UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF FLORIDA ORLANDO DIVISION

POSSIBILITY PICTURES II, LLC,)
a Florida limited liability company,)
)
Plaintiff,)
)
v.)
)
)
SONY PICTURES WORLDWIDE)
ACQUISITIONS, INC.,)
a California corporation,)
)
Defendant.)
)
)

Case No. 6:16-CV-1351-ORL-41DAB

COMPLAINT AND DEMAND FOR JURY TRIAL

COMES NOW, Plaintiff, Possibility Pictures II, LLC (d/b/a Two Streets Entertainment) (hereinafter "Licensor" or "Plaintiff"), by and through its undersigned counsel, and files this action against Defendant, Sony Pictures Worldwide Acquisitions, Inc. (hereinafter "SPWA" or "Defendant"), for breach of contract and in further support states as follows:

Introduction

1. On May 30, 2014 Licensor entered into a Distribution Agreement ("Agreement") with SPWA for the distribution the motion picture, "To Write Love On Her Arms (hereinafter "TWLOHA" or "Picture") which was the subject of the Agreement. See Exhibit 1, attached hereto (Bates Nos. 0001-0094). The common purpose of the Agreement between the parties was vastly compromised and frustrated as a result of the entirely foreseeable and avoidable failure of internal

security to protect the Picture from theft in the wake of a cyber attack on the corporate systems of SPWA and its parent, Sony Pictures Entertainment, Inc. ("SPE," along with SPWA hereafter collectively referred to as "SONY") which occurred on November 24, 2014 by a group calling itself "Guardians of Peace."

2. In the aftermath of the cyber attack at least five SONY films were illegally distributed online. These included "Fury," which was in the theaters at the time, and four (4) yet to be released films: (i) "Annie;" (ii) "Mr. Turner;" (iii) "Still Alice;" and (iv) Licensor's Picture, "To Write Love On Her Arms." The cyber attack or hack upon SONY also resulted in the release of non-public, private information ("NPPI") regarding current and former employees and other internal data of SONY.

3. A class action on behalf of current and former employees whose personal information was compromised by the cyber attack was filed in the United States District Court for the *Central District of California. Corona et al v. Sony Pictures Entertainment, Inc.*, U.S.D.C. No. 2:14-cv-09600-RGK (C.D. Cal. 2014). That action was settled on April 6, 2016 after a ruling by the court that the operative complaint had sufficiently alleged facts that (i) SPE "consciously and deliberately failed to maintain an adequate security system" and (ii) the class sustained a cognizable injury by way of costs related to credit monitoring and identity theft protection. See Case No. 2:14-cv-09600, Doc. 97, pp. 4-6 (denying, in part, SPE's motion to dismiss); see also Doc. 151 (minute entry granting Order for Preliminary Approval of Class Settlement and Conditional Class Certification); and Doc. 165 (Order granting Final Approval of Class Settlement).

4. In view of the fact that the cyber attack identified in the California class action directly resulted in the unauthorized release of Plaintiff-Licensor's Picture and the ensuing damages, and that both SPE and SPWA utilized the same computer systems and safeguards, Plaintiff

re-pleads the relevant allegations of the operative complaint in the class action, Case No. 2:14-cv-09600 (Doc. 43, pp. 10-26, pars. 20-60), in describing the inadequacy of those safeguards and SONY's prior knowledge thereof. Upon information and belief, said factual allegations (set forth below in paragraphs 18 through 48) have evidentiary support or likely will have evidentiary support after a reasonable opportunity for further investigation and discovery. Plaintiff expresses its gratitude to class action counsel in that matter and applauds the thoroughness of counsel's efforts.

5. As developed more fully below, Plaintiff attempted to address the matter as required by the Agreement prior to the initiation of this action. That effort having been rejected by SPWA's dismissive response, Plaintiff now seeks to enforce its contractual rights under the Agreement by filing this action at law for money damages as expressly authorized by Section 16.1 of the Agreement. (Bates No. 0021).

PARTIES

6. Plaintiff Possibility Pictures, LLC is a limited liability company organized under the laws of the state of Florida with its main offices in Orange County Florida, in the Middle District of Florida and is *sui juris*. Plaintiff is in the business of producing feature-length films for international distribution. Plaintiff is the grantor of exclusive licensing and distribution rights to the Picture provided to Defendant as more fully set forth in the Agreement. None of Plaintiff's members are domiciliaries or citizens of the state of California.

7. Defendant Sony Pictures Worldwide Acquisitions, Inc. is a for-profit corporation organized under the laws of the state of California with its headquarters in Culver City, California and is *sui juris*. Defendant is the grantee of the exclusive licensing and distribution rights to the Picture as set forth in the Agreement. Defendant is in the business of acquiring and distributing films for a wide variety of distribution platforms, both in theaters and in non-theatrical markets

which are available to paying viewers in Florida, including those in the Middle District of Florida, and throughout United States as well as internationally.

8. As stated above, SPWA is a wholly-owned subsidiary of SPE (collectively "SONY") and each has their respective corporate headquarters housed in the same location in Culver City, California and use, along with other Sony affiliates, the same corporate systems, servers and databases and information technology ("IT") security safeguards (collectively "Network"). At all times relevant hereto, Defendant SPWA relied upon the computer systems security safeguards employed by its parent SPE and the latter served as agent of the former for protecting and safeguarding the intellectual property, specifically the Picture, entrusted to SPWA by Plaintiff pursuant to the terms of the Agreement. Accordingly, the actions and omissions on the part of SPE with respect to its reckless and conscious disregard of Network security against theft, as more fully identified below, are imputed to SPWA.

JURISDICTION AND VENUE

9. This Court has subject matter over this Complaint pursuant to 28 U.S.C. Section 1332(a)(1) in that there is complete diversity of citizenship between Plaintiff and Defendant and the amount in controversy exceeds the jurisdictional threshold of $75,000, exclusive of costs and interest.

10. Specific personal jurisdiction in the State of Florida and the Middle District of Florida is established by virtue of Florida's long arm statute, Fla. Stat., Section 48.193(1)(a) under one or more independent provisions thereof in that SPWA, either personally or through an agent, did one or more of the following acts out of which this cause of action arose:

(i) Operating, conducting, engaging in, or carrying on a business or business venture in this state or having an office or agency in the state;

(ii) Causing injury to persons or property within the state arising out of an act or omission by the defendant outside the state if, at or about the time of the injury, either the defendant was engaged in solicitation or service activities within the state or products, materials or things processed, serviced or manufactured by the defendant anywhere were used or consumed within the state in the ordinary course of commerce, trade or use; or

(iii) Breaching a contract in the state by failing to perform acts required by the contract to be performed in the state.

11. Venue in the Middle District of Florida is proper under 28 U.S.C. Section 1391(b)(1) and (2) in that (i) SPWA "resides" in this judicial district as that term is defined in Section 1391(c)(2) for the reasons set forth in paragraph 10 above; and (ii) a substantial part of the events or omissions giving rise to the claim arose in this district.

FACTUAL ALLEGATIONS

A. TWLOHA Background

12. TWLOHA (the acronym for "to write love on her arms"), from which the name of the Picture is derived, is a non-profit movement dedicated to presenting hope and finding help for people struggling with depression, addiction, self-injury, and suicide. (The term itself relates to the lead female character who was so consumed by her self-loathing that she carved debasing and obscene remarks into the skin of her arm). TWLOHA exists to encourage, inform, inspire, and also to invest directly into treatment and recovery.

13. The non-profit organization was founded by Jamie Tworkowski after he helped a friend, Renee Yohe, with her journey towards recovery. When Jamie met Renee Yohe, she was struggling with addiction, depression, self-injury, and suicidal thoughts. He wrote about the five days he spent with her before she entered a treatment center, and he sold T-shirts to help cover the

cost. When she entered treatment, he posted the story on MySpace to give it a home. The name of the story was "To Write Love on Her Arms."

14. The Picture was developed by Plaintiff d/b/a as Two Streets Entertainment in 2009 and 2010, based on rights acquired from the individuals involved with Renee's journey to recovery. The Picture was funded and produced in 2012, and completed in 2013. In conjunction with delivery of the Picture to Sony in 2014, and as a condition required by SPWA, Plaintiff acquired rights to use the title "To Write Love on Her Arms' from TWLOHA. The total cost of production, which was absorbed entirely by Plaintiff, was $3,382,919. See Exhibit 1, Schedule H, p. 6 (Bates No. 0091).

B. Marketing Plan for the Picture

15. Under the terms of the Distribution Agreement, the principal cast of the Picture (Kat Dennings, Rupert Friend, Chad Michael Murray, and Corbin Bleu) were contracted to provide promotional and publicity services. In addition, to generate interest in the Picture, the producers developed an extensive social media promotional campaign. The cast was well known and highly regarded as popular personalities among movie and television fans. At the time of the execution of the Agreement in 2014, Dennings was starring in the CBS sitcom "2 Broke Girls" and also was featured in a series of major internationally released motion pictures through Marvel Studios including "Thor" and "Thor: The Dark World." She also had appeared in a number of other well known television productions including HBO's "Sex and the City." Similarly, at the time of execution, Friend had already appeared in a number of acclaimed films and was featured in the principal cast of Showtime's multi Emmy and Golden Globe award-winning series "Homeland" as the CIA analyst/assassin.

16. The planned social media campaign included the breadth of the TWLOHA organization, as well as relationships with promotional partners, musicians, athletes, actors and directors, ministry organizations, and leaders in the Christian community. The TWLOHA organization had 32 million followers on Twitter reasonably likely to show considerable interest in the Picture based upon the origins and mission of their charitable organization.

17. In addition, author and mother of Justin Bieber, Pattie Mallette, was retained as an executive producer to provide marketing services. Reportedly, Mallette had social media influence with over 3 million followers. By implementing an extensive social media campaign, the producers planned to generate significant interest in the Picture while minimizing the costs associated with traditional advertising channels. Collectively, the social media reach of individuals and entities connected with TWLOHA or otherwise associated with the Picture was estimated to exceed 200 million contacts for a sustained and direct marketing campaign.

C. The November 24, 2014 Cyber Attack Upon SONY ("Data Breach")

18. On November 24, 2014, the media reported that SONY suffered a massive data breach in its corporate security of its Network ("Data Breach") whereby nearly 100 terabytes of data was seized from the company and caused the leak of financial, medical, and other personal information of thousands of current and former employees on the internet, as well as the taking of the masters of several film productions including the Picture.

19. A hacker group calling itself the Guardians of Peace, or "#GOP", took over SONY's Network, displayed its own messages and an image of a skeleton, seized control of promotional Twitter accounts for SONY movies, and warned SONY that it had obtained "secrets" that it threatened to leak on the Web.

20. The hackers began releasing portions of stolen data to the public on November 30,

2014, beginning with a series of unreleased movies, including Plaintiff's Picture, produced or acquired by SPE or, in the case of the Picture, by SPWA.

21. The hackers posted an estimated 38 million files on file-sharing sites in eight separate leaks, consisting of massive amounts of SPE employee data in addition to internal SPE emails, profit-and-loss statements, and scripts for upcoming SPE television shows and unreleased SPWA movies, including Plaintiff's Picture, in their entirety.

D. Successive Earlier Data Breaches at SPE[1] and Other Sony Companies Exposed Data Security Weaknesses

22. SPE has been a longstanding and frequent target for hackers, but it apparently made a conscious and deliberate business decision to accept both the risk of losses and the actual losses associated with being hacked.

23. SPE's sister companies, Sony Network Entertainment International LLC and Sony Computer Entertainment America LLC, experienced massive data breaches in April 2011, which compromised information from approximately 101 million users accounts, including 12 million unencrypted credit card numbers. Two weeks before those breaches, the companies received an anonymous warning:

> You have abused the judicial system in an attempt to censor information On how your products work. ... Now you will experience the wrath of Anonymous. You saw a hornet's nest and stuck your [expletive] in it. You must face the consequences of your actions, Anonymous style. ... Expect us.

24. One of the 2011 data breaches involved Sony's PlayStation® Network ("PSN"). After the data breach became public, it became clear that while the Sony companies invested significant resources in protecting their own confidential, corporate proprietary information, they

[1] SPE is an indirect, wholly owned subsidiary of Sony Corporation of America ("Sony America"), which is a wholly owned, indirect subsidiary of Sony Corporation ("Sony").

failed to establish even the most basic safeguards for the PSN and its consumer data. Among other things, the PSN was not protected by appropriate firewalls, a deviation from widespread industry practice and standards. As a result, hackers were able to steal the personal information associated with all of the approximately 77 million customer accounts. Experts have attributed the PSN breach to an unsophisticated method of hacking that would not have been successful if even the most basic security measures had been in place.

25. PSN users filed class action cases after the 2011 breach, which Sony agreed to settle in June 2014 in exchange for $15 million in games, online currency, and identity theft reimbursement.

26. Following the PSN breach, Shinji Hasejima, Chief Information Officer of SPE's ultimate parent Sony, admitted that the attack exploited a "known vulnerability" in the application server platform used in the PSN. Sony President Kazuo Hirai admitted that the company's security had been inadequate before the attack, saying that after the hack, the company had "basically ... done everything to bring our practices at least in line with industry standards or better."

27. Despite these public statements that the company had corrected its inadequate security measures, Sony's networks remained highly vulnerable to attack. John Bumgarner, the chief technology officer of the United States Cyber Consequences Unit, an independent, nonprofit research institute which focuses upon preventing large-scale attacks by terrorist groups and rogue nation states upon the U.S. government and its allies as well as private American corporations, uncovered numerous security problems on Sony company webpages that were readily accessible.

Bumgarner discovered that unauthorized users could still access internal Sony resources, including security management tools.

28. In June 2011, SPE itself experienced a data breach in which hackers stole the personal data of over one million customers and released more than 150,000 of the stolen records. The stolen data included names, home addresses, birthdates, email addresses, and phone numbers, as well as customer passwords, which were stored unencrypted.

29. Following the 2011 data breaches, PCWorld technology journalist Tony Bradley observed that Sony "seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked." He advised companies to follow security "best practices and data security compliance requirements" -- and in short -- "Don't be a Sony." Fred Touchette of the email and web security firm AppRiver echoed Bradley's comments, saying: "There is no doubt that Sony needs to spend some major effort in tightening up its network security. This latest hack against them was a series of simple SQL Injection attacks against its web servers. This simply should not have happened."

30. Sony's security gaps, and the attacks, continued. In 2013, hackers infiltrated Sony's Network, stole gigabytes of data several times a week and encrypted the information to cover their tracks.

31. In February 2014, hackers accessed an FTP server used in connection with SPE's international theatrical sales and distribution system, SpiritWorld. The login credentials for two user accounts were compromised and the personal data of 759 individuals associated with theaters

in Brazil, along with payment information for Brazil film distributors, was stolen.

32. In August 2014, approximately one month after Sony settled the class action litigation brought by PlayStation® gamers as a result of the April 2011 breach -- and just three months before the November 24, 2014 Data Breach -- hackers again took down the PSN as well as the Sony Entertainment Network via "denial of service" attacks. The hackers posted on Twitter that their attacks were intended to raise awareness of Sony's inadequate security measures.

E. Ignoring Prior Data Breaches and the Warnings of Its Employees and Third-Party Auditors, SONY Favored Cost Savings and Convenience Over Sound Data Security Principles

33. Given the recent increase of data breaches aimed at major corporations and the prior data breaches at SPE and its affiliated companies, it would be reasonable to expect that SPE would be more vigilant than ever regarding the need to adopt, implement, and maintain security measures to protect its confidential data and the intellectual property, including the Picture, entrusted to it. Instead, SONY has emphasized cost savings over compliance when it comes to data security.

34. The technology and business website CIO reported that a 2005 audit of SPE's security practices alerted Jason Spaltro, SPE's executive director of information security, to several security weaknesses in the company's systems, including insufficiently strong access controls, a key Sarbanes-Oxley requirement. In a 2007 interview, Spaltro was interviewed about compliance with security and privacy regulations. Discussing the risk analysis of protecting private data, he

weighed the hypothetical $10 million cost of preventing a potential intrusion against the hypothetical $1 million cost of responding to a breach. "With those numbers, says Spaltro, 'it's a valid business decision to accept the risk' of a security breach. 'I will not invest $10 million to avoid a possible $1 million loss,' he suggests."

35. Ari Schwartz, a privacy expert at the Center for Democracy and Technology, called Spaltro's reasoning "shortsighted" because the cost of notification is only a small part of the potential cost to a company. Indeed, Sony reported that the 2011 PSN data breach cost the company $170 million.

36. In 2011, SPE tasked a group of employees to conduct an assessment of the company's data security practices. The assessment was designed to: (1) identify vulnerable data -- referred to as "IT assets" -- that would be embarrassing if compromised and made publicly available, including presumably NPPI and valuable intellectual property, such as the Picture, which had been entrusted to SPE and its subsidiary, SPWA; (2) identify existing security gaps with regard to protecting the implicated IT assets; and (3) recommend steps that could be taken to eliminate these security gaps. Apparently, in view of the November 2014 Data Breach, SPE, acting on its own behalf and that of its subsidiaries, including SPWA, declined to implement its own security recommendations.

37. Lockheed Martin security researchers notably publicized in March 2011 a cyberattack kill chain process, which was developed as a response to a new, sophisticated type of hacking called advanced persistent threats ("APTs") that were bypassing traditional static cyber security

tools and allowing information security professionals to proactively remediate and mitigate targeted, coordinated, purposeful, and persistent future cyber threats. The kill chain takes advantage of the seven steps a hacker must take to plan and execute a successful attack and allows companies to thwart the APT cyberattack by stopping the hacker from completing *just one* of these seven required steps. In other words, a company has several different opportunities along the kill chain to thwart an attack.

38. In 2013, the United States government and several private security research firms widely distributed reports about new types of malicious computer code that should have put SPE on notice that cyber-attacks on retailers continued to evolve.

F. SONY's Continuing Reckless and Conscious Disregard of IT Security Issues

39. Notwithstanding any of the above, SONY's security practices continued to fall below not only prudent industry standards for prevention, detection, and/or containment of APT hacking, but also traditional, static cyber-attack security standards.

40. Kevin Roose, a business and technology writer for New York magazine, reported that SPE took a "remarkably lax approach to data security," given that some of the files released in the Data Breach that contained personal employee data were "unencrypted Excel and Word files, labeled plain as day." Time Magazine reported a former employee's criticism of SPE's information security team and that SPE had largely ignored the employees' reports of security violations: "Sony's 'information security' team is a complete joke. We'd report security violations to them and our repeated reports were ignored." SPE also dedicated insufficient resources to data

security. The leaked documents show that out of 7,000 employees, only eleven were assigned to the information security team, far too few for a multi-billion dollar company with vast amounts of confidential data.

41. Just two months before the November 2014 Data Breach became public, on September 25, 2014, PricewaterhouseCoopers delivered a report of its audit of SPE's computer network. The report detailed gaps in the company's monitoring of its systems, including a firewall and more than 100 other devices that were not being monitored by the corporate security team in charge of overseeing infrastructure. The auditors found that SPE had failed to notify the corporate security team of newly added devices to monitor, including web servers and routers. PricewaterhouseCoopers warned that "[s]ecurity incidents impacting these network or infrastructure devices may not be detected or resolved timely." The report concluded that SPE "was failing to monitor 149 out of a final total of 869 systems they wished to monitor. That meant they were blind to 17 percent of their environment."

42. The leaked emails also exposed lax security practices, including Sony America and SPE CEO Michael Lynton having "routinely received copies of his passwords in unsecure emails for his and his family's mail, banking, travel and shopping accounts, [and] from his executive assistant, David Diamond." A leaked email from October 2014 reveals additional problems with SPE's computer system. David C. Hendler, SPE's CFO, complained that the company had experienced months of "significant and repeated outages due to a lack of hardware capacity, running out of disk space, software patches that impacted the stability of the environment, poor system

monitoring and an unskilled support team."

43. SPE also failed to vigilantly employ intrusion prevention and detection protocols that would have prevented and immediately detected the breach in November 2014. Some experts who have analyzed the malicious software behind the Data Breach have suggested that the hackers may have been inside SPE's network for some time, allowing them to become familiar with the network.

44. Several security firms have noted that the data released by the hackers included a number of SPE's private cryptographic keys. Kevin Bocek, vice president at Venafi, explained to BusinessWeek that losing control of these cryptographic "keys to the kingdom" is "a big deal." A hacker who has access to the cryptographic keys can access encrypted servers without triggering intrusion detection systems because these systems assume the encrypted data is safe. BusinessWeek reported that an attack using cryptographic keys indicates that the hacker likely spent a significant amount of time within the company's network. This is because companies are often slow to change their cryptographic keys, even when they are known to be vulnerable. Bocek noted that the 2011 PSN breach also compromised cryptographic keys, raising the question of why the Sony companies hadn't established greater protection for them by 2014.

45. Anyone with access to the cryptographic keys could access SPE's network until the company changed them -- a process made more difficult by the fact that SPE apparently did not appropriately track the ways that cryptographic keys are used. For example, Kaspersky Lab pointed out that a sample of the malware that hackers installed on the SPE network during the

Data Breach showed traces of being signed by a valid digital certificate from SPE. According to the cybersecurity firm:

> The stolen Sony certificates (which were also leaked by the attackers) can be used to sign other malicious samples. In turn, these can be further used in other attacks. Because the Sony digital certificates are trusted by security solutions, this makes attacks more effective. We've seen attackers leverage trusted certificates in the past, as a means of bypassing whitelisting software and default-deny policies.

46. SPE's ability to prevent further unauthorized access to its Network has been severely compromised given the hacker's access to and ability to release the cryptographic keys. In addition, ARS Technica reported that the hackers were able to collect significant intelligence on the Network from SPE's own information technology department, including lists of all computers on SPE's internal networks. Within the files publicly disclosed the second week of December 2014 was a corporate certificate authority that was intended to be used in creating server certificates for SPE's Information Systems Service (ISS) infrastructure. This corporate certificate authority may have been used to create the server certificate that was used to sign a later version of the malware that took SPE's Network offline as part of the Data Breach.

G. SONY's False Exculpations

47. SPE has claimed that the November 2014 Data Breach was "unprecedented in nature" and "undetectable by industry standard antivirus software." The actual details tell a very different story. As Adam Caudill, an independent security researcher, suggests, "[t]o protect their image, [SPE] need[s] this to be an unpreventable, incredibly sophisticated attack." But the hackers' ongoing conduct should not have remained undetected, he explains: "Even if they couldn't detect

the malware, they should have detected the unusual activity. You don't steal such a large amount of data without raising some red flags -- the question is, was anyone watching?"

48. Mike Gillepsie of Computer Weekly noted that "[t]his was a sustained attack of various visits and Sony was not aware until it was pointed out, and that is worth discussing." He added, "[o]nce the attackers had found their way in, they took time to build a picture of the network architecture and then returned at a future point to attack specific servers—stealing information and then deleting the original files with sophisticated malware." Gillepsie pointed out that a major security issue which the Data Breach exposed was the lack of "effective segregation of data," a problem that "seems to be across the corporation as the hackers were able to easily move between areas, taking whatever they picked. ... The lack of segregation of data is a very poor security hygiene and given the details released by the hackers of usernames and passwords, this was not the only neglected area of security hygiene at Sony." It is not yet known how the hackers actually breached the Network, "but once inside, Sony certainly made it easy for them to move around and take what they wanted with impunity." Philip Lieberman, the president of security management firm Lieberman Software, said: "It's obvious from the scope of what's been done that the intruders owned the entire environment . ... Sony lost control of their environment."

H. Proximately Caused Damages

49. The direct and proximate result of the foreseeable and avoidable Data Breach just four months prior SPWA's planned release of the Picture was an extreme dilution of the otherwise viable market for Plaintiff's Picture. The November 2014 Data Breach resulted in the unauthorized

release of the Picture on multiple sites worldwide and destroyed the audience demand for the Picture. Following the Data Breach and worldwide pirated release of the Picture, SPWA abandoned the social marketing plans and lost all interest in promoting and marketing the Picture since it was otherwise available for free as a result of its failure to maintain adequate security of the Network. As an isolated sample of the damage caused the anticipated video-on-demand ("VOD") revenue stream of the Picture, note that in the first six days alone following the Data Breach, the stolen Picture master was downloaded-for-free a reported 19,949 times (an average rate of over 3300 illegal, revenue-free downloads per day). See Andrew Wallenstein and Brent Lang, *Sony's New Movies Leaked Online Following Hack Attack.* http://variety.com /2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack 1201367036/.

50. The number of downloads in just six days does not take into account the exponential "spidering-effect" of one illegal download then generating by itself numerous other, untraceable downloads and each of those subsequent downloads, in turn and over time, then generating other downloads, much like a chain letter. While the total number of illegal downloads is unknown and unknowable, it is far more than likely many, many times the nearly 20,000 downloads recorded in just six days. The minimal amount of gross revenue actually generated subsequent to the Data Breach resulted in no further shared distribution revenues to Plaintiff beyond the original $800,000 advance paid by SPWA at the time of execution of the Agreement.

51. The destroyed VOD release plans also terminated any potential theatrical, television and DVD exploitation for the Picture moving forward. The net effect of the Data Breach upon

Plaintiff was not only the loss of its contracted and reasonably anticipated share of SPWA distribution revenues, but an out-of pocket-loss to Plaintiff of nearly $2.6 million in un-recouped production costs.

I. Legal Remedies under the Agreement in the Wake of SPWA Failure to Cure

52. Plaintiff proceeded under Section 16.1 of the Agreement entitled "Licensor's Remedies." See Exhibit 1, p. 21 (Bates No. 0021). That section reads as follows:

> 16.1. Licensor's Remedies. If SPWA is in breach of any of the material provisions of this Agreement, including failure to make any payment provided for herein at the time and in the manner herein required, and SPWA shall fail to cure such material breach within thirty (30) days after written notice from the other party (the "**Cure Period**") then Licensor shall be limited to bringing an action at law to recover damages, and in no event shall Licensor or a party transferring rights or rendering services in connection with the Picture, be entitled to terminate or rescind this Agreement or SPWA's rights with respect to the Picture or enjoin or restrain or otherwise interfere with SPWA's production, distribution or exhibition of the Picture or SPWA's use, publication or dissemination of any advertising issued in connection with the Picture. [Emphasis added].

53. On June 15, 2016, Plaintiff made written demand upon SPWA pursuant to Section 16.1, "that SPWA cure, within 30 days of this written notice, its failure to make appropriate payment of the amount of revenue to which Licensor would have been entitled but for your breach of the anti-piracy provisions of the Agreement. The amount of that revenue for which we seek payment, less amounts paid to date, is $8,738,331 as set forth in [the pre-suit expert report]." See Exhibit 2, attached hereto (without exhibits), p. 2 (Bates No. 0097).

54. In a letter dated July 12, 2016, SPWA rejected Plaintiff's demand to cure, denying any liability or responsibility in the matter. Furthermore, SPWA contended that any dispute would have to be resolved by way of arbitration in California pursuant to Section 16.5 of the Agreement

See Exhibit 3, attached hereto, pp. 1-3 (Bates Nos. 0102-0104). The Arbitration provision in the Agreement (Exhibit 1, p. 22) (Bates No. 0022) is set forth in Section 16.5 and reads as follows:

> Arbitration. The parties acknowledge and agree that all actions or proceedings arising in connection with, touching upon or relating to this Agreement, the breach thereof and/or scope of the provisions of this Paragraph 14.5 [sic] (a **"Proceeding"**) (whether or not relating to the Picture or to any of the matters referred to in clauses (i), (ii) and/or (iii) of Paragraph 14.4 [sic] above) shall be submitted to JAMS ("JAMS") for binding arbitration under its Comprehensive Arbitration Rules and Procedures if the matter in dispute is over $250,000 or under its Streamlined Arbitration Rules and Procedures if the matter in dispute is $250,000 or less (as applicable, the **"Rules"**) to be held solely in Los Angeles, California, U.S.A., in the English language in accordance with the provisions below.

55. The purported "mandatory" arbitration language contained in Section 16.5 of the Agreement, upon which Defendant relies (see Exhibit 3, pp. 1-2) (Bates Nos. 0101-0103), is seemingly at odds with Section 16.1-- which is neither referenced nor negated by Section 16.5-- and which permits Licensor, under prescribed circumstances, "to bring[] an action at law to recover damages." (Exhibit 1, p. 21) (Bates No. 0021). The term "bringing an action at law to recover damages" is synonymous with the initiating of judicial, not arbitral proceedings. Any seeming facial inconsistency between Sections 16.1 and 16.5 must be resolved under California general contract principles which are not violative of Section 2 of the Federal Arbitration Act ("FAA").

56. California Civil Code Section 1652 states that "repugnancy in a contract must be reconciled, if possible, by such an interpretation as will give some effect to the repugnant clauses, subordinate to the general intent and purpose of the whole contract." Here, the parties carefully laid out those disputes which were subject to mandatory arbitration and those disputes which were subject to an action at law.

57. Section 16.1, by its very terms, expressly limits judicial proceedings "to bringing an action at law to recover damages" where SPWA [and not Licensor] "is in breach of any of the

material provisions of this Agreement, including the failure to make any payment provided for herein at the time and in the manner herein required... ." [Added]. See Exhibit 1, p. 21 (Bates No. 0021). Section 16.1 disallows any judicial action where the remedy sought by Licensor is a termination or rescinding of the Agreement or any form of injunctive relief which would interfere with SPWA's distribution, exhibition or advertisement of the Picture, as opposed to "bringing an action at law to recover [monetary] damages" as expressly permitted by Section 16.1. (Bates No. 0021). Any claims by SPWA, for either monetary or injunctive relief, and any claims by Licensor for other types of non-prohibited, non-monetary relief are controlled by Section 16.5 which otherwise requires mandatory arbitration in those circumstances only. Thusly interpreted, there is no repugnancy or inconsistency between the sections.

58. Even if there were any such non-resolvable repugnancy, California law requires that the provision which first appears in the contract control over the second inconsistent provision. *Burns v. Peters*, 55 P.2d 1182, 1184 (Cal. 1936) ("The general rule is that where two clauses of a contract cannot be reconciled the first shall be received and the latter rejected."); *Estate of Cox v. Snyder*, 8 Cal. App. 3d 168, 199 (4th Dist. 1970) (quoting the California Supreme Court's decision in *Burns v. Peters*).

59. These California rules of contract interpretation are not limited to arbitration agreements but apply to any agreement and, thus, are not in violation of Section 2 of the FAA. The United States Supreme Court has repeatedly observed that "States may regulate contracts, including arbitration clauses, under general contract law principles and they may invalidate an arbitration clause 'upon such grounds as exist at law or in equity for the revocation of any contract.'" *Doctor's Associates, Inc. v. Casarotto*, 517 U.S. 681, 686 (1996) (quoting from *Allied-Bruce Terminex Coso v. Dobson*, 513 U.S. 265, 281 (1995) and 9 U.S.C. Section 2).

J. California Law of Implied Covenant of Good Faith and Fair Dealing

60. The only remedy which Plaintiff seeks in this action is payment by SPWA of the amounts which would otherwise have been earned from the full exploitation of the distribution rights exclusively held by SPWA but for its breach of one or more of the material provisions of this Agreement, most notably the anti-piracy provisions of Section 16.7. That section authorized and effectively obligated SPWA "to protect the Picture worldwide on the Internet directly or through third party vendors, representative or agents" and further stated that SPWA was "to use appropriate technical measures or other techniques, now known or hereafter devised, to assist in efforts to remove, disable or otherwise prevent unauthorized versions of the Picture on the Internet." See Exhibit 1, p. 24 (Bates No. 0024). Clearly, SPWA failed to do those things, either on its own or in reliance upon the IT safeguards of parent-agent, SPE.

61. The anti-piracy provision of the Agreement (Exhibit 1, p. 24) (Bates No. 0024) is set forth in Section 16.7 and reads in full as follows:

> Anti-Piracy Authorization. Without limiting the foregoing, Licensor hereby confirms that SPWA is authorized to protect the Picture worldwide on the Internet directly or through third party vendors, representatives or agents. Licensor hereby confirms that SPWA is authorized to use appropriate technical measures or other techniques, now known or hereafter devised, to assist in efforts to remove, disable or otherwise prevent unauthorized versions of the Picture on the Internet. If Licensor is not the owner and copyright claimant for the Picture or if Licensor is a joint owner and/or copyright claimant for the Picture, at SPWA's request, from time to time, Licensor will obtain and provide written confirmation from all owners and/or copyright claimants to the Picture, as applicable, that SPWA is authorized to protect the Picture worldwide on the Internet as described above.

62. SPWA, in its letter of July 12, 2016, incredulously contends that it had "no obligation... to take any anti-piracy measures whatsoever." See Exhibit 3, p. 3 (Bates No. 0104). While Defendant concedes that California law controls the interpretation of the Agreement, it nonetheless argues, in effect, that the "authorization" in Section 16.7 to employ anti-piracy measures did not

create the "obligation" to employ anti-piracy measures. This argument is ludicrous on its face and hardly represents the intention of the parties, a cornerstone of California contract interpretation; nor is such contention consistent with a fair reading of the Agreement. Defendant-Licensee stands in the shoes of Plaintiff-Licensor and must receive the latter's authority to protect the intellectual property from unlawful infringement over which SPWA had total control. See Section 11.1.11 of Exhibit 1, p.15 and further defined terms referenced on pp. 13, 30) ("Materials shall become the sole and exclusive property of SPWA," including, amongst other materials, all of the masters of the Picture) (Bates Nos. 0013, 0015, 0030-0047); see also Section 16.6 (Exhibit 1, p. 24) (Bates No. 0024) (providing SPWA the right to prosecute and defend actions of any nature concerning infringement or interference of any rights granted under the Agreement). Having been given that exclusive authority and control, SPWA must act in good faith and deal fairly with Plaintiff in discharging its obligations. By Plaintiff having agreed to give Defendant total control over the subject intellectual property (namely, the Picture), in an effort to achieve the common goal of both parties to the Agreement, California's implied covenant of good faith and fair dealing is implicated.

63. Any negatory interpretation by SPWA regarding its "authority" to safeguard the Picture represents a violation of well-settled California law which holds that "every contract imposes an obligation of good faith and fair dealing between the parties in its performance and enforcement. The duty embraces, among other things, an implied obligation that neither party will do anything to injure or destroy the rights of the other party to receive the benefits of the agreement." *Corona el al v. Sony Pictures Entertainment, Inc., supra*, No. 2:14-cv-09600 (Doc. 97, p. 6) (citing *Harm v. Fisher*, 181 Cal. App. 2d 405, 418 (1960)).

64. The implied covenant of good faith and fair dealing, in the words of the California Supreme Court, "finds particular application in situations where one party is invested with a discretionary power affecting the rights of another. Such power must be exercised in good faith." *Carma Devs. (Cal.) Inc. v. Marathon Dev. Cal. Inc.*, 2 Cal. 4th 342, 372 (Cal. 1992) (internal citations omitted). "In the case of a discretionary power, it has been suggested that the covenant requires the party holding such power to exercise it 'for any purpose within the reasonable contemplation of the parties at the time of formation--to capture opportunities that were preserved upon entering the contract, interpreted objectively.'" *Id.* (internal citation omitted). Thus, even assuming Defendant's interpretation of Section 16.7 is, in a vacuum, literally accurate, such interpretation is legally bankrupt and misses the mark entirely with respect to the implied covenant of good faith and fair dealing. It is beyond cavil that only SPWA and its parent-agent, SPE, were in a position to properly secure and protect the intellectual property, including the Picture, on SONY's Network. Plaintiff was totally at their mercy.

65. As set forth above, SPWA breached the implied covenant of good faith and fair dealing by having acted "consciously and deliberately in fail[ing] to maintain an adequate security system" including anti-piracy measures as envisioned by Section 16.7, the direct and proximate result of which was to unfairly frustrate the agreed-upon, common purpose of the Agreement with Plaintiff-Licensor which was to maximize revenue from the lawful distribution of the Picture, free from any market-diluting infringements. Cf. *Corona, supra*, No. 2:14-cv-09600 (Doc. 97, p. 6).

66. Here, an express, written and executed contract, along with the implied covenant of good faith and fair dealing, existed between the parties: there was mutual assent; consideration; legal capacity of both parties; and a lawful subject matter. Furthermore, all conditions precedent to the filing of this action have been performed or otherwise waived.

COUNT ONE
BREACH OF EXPRESS MATERIAL TERMS OF THE CONTRACT

67. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 66 above, as though more fully stated herein.

68. Defendant breached one or more express material terms of the contract.

69. Defendant breached the implied covenant of good faith and fair dealing.

70. As a proximate result of Defendant's material breach, Plaintiff suffered significant monetary damages and seeks recovery thereof.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests this Court to award it all appropriate relief including, but not limited to:

(a) any and all actual, compensatory damages;

(b) pre-and post judgment interest as may be authorized by law;

(c) reasonable attorney fees and costs to the extent permitted under the Agreement; and

(d) any such further relief as may be just and fair.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury on all issues so triable as a matter of right.

Respectfully submitted,
NeJame Law, P.A.

By: *s/ Stephen J. Calvacca*
Florida Bar No. 561495
189 S. Orange Avenue
Suite 1800
Orlando, Florida 32801
Telephone: (407) 500-0000
Facsimile: (407) 245-2980

civilservice@nejamelaw.com
stephen@nejamelaw.com
darlene@nejamelaw.com

W. Edward McLeod, P.A.

By: *s/ W. Edward McLeod*
Florida Bar No. 871419
P.O. Box 917412
Longwood, Florida 32791
Telephone: (407) 862-5572
Facsimile: (407) 917-210-3950
nedmcleodesq@gmail.com
Attorneys for Plaintiff