *Id.* SCEA has invested and continues to invest substantial time, effort and expense in the design, development, testing, manufacturing and marketing of its video games. *Id.* at ¶4. Those games are highly creative and SCEA has obtained copyright registrations to protect them. *Id.* at ¶7. For example, SCEA owns valid copyright registration for the following video game software: *Ratchet & Clank Future: Tools of Destruction* (Copyright No. PA 1-616-055); *Resistance 2* (Copyright No. PA 1-619-506), and *Uncharted Drake's Fortune* (Copyright No. PA 1-611-286). *Id.*, Exh. A.

All PlayStation3 video games are programmed with computer code, referred to herein as PlayStation3 Programmer Tools ("PS3 Programmer Tools"), that authenticate authorized video game software and facilitate interaction with the central processing unit and microprocessors in the PS3 System. Mogilefsky Decl. at ¶3. A video game whose program does not incorporate the PS3 Programmer Tools cannot be played on the PS3 System. *Id.* The PS3 Programmer Tools are also incorporated within the PS3 System firmware. *Id.* SCEA is the licensee of the registered copyright for the PS3 Programmer Tools (Copyright No. TX0007208564) and is authorized to sublicense its rights to use, copy and distribute the Tools to third party video game developers and publishers. Russell Decl., Exh. B.

SCEA also offers licenses to third parties to develop interactive entertainment software products for the PS3 System. Russell Decl. at ¶6. These licensees are authorized to use proprietary PlayStation®3 technology to develop video game software for the PS3 System and to publish and distribute their video games. *Id*. SCEA receives royalties on each PlayStation®3 video game manufactured pursuant to its licenses with third party publishers. *Id.*

C. Defendants' Illegal Activities

Since the release of the PS3 System in 2006, software hackers have attempted to write code to run unauthorized software on SCEA's gaming system. Mogilefsky Decl. at ¶15.

Until a few days ago, the efforts of these hackers were largely thwarted by the TPMs that secure the various levels of the PS3 System. *Id.* at ¶15. In late December 2010, a hacking group called FAIL0VERFLOW discovered a way to access certain (but not all) levels of the PS3 System by circumventing the corresponding TPMs. *Id.* at ¶16; Bricker Decl. at ¶5, Exh. D. At that point, hackers were given the tools to run unauthorized and pirated software on the PS3 System. Mogilefsky Decl. at ¶¶16-18. Building on FAIL0VERFLOW's work, Defendant Hotz unlawfully gained access to a critical level of the PS3 System by circumventing the corresponding TPMs. *Id.* at ¶26. In early January 2011, Hotz publicly distributed the circumvention devices necessary to access that level, providing them to the public via the Internet and releasing software code that will allow users to run unauthorized or pirated software on the PS3 System. *Id*. at ¶¶20-25. Unless this Court enjoins Defendants' unlawful conduct, hackers will succeed in running and distributing Circumvention Devices that run pirated software on the PS3 System.

1. The FAIL0VERFLOW Defendants' Unlawful Conduct and Circumvention Devices

Defendants Bushing, Hector Cantero, Sven Peter and Segher formed FAIL0VERFLOW, a hacking group, with the purpose of circumventing the technological protection measures in the PS3 System and accessing and obtaining SCEA's proprietary code from within the System. Bricker Decl. at ¶¶3-4, Exhs. B-C.[2] On December 29, 2010, the FAIL0VERFLOW Defendants appeared at the Chaos Communication Conference (the "Chaos Conference"), a hacker event in Berlin. *Id.* at ¶4, Exh. C. Boasting that they had circumvented TPMs for certain levels of the PS3 System, the FAIL0VERFLOW Defendants broadcast detailed instructions for their circumvention method (the "FAIL0VERFLOW Instructional Materials") and promised to divulge information and proprietary code they obtained by unlawfully accessing the PS3 System. *Id.* at ¶5, Exh. D. Hours after the Chaos

[2] Each member of FAIL0VERFLOW has a history of circumventing TPMs and touting their exploits. Bricker Decl. at ¶3, Exh. B; ¶¶6-7, Exhs. E-F; ¶¶10-19, Exhs. I-R; ¶28-29, Exhs. AA-BB.

Conference, the FAIL0VERFLOW Defendants' Instructional Materials were published on the Internet. *Id.* Within two days, the group began publishing the code, software tools and scrambled or encrypted keys derived from their circumvention of the TPMs on Twitter and other websites. *Id.* at ¶¶6-7, Exhs. E-F; Mogilefsky Decl. at ¶18.

The FAIL0VERFLOW Defendants' Instructional Materials and code, software tools and keys constitute Circumvention Devices. The Instructional Materials enable others to gain access to certain protected levels in the PS3 System. Mogilefsky Decl. ¶17. Armed with the code, software tools and keys released by the FAIL0VERFLOW Defendants, individuals can now decrypt, avoid, bypass, deactivate or impair TPMs that protect fundamental levels of the PS3 System, and impermissibly run unauthorized software at those levels. *Id.* at ¶¶17-18. Indeed, other hackers have used the information and tools released by the FAIL0VERFLOW Defendants to circumvent the TPMs of the PS3 System and publish and traffick in circumvention devices. *Id.* at 17; Bricker Decl. at ¶8, Exh. G. This is exactly what the FAIL0VERFLOW Defendants wanted when, prior to releasing their Circumvention Devices, they posted the following message on Twitter:

> We'll release tools … someone else can take over. The fun part is done ;)

Bricker Decl. at ¶3, Exh. B.

The FAIL0VERFLOW Defendants intentionally circumvented SCEA's TPMs, accessed the PS3 System and trafficked in Circumvention Devices and SCEA's proprietary information, with full knowledge that their unlawful conduct would irreparably harm SCEA. Indeed, five days prior to appearing at the Chaos Conference, Bushing echoed a fellow hacker's comment anticipating this irreparable harm: "Last chance to sell any Sony stock you may have." *Id.* at ¶18, Exh. Q.

2. George Hotz's Unlawful Conduct and Circumvention Devices

Defendant Hotz is a well-known hacker who has gained notoriety for circumventing the technological protection measures in a number of sophisticated software and hardware systems. *Id.* at ¶20, Exh. S. Building on the FAIL0VERFLOW Defendants' Circumvention

Devices, Hotz circumvented certain other TPMs in the PS3 System, intentionally accessed the PS3 System without authorization, and misappropriated critical SCEA Keys (referred to hereinafter as the "Metldr Keys" or the "Root Keys"):

> forgot to thank fail0verflow. . . . They had several keys but not the root key, I used their discoveries to find the [] root key."

Id. at ¶21, Exh. T.[3] The Root Keys, or "Metldr Keys," that Hotz wrongfully compromised are part of a TPM in the PS3 System, and are necessary to authenticate code that runs on a critical level of that System. Mogilefsky Decl. ¶12. With access to this particular level, one can control crucial functions and operations of the PS3 System and execute code that will enable pirated video games to run on the PS3 System. *Id*.

Knowing that the "Metldr Keys" can defeat TPMs in the PS3 System, Hotz began using these proprietary Keys as a component of a Circumvention Device that applies SCEA signatures to any file, effectively "tricking" the PS3 System into running unauthorized programs. Mogilefsky Decl. ¶23. On January 2, 2011, Hotz published the Metldr Keys on his website under the banner "keys open doors." Bricker Decl. at ¶23, Ex. V. By doing so, Hotz purposefully compromised the confidentiality of those Keys and invited other software pirates to incorporate the Keys into their own circumvention technology. *Id.* (quoting Hotz January 2nd post: "use this info wisely"). Hotz's distribution of the Metldr Keys enabled software pirates to create and run unauthorized copies of video games. Mogilefsky Decl. ¶20.

Shortly thereafter, Hotz began incorporating the Metldr Keys into other Circumvention Devices and software packages that he or other hackers had built. Mogilefsky Decl. ¶23. Many of these Devices and packages – including "dePKG Firmware Decrypter" – were of limited use without SCEA's proprietary Keys. Armed with some of SCEA's Keys, however,

---

[3] Hotz further recognized the FAIL0VERFLOW Defendants' contribution to his circumvention method, stating "props to fail0verflow." Bricker Decl. ¶22, Exh. U. The FAIL0VERFLOW Defendants confirmed their collaboration with Hotz by posting the following statement on their Twitter page: "We discovered how to get the keys. . . . Geohot exploited metldr, then used our trick to get its keys." *Id.* at ¶3, Exh. B.

Hotz was able to use his dePKG Firmware Decrypter to decrypt a version of SCEA's firmware,[4] modify the firmware to remove and/or bypass some of its TPMs, and add a digital signature using the compromised Metldr Keys. Mogilefsky Decl. ¶22. On January 7, 2011, Hotz posted a video to YouTube demonstrating his circumvention of the PS3 System's access controls and execution of this unauthorized, modified version of SCEA's firmware. Bricker Decl. at ¶24, Exh. W. He referred to this process as "jailbreaking," and happily explained that the "jailbroken" firmware allowed him to run other unauthorized programs on the PS3 System. *Id.*

One day later, in furtherance of his unlawful conduct, Hotz published on his website the "3.55 Firmware Jailbreak" code, a circumvention device or component thereof that disables, avoids, bypasses, removes, deactivates and/or impairs a critical TPM in the PS3 System. *Id.* at ¶22, Exh. U; ¶25, Exh. X; ¶26, Exh. Y; Mogilefsky Decl. ¶24. The 3.55 Firmware Jailbreak code allows users to install and run unauthorized software – including pirated video games – in circumvention of the TPMs on the PS3 System. Mogilefsky Decl. ¶24. Indeed, in the last few days, people have already started copying, playing and trafficking in pirated copies of video games using the 3.55 Firmware Jailbreak. Bricker Decl. at ¶2, Exh. A.

Most recently, on January 9, 2011, Hotz published "Signing Tools" that enable encryption and signing of unauthorized content, thereby permitting that content to run in circumvention of the TPMs on the PS3 System. *Id.* at ¶22, Exh. U; Mogilefsky Decl. at ¶25. These Signing Tools work together with the 3.55 Firmware Jailbreak to allow piracy. Mogilefsky Decl. at ¶25.

By distributing the Circumvention Devices discussed herein, Hotz has caused irreparable injury and damage to SCEA. Russell Decl. at ¶¶9-10. Recognizing the harmful impact of his unlawful conduct on SCEA and attempting to leverage his circumvention

---

[4] Firmware is a fixed program or data structure that internally controls various electronic devices, such as the PS3. Mogilefsky Decl. at ¶2.

activities, Hotz addressed SCEA when he posted the Metldr Keys. Bricker Decl. at ¶22, Exh. U. In an attempt to obtain employment, he wrote: "if you want your next console to be secure, get in touch with me." *Id.* Furthermore, in a January 6, 2011 interview with the BBC, Hotz acknowledged that his conduct will catalyze the piracy of video games: "I hate that it enables piracy." *Id.* at ¶27, Exh. Z. Despite feigning disturbance resulting from the proliferation of piracy, Hotz then went on to release 3.55 Firmware JailBreak and the Signing Tool – both components of Circumvention Devices that are designed to facilitate videogame piracy. *Id.* at ¶22, Exh. U. Even the FAIL0VERFLOW Defendants, when interviewed, admitted that they expect Mr. Hotz's conduct "to make piracy easier without accomplishing anything intrinsically useful." *Id.* at ¶28, Exh. AA.[5]

III. A TEMPORARY RESTRAINING ORDER IS NECESSARY TO PREVENT VIOLATIONS OF THE DMCA AND THE CFAA

A. SCEA Has Satisfied The Standards For Granting A Temporary Restraining Order And A Preliminary Injunction

The standards in the Ninth Circuit for obtaining a temporary restraining order are identical to those for obtaining a preliminary injunction. *State of Alaska v. Native Village of Venetie*, 856 F.2d 1384, 1389 (9th Cir. 1988). SCEA is entitled to preliminary injunctive relief if it shows (1) a likelihood of success on the merits; (2) a likelihood of irreparable harm absent a preliminary injunction; (3) that the balance of equities tips in favor of issuing an injunction; and (4) that an injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 129 S.Ct. 365, 374 (2008). A preliminary injunction is a way to preserve the status quo and prevent irreparable loss of rights before judgment. *See, e.g., Textile Unlimited, Inc. v. A. BMH & Co.*, 240 F.3d 781, 786 (9th Cir. 2001); *Sierra On-Line,*

---

[5] In a public on-line forum, FAIL0VERFLOW Defendant, Cantero, said "We didn't release keys due fear of legal repercussions, but we told people exactly how to calculate them, and they did." Bricker Decl. at ¶28, Exh. AA. In an earlier post, Defendant Cantero said, "we used these techniques to obtain encryption, public, and private keys [for several fundamental levels of the PS 3 System]. With these keys we could decrypt and sign our own firmware. … The metldr key does break the console's security even more (especially with respect to newer, future firmwares – and thus also piracy of newer games) …." *Id*.

Inc. v. Phoenix Software, Inc., 739 F.2d 1415, 1422 (9th Cir. 1984). Indeed, "public policy favors injunctive relief to remedy the infringement of intellectual property rights." *Yash Raj Films (USA), Inc. v. Sidhu*, 2010 U.S. Dist. LEXIS 25988, *17-18, 2010 WL 1032792, *7 (E.D. Cal. 2010). Courts may also consider whether the granting of a preliminary injunction favors the public interest. *Sun Microsystems, Inc. v. Microsoft Corp*., 21 F. Supp. 2d 1109, 1118 (N.D. Cal. 1998). Both a temporary restraining order and preliminary injunction are clearly proper here.

B. The DMCA Authorizes Courts To Enjoin Persons From Trafficking In Circumvention Devices, And The CFAA Authorizes Courts To Enjoin Persons From Accessing Computers Without Authorization, Obtaining Proprietary Information And Trafficking In Such Information

SCEA has brought suit against Defendants based, *inter alia*, on their violations of the Digital Millennium Copyright Act ("DMCA").[6] The DMCA specifically authorizes the granting of "temporary and permanent injunctions" to restrain violations of the DMCA, including circumvention of technological protection measures and trafficking in circumvention devices. 17 U.S.C. § 1203(b)(1). Likewise, the CFAA provides "injunctive or other equitable relief." 18 U.S.C. § 1030 (g). Courts, including this one, have issued temporary and preliminary injunctive relief to restrain violations of the DMCA in situations like the threat posed by Defendants here. *See, e.g., Realnetworks, Inc. v. DVD Copy Control Ass'n.,* 641 F. Supp. 2d 913 (N.D. Cal. 2009) (granting TRO and preliminary injunction based on defendants' sale of circumvention devices that make copies of copyrighted content); *SuccessFactors, Inc. v. Softscape, Inc*., 544 F. Supp. 2d 975, 981 (N.D. Cal. 2008) (granting preliminary injunction under the CFAA to cease unauthorized access of computer and use of confidential information); *YourNetDating, LLC v. Mitchell*, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (granting TRO against computer hacker under the CFAA).

---

[6] In its Complaint, SCEA has also alleged claims for contributory copyright infringement under the Copyright Act, the California Comprehensive Computer Data Access and Fraud Act, breach of contract, tortious interference with contractual relations, trespass and common law misappropriation. SCEA is basing its request for TRO only on its DMCA and CFAA claims.

C. SCEA Has Demonstrated An Indisputable Likelihood of Success On T7he Merits Of Its DMCA Claim

The DMCA was enacted to prohibit, *inter alia*, circumvention of effective technological protection measures and the trafficking of devices that circumvent the technological measures used by copyright owners to restrict access to their copyrighted works. *See* 17 U.S.C. § 1201 *et seq*. Liability under the DMCA for circumventing a technological protection measure is established by showing that: (1) plaintiff's TPMs, in the ordinary course of operation, prevent access to a work protected under the Copyright Act; and (2) defendant has circumvented those TPMs. *See* 17 U.S.C. § 1201(a)(1)(A); *321 Studios v. Metro Goldwyn Major Studios, Inc.,* 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004). Liability under the DMCA for trafficking in circumvention devices is established by showing that: (1) plaintiff's technological mechanism, in the ordinary course of operation, prevents access to a copyrighted work (or protects a right of the copyright owner in the work); and (2) defendant traffics in devices, or components thereof, primarily designed to circumvent such protections. *See* 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1); *321 Studios,* 307 F. Supp. 2d at 1097-99. SCEA easily satisfies the elements to prove that Defendants have both circumvented the TPMs that prevent access to SCEA's copyrighted works and trafficked in circumvention devices or components thereof.

Defendants have circumvented technological protection measures that effectively control access to the PS3 System, the works therein, and other copyrighted SCEA works and the in violation of the DMCA, insofar as Defendants decrypted, avoided, bypassed, removed, deactivated, or impaired those technological measures. Indeed, both the FAIL0VERFLOW Defendants and George Hotz circumvented multiple encryption and access controls in order to retrieve and compromise various Keys used by SCEA to prevent individuals from running unauthorized code on the PS3 System. Bricker Decl. at ¶28, Exh. AA (Canton, a member of FAIL0VERFLOW, noting that the group "deserve[s] a little more credit than we're getting for [Hotz's 3.55 Firmware Jailbreak]" because "he used our key recovery attack verbatim"); Bricker Decl. at ¶5, Exh. D (explaining the "recovery attack" used by the FAIL0VERFLOW

Defendants and Defendants Hotz in detail). In addition to their circumvention of such encryption and access controls, the Defendants misappropriated SCEA's proprietary Keys and used those Keys without permission in order to avoid SCEA's effective technological measures. Bricker Decl. at ¶21, Exh. T (announcing Hotz's disclosure of Metldr Keys). By circumventing those effective TPMs, all Defendants have clearly violated 17 U.S.C. §1201(a)(1). Such conduct constitutes circumvention, as this Court has recognized several times. For example, in *Realnetworks, Inc. v. DVD Copy Control Ass'n,* 641 F. Supp. 2d 913, 934 (N.D. Cal. 2009), this Court held that the defendant had circumvented technological measures that effectively controlled access to copyrighted DVD content, where the defendant had a limited license to use some of the Plaintiff's "decryption keys," but used those keys outside of the scope of its license to gain unlawful access to the DVD content and create a permanent copy. Moreover, this Court concluded that the defendant in *Realnetworks* circumvented technological measures each time it accessed the content that it copied during its first instance of circumvention. *Id. See also 321 Studios v. Metro Goldwyn Mayer Studios, Inc.,* 307 F. Supp. 2d 1085 (N.D. Cal. 2004) (holding that decryption software violated the DMCA by avoiding and bypassing an encoding scheme used by DVD producers, because although the software used authorized "decryption keys," it did so without the permission of the content owner).

The law is also clear that trafficking in Circumvention Devices is illegal under the DMCA in that their primary purpose is to bypass a technological measure designed to protect copyrighted works. For example, in *Sony Computer Entertainment America v. Divineo, Inc.*, 457 F. Supp. 2d 957 (N.D. Cal. 2006), this Court granted summary adjudication and injunctive relief based on defendants trafficking in similar "mod chip" circumvention devices in violation of the DMCA. *See also 321 Studios,* 307 F. Supp. 2d at 1085 (granting summary judgment and injunction in favor of copyright holders on DMCA claim); *Nintendo of America Inc. v. Chan*, 2009 U.S. Dist. LEXIS 66624, 2009 WL 2190186 (C.D. Cal. 2009) (granting preliminary injunction based on defendant's marketing and trafficking of "game copiers."); *Coxcom, Inc. v. Chaffee,* 536 F.3d 101 (1st Cir. 2008) (granting TRO and preliminary

injunction based on defendants' sales of digital cable filters in violation of the DMCA); *Macrovision v. Sima Products Corp.*, 2006 U.S. Dist. LEXIS 22106, 2006 WL 1063284 (S.D.N.Y. 2006) (granting preliminary injunction based on defendants' sale of "video enhancer" products that circumvented plaintiff's DVD copy protection technology); *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 225-26 (S.D.N.Y. 2000) (granting preliminary injunction on DMCA claim).

The Ninth Circuit in *MDY Industries* clarified this standard, explaining that the test requires that the defendant (1) traffics in (2) a technology or part thereof (3) that is primarily designed, produced, or marketed for, or has limited commercially significant use other than (4) circumventing a technological measure (5) that effectively controls access (6) to a copyrighted work. *MDY Industries v. Blizzard Entertainment, Inc.,* 2010 WL 5141269 at *18, 2010 U.S. App. LEXIS 25424 at *28-29, 2010 WL 5141269 at *18, No. 09-15932 Slip. Op. (9th Cir., Dec. 14, 2010).

1. Traffics In

The Defendants are trafficking, offering, and distributing their Circumvention Devices through various internet channels, including their websites and Twitter accounts. Bricker Decl. at ¶¶5-7, Exhs. D-F; ¶22, Exh. U.

2. A Technology or Part Thereof

These Circumvention Devices comprise computer code that circumvents the TPMs in the PS3 System, thereby allowing users to install and run unsigned programs, and play pirated video games. Mogilefsky Decl. at ¶¶18-24.

3. Primarily Designed

The FAIL0VERFLOW team and George Hotz designed these illegal Devices with the sole purpose and function to circumvent the TPMs that effectively prevent access to the PS3 System and related copyrighted works. *Id.* at ¶ 27. Indeed, the Defendants themselves advertise and promote their own circumvention, and distribute those Circumvention Devices with a clear message inducing others to use the Devices in the same manner. *See, e.g.,* Bricker Decl. at ¶24, Exh. W (video showing Defendant Hotz using his "3.55 Firmware

Jailbreak" to circumvent TPMs in the PS3 System); *Id.* at ¶22, Exh. U (offering links to download the "3.55 Firmware Jailbreak," the "Signing Tools).

4. Circumvention Device

The Circumvention Devices distributed by Defendants enable users to circumvent or disable the TPMs in the PS3 System: Hotz's Metldr Keys, dePKG Firmware Decrypter, 3.55 Firmware Jailbreak code and Signing Tool, individually, or in combination, decrypt, bypass, disable, or impair certain TPMs within the PS3 System and enable users to run pirated video games; indeed, some of these Circumvention Devices have even been packaged together to facilitate piracy. *Id.* at ¶30, Exh. CC ("First PS3 Backup Working on Geohot CFW 3.55," providing step-by-step instructions for using the 3.55 Firmware Jailbreak code and Signing Tool to pirate video games). Further, the FAIL0VERFLOW Defendants' code, software tools and keys together with their Instruction Materials enable users to bypass TPMs to allow unauthorized software to run. Mogilefsky Decl. at ¶18; *supra,* Section I (C)(1). Moreover, The combination of Defendants' various Circumvention Devices and/or components thereof have no commercially significant purpose other than to circumvent SCEA's technological protection measures. The Defendants designed the methods, programs, and code described herein, and offered to the public, trafficked in, and/or distributed those Circumvention Devices with the express intent of allowing others to circumvent SCEA's technological protection measures so that they can impermissibly run unauthorized code on the PS3 System.

5. Effective TPMs

As noted above, the TPMs in place on the PS3 System prevent users from playing unlicensed or copied video game discs and installing unlicensed software, such as Hotz's 3.55 Firmware Jailbreak. Mogilefsky Decl. ¶ 7.

6. Copyrighted Work

If these TPMs are circumvented or disabled, users can access the copyrighted PS3 Programmer Tools and can copy borrowed or rented video game discs, and play those copied video games later without inserting the authentic, licensed disc. *Id*. at ¶14.

In sum, SCEA has shown an unquestionable likelihood of success on the merits of its DMCA claim.[7]

D. SCEA Has Demonstrated An Indisputable Likelihood of Success On The Merits Of Its Claim Under The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq*.

Defendants have committed numerous offenses under the Computer Fraud and Abuse Act (CFAA"), 18 U.S.C. §1030 (a), including: circumventing the TPMs in the PS3 System, intentional unauthorized accessing of the PS3 System firmware, obtaining SCEA's proprietary information or code and distributing it, and impairing the confidentiality of information obtained from the PS3 System.

1. 18 U.S.C. § 1030(a)(2)(C) – Confidential Information On Computer

To prove a violation under 18 U.S.C. § 1030(a)(2)(C), SCEA must show that Defendants: (1) intentionally accessed a protected computer used for interstate commerce or communication; (2) without authorization or by exceeding authorized access to the protected computer; and (3) thereby obtained information from the protected computer. SCEA has established these elements.

First, the PS3 System consists of a "protected computer" because it is used in interstate commerce (e.g., the Internet.) Second, without SCEA's authorization, Defendants intentionally accessed certain levels of the PS3 Systems by circumventing SCEA's TPMs in the PS3 Systems. Mogilefsky Decl. at ¶¶16-22. Defendants' access to such levels in the PS3 Systems is not authorized; to the contrary, the PlayStation Network Terms of Service and User Agreement ("PSN User Agreement") prohibits the circumvention of security

---

[7] "Fair use" is no defense even if there were a conceivable noninfringing use for these devices. As this Court explained in *Divineo*, "downstream customers' lawful or fair use of circumvention devices does not relieve [defendant] from liability for trafficking in such devices under the DMCA." 457 F. Supp. at 965. *See, e.g., Realnetworks,* 641 F. Supp. 2d at 942 (any limited "fair use" exception does not apply to manufacturers or traffickers of the circumvention devices); *321 Studios*, 307 F. Supp. 2d at 1097 ("the downstream uses of the software by the customers of [defendant], whether legal or illegal, are not relevant to determining whether [defendant] itself is violating the statute."); *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000).

features in the PS3 System. Complaint at ¶15, Exh. A.[8] *See, e.g., Craigslist, Inc. v. Naturemarket, Inc.,* 694 F. Supp. 2d 1039, 1052 (N.D. Cal. 2010) (violation of user agreement established "without authorization" requirement of the CFAA); *eBay v. Digital Point Solutions*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) ("access and use beyond those set forth in a user agreement constitute unauthorized use under the CFAA."); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) ("Defendants' actions violated [the] Terms of Service, and as such was unauthorized.") Finally, as a result of their unauthorized access, Defendants succeeded in discovering – then obtaining – SCEA's proprietary information, including SCEA's Keys that digitally sign code to run on certain secure levels of the PS3 System. Mogilefsky Decl. at ¶¶16-20.[9]

2. 18 U.S.C. § 1030(a)(4) – Intent To Defraud And Obtain Value

To prevail on a claim under § 1030(a)(4), SCEA must show that Defendants: (1) knowingly and with intent to defraud accessed a protected computer without authorization, or exceeded authorized access; and (2) by means of such conduct furthered the intended fraud and obtained anything of value. SCEA has satisfied these elements.

As discussed above, Defendants accessed the PS3 Systems without authorization. Because Defendants intentionally circumvented the TPMs in the PS3 Systems, their acts were knowing and with intent to defraud, and they furthered the intended fraud and obtained something of tremendous value – SCEA's proprietary information, including the Keys to the PS3 Systems. Bricker Decl. at ¶¶3, 22, Exhs. B, U. Indeed, "fraud" in this context means simply "wrongdoing and not proof of the common law elements of fraud." *Shurgard Storage*

---

[8] In its Complaint, SCEA has also brought claims for breach of the PSN User Agreement and tortious interference with contractual relations.

[9] SCEA has standing to assert claims under the CFAA because Defendants' conduct has caused loss to SCEA during any one year period aggregating far more than $5,000 in value, and because Defendants' conduct has caused damage affecting 10 or more PS3 Systems during any one year period. *See Mortensen v. Bresnan Commun*., 2010 U.S. Dist. LEXIS 13419, at *20-21, 2010 WL 5140454, at *7 (D. Mont. 2010) (installation and distribution of Internet cookies onto multiple computers was sufficient to allege damages in excess of $5,000)

Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wa. 2000); s*ee also eBay, Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) ("'fraud'" under the CFAA only requires a showing of unlawful access."). Accordingly, Defendants have violated §1030 (a) (4) of the CFAA.

3. 18 U.S.C. § 1030(a)(5)(A) – Knowing Transmission of Code

Under 18 U.S.C. § 1030(a)(5)(A), SCEA will also likely prevail on its claim that Defendants "knowingly caused the transmission of a program, information, code or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer." Defendants knowingly transmitted SCEA's proprietary information or code via the Internet, which has greatly damaged SCEA and threatens to cause immeasurable damage to the PS3 System. Bricker Decl. at ¶¶6-7, 21, Exhs. E-F, T.

4. 18 U.S.C. § 1030(a)(5)(B) and (C) – Intentional and Reckless Damage And Loss

To prove a violation under 18 U.S.C. § 1030(a)(5)(B) and (C), SCEA must show that Defendants "intentionally accessed a protected computer without authorization, and, as a result of such conduct, recklessly causes damage" or "recklessly causes damage or loss." As established above, Defendants intentionally accessed the PS3 System without SCEA's authorization. There is no doubt that Defendants' unlawful access of the PS3 Systems has caused and will continue to cause great damage and loss to SCEA unless enjoined. Russell Decl. at ¶10. By accessing the PS3 Systems, Defendants have impaired the TPMs in the PS3 Systems, which protect fundamental levels of the PS3 System, and they are illegally running unauthorized software at those levels. Mogilefsky Decl. at ¶¶23-24. *See Black & Decker (US), Inc. v. Smith,* 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008) ("intentionally rendering a computer system less secure should be considered 'damage" even when no data, program or system is damaged or destroyed."). Unless Defendants are enjoined, SCEA will continue to sustain great loss, including lost video game software sales for SCEA and other game publishers, as a result of Defendants' unauthorized access to the PS3

System. Russell Decl. at ¶¶9-10.

5. 18 U.S.C. § 1030(a)(6)(A) – Trafficking in Password

Under 18 U.S.C. § 1030(a)(6)(A), SCEA will likely prevail on its claim that Defendants "knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce." As discussed above, Defendants have trafficked in Circumvention Devices and SCEA's proprietary information, including the Keys which effectively provide the "password" to access the most secure areas of the PS3 System, with full knowledge that their unlawful conduct would irreparably harm SCEA.

6. 18 U.S.C. § 1030(a)(7)(B) – Intent to Extort

Finally, SCEA will likely prevail on its claim under §1030(a)(7)(B), which prohibits "intent to extort from any person any money or other thing of value" by threatening "to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access." Hotz violated this provision when, in the same post in which the published SCEA's Keys, he attempted to obtain from SCEA "a thing of value" in the form of employment: "if you want your next console to be secure, get in touch with me." Bricker Decl. at ¶22, Exh. U.

To prevent further harm to SCEA, the Court should immediately enjoin Defendants' unauthorized access of the PS3 Systems.

E. Absent Injunctive Relief, SCEA Will Suffer Irreparable Injury And The Balance Of Hardships Strongly Favors SCEA

Defendants' distribution of Circumvention Devices and unauthorized access of the PS3 System allow copyright infringement to occur unchecked. Unless Defendants are enjoined, SCEA will be irreparably harmed. *See e.g., Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 215 (S.D.N.Y. 2000) (technology that circumvents copy

protection systems gives rise to "the same immediate and irreparable injury" as would occur with direct copyright infringement.)[10]

There can be no dispute that Defendants' continued illegal distribution of the Circumvention Devices will greatly erode SCEA's ability to protect its valuable intellectual property rights. *A&M Records, Inc. v. Napster, Inc*., 239 F.3d 1004, 1029 (9th Cir. 2001) (granting injunctive relief because otherwise "plaintiffs would lose the power to control their intellectual property."). If SCEA "is unable to prevent the circumvention of its technology, its business goodwill will likely be eroded, and the damages flowing therefrom extremely difficult to quantify." *Macrovision v. Sima Products Corp*., 2006 U.S. Dist. LEXIS 22106, *8, 2006 WL 1063284, *3 (S.D.N.Y. 2006). *See, e.g., Apple Inc. v. Psystar Corp.*, 673 F. Supp. 2d 943, 948 (N.D. Cal. 2009) (irreparable harm in a copyright infringement action may be established through reputational harm); *MGM Studios, Inc. v. Grokster,* Ltd., 518 F. Supp. 2d 1197, 1215 (C.D. Cal. 2007). All the cases hold that "Intangible injuries such as damage to. . . goodwill qualify as irreparable harm." *Rent-A-Center, Inc. v. Canyon Television & Appliance Rental, Inc.*, 944 F.2d 597, 603 (9th Cir. 2001).

The Central District of California in *Nintendo of America, Inc. v. Bung Enterprises, Ltd*., 1999 U.S. Dist. LEXIS 23588 at *36, 1999 WL 34975007, *13 summed up the dilemma facing copyright owners like SCEA:

> The sale of pirated video games, primarily through electronic transfers on the Internet, is proliferating. For obvious practical reasons, Nintendo and other owners of game copyrights, cannot attack this practice through actions against the direct infringers, who are frequently individuals or small commercial operations that use [circumvention devices] to make illegal copies of Nintendo

---

[10]There is a split of authority among the courts in the Northern District of California on whether a presumption of irreparable harm based on likelihood of success on the merits in copyright actions exists after the U.S. Supreme Court's decision in *Winter v. Natural Res. Def. Council, Inc*., 129 S. Ct. 365, 374 (2008). *Realnetworks, Inc. v. DVD Copy Control Ass'n, Inc.,555 U.S. 7,* 641 F. Supp. 2d 913, 953 (N.D. Cal. 2009) (recognizing presumption of irreparable harm in copyright infringement case). *But see Jacobsen v. Katzer,* 609 F. Supp. 2d. 925, 936 (N.D. Cal. 2009) (rejecting any presumption of irreparable harm in copyright cases). However, even if irreparable injury is not presumed, SCEA has established such harm.

> products, which are then sold or given to others or uploaded to the Internet. As Congress clearly recognized when it adopted Section 1201 of the DMCA, the only effective way to protect a game or other software developer's investment in its copyright is by bringing an end to the sale of devices which are designed to circumvent the security protection placed within the software. Congress thereby recognized that ***the only effective way to stop the game counterfeiting industry is by enjoining companies… from making the devices through that industry is able to thrive***.

Nintendo of America, Inc. v. Bung Enterprises, Ltd., 1999 U.S. Dist. LEXIS 23588 at *36, 1999 WL 34975007, *13 (emphasis added). Unless enjoined, the proliferation of PS3 video game piracy will irreparably harm SCEA by: (1) undermining SCEA's monumental investment in the PS3 System; (2) eliminating SCEA's control over distribution of its copyrighted works; (3) harming SCEA's reputation with third party game developers; and (4) diminishing the sales of legitimate PS3 video games by SCEA and its authorized retailers. Russell Decl. at ¶¶10-12.

SCEA's affiliates invested hundreds of millions of dollars developing the PS3 System, including the PS3 System's security measures. *Id*. at ¶12. The widespread distribution of devices that disable or circumvent these measures, however, eradicates the investment in the technology and undermines the values that these TPMs are meant to preserve. *Id.* Primary among these values is SCEA's ability to control distribution of its copyrighted video games, as well as those video games owned by third party licensees. *Id.* For each new consumer that gains access to Defendants' circumvention devices, SCEA loses the ability to prevent that consumer from copying and playing copied SCEA-copyrighted video games. *Id.* Once these devices are in the hands of consumers, the loss of control over SCEA's copyrighted material is permanent and irreparable. *Id.* Equally serious is the damage to SCEA's reputation and goodwill with third party game developers, whose own copyrighted video games are pirated for use with the PS3 System as well. *Id*. All of this piracy adds up ultimately to lost sales for SCEA and other video game publishers as an enormous number of consumers naturally prefer free copies of video games over spending money to purchase the originals. *Id*.

SCEA has established that Defendants' publication, trafficking in and distribution of the Circumvention Devices facilitate the sale and playing of unauthorized or unlicensed copies of PS3 System video game software. *See* Section III.c., *supra*. If these devices are made further available on the market, they will have a dramatic downward effect on the sales of PS3 video games, as unauthorized copies of PS3 System video games will quickly circulate and become prevalent in the marketplace. Russell Decl. at ¶¶10-12; Bricker Decl. at ¶30, Exh. CC. *It is already happening*. Even now, pirated video games are being packaged and distributed with these circumvention devices. Bricker Decl. at ¶¶2, 30, Exhs. A, CC. In the absence of injunctive relief, Defendants will continue their illegal activity while SCEA will continue to be greatly harmed by the distribution of these circumvention devices to the public. The lack of injunctive relief will therefore result in the loss of goodwill to licensees, encourage infringers to increase operations, and discourage anti-piracy enforcement – all of which is great and irreparable harm. In contrast, Defendants will only be ordered to cease their illicit activity. They will not suffer any monetary damage since, at this point, they are only distributing Circumvention Devices for free on the Internet. Because of the irreparable harm to SCEA and because the balance of hardships weighs heavily in favor of SCEA, SCEA is entitled to a TRO and preliminary injunction.

F. The Public Interest Strongly Favors Granting SCEA Injunctive Relief

In copyright infringement cases, it is ordinarily presumed that an injunction will serve the public interest if the copyright holder shows a likelihood of success on the merits. *Concrete Mach. Co. v. Classic Lawn Ornaments, Inc.*, 843 F.2d 600, 612 (1st Cir. 1988). "[I]t is virtually axiomatic that the public interest can only be served by upholding copyright protections and, correspondingly, preventing the misappropriation of the skills, creative energies, and resources which are invested in the protected work."

The interest of the public will be strongly served through a TRO and preliminary injunction against Defendants' trafficking of the Circumvention Devices and unauthorized access to the PS3 System. Allowing the ongoing distribution of Circumvention Devices will reward – not deter – software piracy, ultimately harming the public. True innovators will be

deterred from investing the effort and resources needed to create new products if counterfeit-enabling developers are allowed to siphon away the compensation that real creators such as SCEA otherwise would earn. On the other hand, no public benefit results from Defendants' activities. No new works have been created; indeed, piracy deters creativity. Public policy certainly does not support violations of the DMCA to facilitate software piracy.

G. SCEA Has Complied With The Procedural Requirements For Issuance Of A TRO And Order To Show Cause Re: Preliminary Injunction

SCEA has complied fully with Fed. R. Civ. P. 65, Local Rules 65-1 and 7-10 for issuance of an *ex parte* TRO and an Order to Show Cause why a preliminary injunction should not issue. SCEA has submitted declarations and other evidence showing that it will be irreparably harmed without an Order restraining Defendants from any further distribution of Circumvention Devices. SCEA has submitted the required documentation in compliance with Local Rule 65-1(a). Bricker Decl. at ¶32.

Fed. R. Civ. P. 65 (c) provides that a bond be posted "in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." A bond "may not be required, or may be minimal, when the harm to the enjoined party is slight or where the movant has demonstrated a likelihood of success." *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1116 (C.D. Cal. 2007); *see also Connecticut Gen. Life Ins. Co. v. New Images of Beverly Hills*, 321 F.3d 878, 882 (9th Cir. 2003) ("bond amount may be zero if there is no evidence the party will suffer damages from the injunction."); *YourNetDating, LLC,* 88 F. Supp. 2d at 872 (no bond required for TRO against hacker who violated the CFAA). Here, there is virtually no prospect that any of Defendants' legitimate interests would be impinged by an order requiring them to cease distribution of the Circumvention Devices. However, if the Court requires that a bond be posted, SCEA submits that the bond should not exceed $5,000 since that amount is more than sufficient to account for the unlikely possibility that Defendants would be "wrongfully enjoined or restrained," from distributing the Circumvention Devices. Fed. R. Civ. P. 65 (c)

IV. AN ORDER OF IMPOUNDMENT OF THE CIRCUMVENTION DEVICES IS WARRANTED

Section 1203 (b) (2) of the DMCA specifically authorizes impoundment of "any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation" of §1201.[11] Accordingly, SCEA seeks the impoundment of any and all media in which circumvention devices are stored within the possession, custody or control of Defendants, including computers, hard drives, CD-ROMs, DVDs, USB sticks and other media.

Impoundment "most often is granted in 'piracy' actions involving widespread duplication or marketing of counterfeit merchandise such [as] . . . video game and other software." 6-35 Nimmer on Copyright §35.05 (2008). Impoundment "is a form of preliminary relief and the same standards apply with respect to issuance of an impoundment order as to issuance of a preliminary injunction." *Yamate USA Corp. v. Sugerman*, 1991 U.S. Dist. LEXIS 20701, *41-42, 1991 WL 274854, at *14 (D.N.J. 1991). Accordingly, courts routinely order the impoundment of infringing materials in preliminary injunction cases. *See, e.g., Sega Enters. v. MAPHIA,* 857 F. Supp. 679, 691 (N.D. Cal. 1994) (ordering the impoundment of video game copiers and unauthorized copies of video game software); *Rebis v. Universal CAD Consultants, Inc*., 1998 U.S. Dist. LEXIS 12366, *12, 1998 WL 470475 *4-5 (N.D. Cal. 1998) (ordering the impoundment of infringing software); *Yamate USA Corp.*, 1991 U.S. Dist. LEXIS 20701 at *44-45, 1991 WL 274854, *14 (ordering the impoundment of defendants' equipment used in making the infringing video games); *Nintendo of America, Inc. v. Elcon Indus., Inc.*, 564 F. Supp. 937, 938 (E.D. Mich. 1982) (ordering the impoundment of infringing video games); *WPOW, Inc. v. MRLJ Enters.*, 584 F. Supp. 132, 139 (D.D.C. 1984)

---

[11] Section 503(a) of the Copyright Act also provides that "at any time while an action under this title is pending, the court may order the impounding, on such terms as it may deem reasonable, of all copies. . . . claimed to have been made or used in violation of the copyright owner's exclusive rights. . .or other articles by means of which such copies. . . may be reproduced."

(impoundment of infringing material issued since the standard for preliminary injunction was met); *Dollcraft Industries, Ltd. v. Well-Made Toy Mfg. Co*., 479 F. Supp. 1105, 1118 (E.D.N.Y 1978) (ordering impoundment of materials infringing copyright and components used for manufacture of the infringing items); *Duchess Music Corp. v. Stern*, 458 F.2d 1305, 1308 (9th Cir. 1972), *cert. denied,* 409 U.S. 847 (1972) (impoundment order in copyright infringement case should "impound *everything* the plaintiff alleges infringes his copyright," including any "means" for making infringing copies.) (emphasis in original). In *Duchess Music Corp*., the Ninth Circuit held it was error for the district court not to order impoundment of machines used by defendants to reproduce the copyrighted records. The Ninth Circuit explained that "machines, blank cassettes and cartridges . . . and other devices are 'other means' for making infringing copies to [plaintiff's] copyrights" and thus "fall within the scope of both the statute and the rules and were properly impounded." *Id.* at 1308. Further, computers, when used to copy and store copyrighted programs, also are subject to impoundment. In *Mitchell Int'l, Inc. v. Fraticelli*, 2007 U.S. Dist. LEXIS 86787, *25-26, 2007 WL 4197583, *10 (D. P.R. 2007), the district court ordered the impoundment of defendant's computers to determine whether they contained any of plaintiff's copyrighted software programs. The same should occur here, as it is almost certain the original Circumvention Devices are stored by Defendants on their computers.

V. CONCLUSION

SCEA respectfully requests that the Court grant the relief in the proposed Order submitted herewith.

DATED: January 11, 2011

Respectfully submitted,
KILPATRICK TOWNSEND & STOCKTON LLP

By:_____
JAMES G. GILLILAND, JR.

Attorneys for Plaintiff
SONY COMPUTER ENTERTAINMENT AMERICA LLC