

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

JON HART, on behalf of himself and all others
similarly situated,

Plaintiff,

v.

WARNER MUSIC GROUP, CORP., a Delaware
corporation

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jon Hart, individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, by and through the undersigned counsel, hereby brings this Class Action Complaint against Defendant Warner Music Group, Corp., (“WMG” or “Defendant”), and alleges as follows:

INTRODUCTION

1. Warner Music Group, Corp., is a New York based multinational entertainment and recording label conglomerate and the third largest company in the global music industry with revenues of nearly \$4.5 billion.

2. As an essential part of its billion-dollar business, WMG operates and maintains a number of e-commerce websites throughout the United States. WMG sells its products and services through these sites, all of which use a payment system designed and maintained by WMG.

3. On or about September 2, 2020, WMG began notifying various state Attorneys General, including the California Attorney General, that unauthorized third parties compromised an undisclosed number of WMG’s U.S.-based e-commerce websites, from approximately April 25, 2020 to August 5, 2020 (the “Data Breach”). WMG’s e-commerce websites are serviced through an external provider.

4. Around the same time, WMG also began sending notices to customers who may have made purchases on one of their e-commerce sites during the aforementioned time period that their Personally Identifiable Information (“PII”) was potentially acquired by an unauthorized third party. The PII includes name, email address, telephone number, billing and shipping address, and payment card details (card number, three-digit verification code, and expiration date).

5. Due to WMG’s failure to safeguard its customers’ PII, Plaintiff and Class Members have suffered irreparable harm and are subject to an increased risk of identity theft.

Plaintiff and Class Members must now take additional security measures to minimize the risk of identity theft.

JURISDICTION AND VENUE

6. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant to establish minimal diversity.

7. The Southern District of New York has personal jurisdiction over WMG because WMG is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

8. Venue is proper in this District under 28 U.S.C. §1391(b) because WMG is headquartered in this District and a substantial amount of the WMG's conduct harming Plaintiffs and Class Members originated from this District.

PARTIES

9. Plaintiff Jon Hart resides in Sausalito in the State of California.

10. Plaintiff Hart purchased music and other goods from WMG's e-commerce websites between April 25, 2020 and August 5, 2020.

11. Defendant Warner Music Group, Corp. is a Delaware Corporation headquartered in New York, New York. Its principal place of business is at 1633 Broadway, New York, NY 10019.

FACTUAL BACKGROUND

12. WMG is one of the largest and most profitable music-entertainment and recording label conglomerates in the world. Based in New York City, WMG represents over 60,000 artists and has operations in more than 50 countries.

13. WMG operates thousands of websites through which its customers purchase music and music-related merchandise. Plaintiff and Class Members used such platforms for their

purchases. When making purchases on Defendant's website, customers must enter their PII. Plaintiff and Class Members had a reasonable expectation that WMG would keep that PII safe and secure.

14. As a sophisticated multi-billion dollar entity, WMG had both the duty and the financial resources to provide secure platforms for its customers to make purchases.

15. On or about September 2, 2020, Plaintiff and Class Members were notified their PII had been stolen in a "months-long magecart¹ style attack." The compromised PII includes "name, email address, telephone number, billing and shipping address, and payment card details (card number, CVC/CVV and expiration date)" according to the Notice of Data Breach submitted to the Office of the Attorney General for the State of California.²

16. Since the breach, WMG has been unwilling to voluntarily disclose to Plaintiff and Class Members which of its sites were impacted by the Data Breach, making it difficult for Plaintiff and the Class Members to mitigate any harm resulting from the theft of their PII. "When asked, the WMG spokesperson declined to name the e-commerce sites affected in the attack, saying that the company 'isn't commenting further than the statement.'"³

17. Not only is WMG unwilling to disclose which of its e-commerce sites were impacted, but it waited almost an entire month before notifying Plaintiff and Class Members that they may have been victims of the Data Breach. As a result of this delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and it gave the hackers time to use the stolen PII without restriction, further harming Plaintiff and Class Members.

¹ "Magecart" refers to a loose affiliation of hackers/identity thieves that specialize in cyberattacks involving digital credit card theft by skimming online payment forms. These hackers then proceed to sell payment card information on the dark web.

² Warner Music Group Notice of Data Breach, Office of the Attorney General for the State of California, available at https://oag.ca.gov/system/files/California_Consumer%20Letter.pdf (last accessed October 22, 2020).

³ See Gatlan, S. *Warner Music Group finds hackers compromised its online stores*, Sep. 3, 2020, accessible at: <https://www.bleepingcomputer.com/news/security/warner-music-group-finds-hackers-compromised-its-online-stores/> (last accessed October 21, 2020).

18. According to FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." However, WMG did not rapidly report to Plaintiff and Class Members that their PII had been stolen because it took WMG almost four weeks to notify them.

19. WMG failed to utilize reasonable security procedures and practices to detect data intrusions, which allowed hackers to steal payment and personal information for approximately four months without internal detection. The extremely long duration of the data breach without any detection by WMG shows WMG's data security practices were and are grossly inadequate.

20. Once unauthorized third parties obtain access to WMG's customers' PII, hackers can then sell stolen PII on the "dark web."⁴ PII is highly valuable to criminals and stolen bank details can be sold on the dark web for up to \$200.⁵

21. By obtaining victim's PII, hackers and identity thieves can gain access to a number of the victim's accounts—such as bank, social media, and email accounts. Additionally, stolen PII is often used to open new financial accounts in the victim's name, incur charges in the name of Plaintiff and Class Members, close credit and debit cards, and other unauthorized activities.

22. Victims of identity theft can often suffer extensive financial harms, including unauthorized charges to accounts, tax fraud, and damage to credit score and reports. Additionally, victims of identity theft must also remain vigilant for years after their PII was stolen to protect themselves from future identity theft.

Plaintiff's Experience

23. Plaintiff purchased music and merchandise from multiple WMG e-commerce sites between April 25, 2020 and August 5, 2020 using his credit and debit cards.

⁴ The "dark web" refers to a heavily encrypted part of the Internet that is not accessible to traditional search engines. Law enforcement has difficulty in policing the "dark web" due to the heavy encryption, which allows users to conceal identities and online activity.

⁵ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Oct. 22, 2020).

24. In mid- September 2020, Plaintiff received a Notice of Data Breach from Warner Music Group dated September 3, 2020, which indicated his PII had been acquired by an unauthorized party.

25. Since that time, Plaintiff has spent time reviewing his past and current credit and debit card statements as well as related bank account information looking for irregular and fraudulent transactions. Plaintiff has expended significant time and energy on these endeavors.

CLASS ACTION ALLEGATIONS

26. Plaintiff brings this lawsuit as a class action on behalf of himself and all others similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), 23 (b)(2), 23(b)(3), and 23(c)(4).

27. Plaintiff seeks to represent a proposed nationwide class defined as follows:

All individuals residing in the United States who made purchases on Defendant's e-commerce websites between April 25, 2020 and August 5, 2020.

28. Excluded from the proposed classes is Defendant, including any entity in which Defendant has a controlling interest, is a subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

29. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

30. **Numerosity:** Plaintiff is unable to state the precise number of potential members of the proposed Class because that information is in the possession of Defendant. However, the number of Class members is so numerous that joinder would be impracticable for purposes of Rule 23(a)(1). The exact size of the proposed Class and the identity of its members will be readily ascertainable from the business records of Defendant. Further, the disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties

and to the Court. The Class members are readily identifiable from information and records in Defendant's possession, custody, or control.

31. **Typicality:** Plaintiff asserts claims that are typical of the claims of the entire Class for purposes of Rule 23(a)(3). Plaintiff and all members of the Class have been subjected to the same wrongful conduct because they all had their PII compromised as a result of the Data Breach due to WMG's inadequate security measures. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff.

32. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class Members. These include:

- a. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;
- b. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other class members to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;
- d. Whether Plaintiff and the Class have suffered benefit of the bargain losses because of the Data Breach;
- e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised by an unauthorized party;
- f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- g. Whether Defendant has been unjustly enriched;

- h. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- i. Whether Plaintiff and the other Class Members are entitled to injunctive, equitable and monetary relief.

33. These issues not only predominate, but they are also appropriate for issue certification under Rule 23(c)(4).

34. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

35. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members. Additionally, Plaintiff has retained counsel experienced in complex class action litigation. Class Members' interests will be fairly and adequately protected by Plaintiff and his counsel.

36. **Superiority:** Proceeding as a class action provides substantial benefits to both the parties and the Court because this is the most efficient method for the fair and efficient adjudication of the controversy. Plaintiff and Class Members have suffered and will suffer irreparable harm and damages as a result of Defendant's wrongful conduct. Because of the nature of the individual Class Members' claims, few, if any, could or would otherwise afford to seek legal redress against Defendant for the wrongs complained of herein, and a representative class action is therefore appropriate, the superior method of proceeding, and essential to the interests of justice insofar as the resolution of Class members' claims are concerned. Even if separate actions could be brought by individual members of the Class, the resulting multiplicity of lawsuits would cause undue hardship, burden and expense for the Court and the litigants, as well as create a risk of inconsistent rulings which might be dispositive of the interests of the

other members of the Class who are not parties to the adjudications or may substantially impede their ability to protect their interests.

CHOICE OF LAW

37. The WMG Terms of Service provide that all users “hereby agree that this Agreement (and any claim or dispute arising in connection with this Agreement or your use of the Site) is governed by and shall be construed in accordance with the laws of the State of New York, U.S.A., without regard to its principles of conflicts of law...” Thus, New York law applies to the claims of all Class Members regardless of their state of residence.

UNCONSCIONABILITY OF DISCLAIMER

38. The WMG Terms of Use contain a purported disclaimer of liability and damages that is both procedurally and substantively unconscionable. It provides:

WE, OUR AFFILIATES AND OUR RESPECTIVE ARTISTS, REPRESENTATIVES AND PROVIDERS WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES OF ANY KIND IN CONNECTION WITH THE SITE, NOR FOR ANY DAMAGES FOR LOSS OF PROFITS, LOSS OR INTERRUPTION OF BUSINESS, LOSS OF USE, LOSS OF DATA, LOSS OF OTHER INTANGIBLES, LOSS OF SECURITY OF INFORMATION YOU HAVE PROVIDED IN CONNECTION WITH YOUR USE OF THE SITE (INCLUDING, WITHOUT LIMITATION, IN CONNECTION WITH YOUR USE OR RECEIPT OF ANY THIRD PARTY APPLICATIONS OR THIRD PARTY CONTENT), OR UNAUTHORIZED INTERCEPTION OF ANY SUCH INFORMATION BY THIRD PARTIES, EVEN IF ADVISED IN ADVANCE OF SUCH DAMAGES OR LOSSES. FURTHER, WE, OUR AFFILIATES AND OUR RESPECTIVE ARTISTS, REPRESENTATIVES AND PROVIDERS WILL NOT BE LIABLE FOR DAMAGES OF ANY KIND RESULTING FROM YOUR USE OF THE SITE OR FROM ANY THIRD PARTY APPLICATIONS, THIRD PARTY CONTENT, INFORMATION OR MATERIALS ON THE SITE. YOUR SOLE AND EXCLUSIVE REMEDY FOR DISSATISFACTION WITH THE SITE IS TO STOP USING THE SITE. OUR MAXIMUM LIABILITY FOR ALL DAMAGES, LOSSES AND CAUSES OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE) OR OTHERWISE SHALL BE THE TOTAL AMOUNT PAID BY YOU TO US TO ACCESS AND USE THE SITE.

IT IS POSSIBLE THAT APPLICABLE LAW MAY NOT ALLOW FOR LIMITATIONS ON CERTAIN IMPLIED WARRANTIES OR EXCLUSIONS OR LIMITATIONS OF CERTAIN DAMAGES; SOLELY TO THE EXTENT THAT SUCH LAW APPLIES TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.

39. By its own terms, the disclaimer of liability does not apply to direct damages. And to the extent the Terms of Use purports to exempt consequential damages and damages relating to “loss of security of information you have provided,” and to the extent the damage limitation purports to eliminate damages or limit them to the amount the Class members paid to use the site, the Terms of Use are “so grossly unreasonable or unconscionable in the light of the mores and business practices of the time and place as to be unenforceable... according to [their literal terms.]”

40. These provisions of the Terms of Use are procedurally unconscionable because they are buried in an adhesion contract foisted on Class members with no opportunity to negotiate. They are also substantively unconscionable because they create an unfairly one-sided allocation of risk and are not commercially reasonable. No Class member signing up for any WMG service can be fairly expected to understand and agree that he or she is purportedly waiving any right to remedies for a “loss of security of information you have provided...”

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

41. Plaintiff re-alleges and incorporates by reference all allegations in this Complaint as though fully set forth herein.

42. To use the WMG’s services, customers, including Plaintiff and the Class, were obligated to provide their PII, including personal and payment card information.

43. WMG owed a duty to Plaintiff and the other Class members to exercise reasonable care in safeguarding and protecting their PII from unauthorized third parties.

44. WMG had a duty to protect Plaintiff and other Class members’ PII that was in its possession from being compromised, lost, stolen, misused, or disclosed to unauthorized parties. At a minimum, this includes designing, maintaining, and testing its security systems to ensure that Plaintiff’s and the other Class Members’ PII was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

45. WMG also had a duty to disclose to Plaintiff and the other Class Members that their PII had been or was reasonably believed to have been compromised in a timely manner. Timely disclosure was appropriate, given the sensitivity of the compromised information, so that Plaintiff and the other Class Members could take appropriate measures to cancel or change usernames, pin numbers, and passwords on compromised accounts, begin monitoring their accounts for unauthorized access, contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions.

46. WMG had a duty to employ proper procedures to prevent the unauthorized collection and dissemination of the PII of Plaintiff and Class members.

47. Plaintiff and the Class entrusted their PII to WMG through use of its websites. WMG had a special relationship with Plaintiff and the Class and had a duty to safeguard the PII of Plaintiffs and Class members, given that the PII was within WMG's possession or control.

48. Plaintiff and the Class purchased music and merchandise from WMG and agreed to provide their PII with the understanding that WMG would take appropriate measures to protect it and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. WMG did not. In fact, WMG not only knew its data security was inadequate, it also knew it did not even have the tools to detect and document intrusions or exfiltration of PII. WMG is morally culpable given its wholly inadequate safeguards and refusal to notify Plaintiff and the Class of its security vulnerabilities.

49. WMG breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiff's and the other Class members' PII stored by Defendant; and failing to recognize and stop the breach in a timely manner.

50. WMG also breached its duty to timely disclose that Plaintiff and the other Class members' PII had been, or was reasonably believed to have been, stolen or compromised.

51. WMG's failure to comply with industry regulations and the delay between the first vulnerability date and the date WMG informed users of the data breach is additional evidence of WMG's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII.

52. But for WMG's wrongful and negligent breach of its duties owed to Plaintiff and the other Class members, their PII would not have been compromised, stolen, and viewed by unauthorized persons.

53. Defendant knew or should have known that its systems and technologies for processing and securing Plaintiff's and the other Class Members' PII had security vulnerabilities.

54. WMG's failure to exercise reasonable care in safeguarding and protecting Plaintiff and the other Class Members' PII created a foreseeable risk of harm to Plaintiff and Class Members.

55. As a direct and proximate result of WMG's negligence, Plaintiff and the other Class Members suffered economic damages, including expenses to mitigate the potential harm from their stolen PII; credit monitoring; loss of use and value of their debit and/or credit cards; lost opportunity costs associated with their efforts to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; costs associated with placing freezes on credit reports; the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and expectation damage.

56. These injuries were reasonably foreseeable given the history of security breaches of this type.

COUNT II

**Violations of New York Consumer Law for Deceptive Acts and Practices
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)**

57. Plaintiff re-alleges and incorporates by reference all allegations in this Complaint as though fully set forth herein.

58. New York's Uniform Deceptive Trade Practices Act, Gen. Bus. Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

59. Plaintiff and the Class Members provided their PII to Defendant WMG as a part of transactions in business, trade, or commerce as defined in § 349. Defendant's actions as described herein constituted "consumer-oriented conduct" under § 349.

60. As outlined above, WMG engaged in deceptive acts and practices in the conduct of its business and in the furnishing of its services, including failing to implement adequate data security measures, failing to protect Plaintiff's and the Class Members' PII from theft, failing to advise Plaintiff and the Class Members of its inadequate data security, and failing to timely notify Plaintiff and the Class Members of the breach.

61. WMG misrepresented, by both affirmative conduct and by omission, the safety of its website platforms and services, particularly the security of such systems, and its ability to safely store Plaintiff's and the Class members' PII.

62. These acts and omissions were materially misleading. WMG's continued non-compliance with data security practices affected a broad group of individuals, including Plaintiff and the Class.

63. Plaintiff and the Class Members relied on WMG to safeguard their PII when they provided it to WMG and relied on WMG's deceptive acts and practices when they provided that PII in exchange for WMG's goods and services.

64. Plaintiff and the Class would not have provided their PII if they knew that WMG failed to maintain sufficient security systems to keep their PII safe and secure from hackers and identity thieves.

65. As a direct and legal result of WMG's deceptive acts and practices, Plaintiff and the Class Members have suffered concrete and ascertainable damages as alleged above.

66. Plaintiff brings this action on behalf of himself and the Nationwide Class under § 349(h) of the New York General Business Law for actual or statutory damages and treble damages as permitted by law.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

67. Plaintiff re-alleges and incorporates by reference all allegations in this Complaint as though fully set forth herein.

68. WMG solicited Plaintiff and the Class Members to make purchases through WMG's e-commerce platforms using credit and debit cards. Through this operation, WMG was making an offer to Plaintiff and the Class Members that included the implied promise to safely and securely maintain the PII provided by Plaintiff and the Class members in their commercial transactions with WMG and its affiliates.

69. Plaintiff and the Class Members accepted WMG's offer when they agreed to purchase goods or services from WMG and its affiliates through their e-commerce platform. At the time of acceptance, an implied contract was formed between Plaintiff and the Class Members and Defendant WMG that included WMG's implied promise to protect any PII provided by Plaintiff and the Class Members.

70. WMG breached these implied contracts by failing to keep the PII provided by Plaintiff and the Class Members safe and secure, as described above.

71. As a result of the breach of these implied contracts by WMG, Plaintiff and the Class Members suffered the economic damages described above.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

72. Plaintiff re-alleges and incorporates by reference all allegations in this Complaint as though fully set forth herein.

73. Plaintiff and the Class Members conferred benefits on Defendant WMG by purchasing goods or services through WMG's e-commerce platforms and provided WMG with their PII and payment information.

74. Defendant has knowledge of such benefits.

75. Defendant voluntarily accepted and retained the benefits conferred, resulting in inequity.

76. WMG has been unjustly enriched in retaining the revenues derived from Plaintiff's and the Class Members' purchases through WMG's e-commerce platforms and has failed to provide adequate data security for Plaintiff's and Class Members' valuable PII.

77. Defendant WMG failed to provide Plaintiff and the Class with full compensation in exchange for their PII, which WMG obtained through inequitable means because WMG failed to disclose its inadequate data security practices.

78. Retention of the revenues derived from Plaintiff and the Class is unjust and inequitable.

79. This claim is pled in the alternative in the event Plaintiff and the Class Members do not have an adequate remedy at law.

80. As a direct and proximate result of WMG's unjust enrichment, Plaintiff and the Class Members are entitled to restitution or disgorgement in an amount to be proved at trial.

COUNT V
Negligence per se
(On Behalf of Plaintiff and the Class)

81. Plaintiff re-alleges and incorporates by reference all allegations in this Complaint as though fully set forth herein.

82. Section 5 of the FTC Act prohibits “unfair...practices in or affecting commerce,” including the unfair act of failing to have adequate data security measures to protect PII.

83. Defendant WMG violated Section 5 by not complying with applicable industry standards and continually failing to have proper measures in place to protect the PII of Plaintiff and the Class Members.

84. Section 5 of the FTC Act was intended to guard against the harm that occurred as a result of the Data Breach and Plaintiff and the Class Members are among the class of persons Section 5 was designed to protect. As a result, Defendant WMG is negligent *per se*.

85. As a direct and proximate result of WMG’s negligence *per se*, Plaintiff and the Class Members suffered the damages described above and will continue to suffer other economic and non-economic injuries as a result of WMG’s practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

- a. certifying the Class as defined herein, and appointing Plaintiff and his Counsel to represent the Class;
- b. finding that Defendant engaged in the unlawful conduct as alleged herein;
- c. enjoining Defendant’s conduct and requiring Defendant to implement proper data security practices;
- d. awarding Plaintiff and the other Class members damages;
- e. requiring Defendant to rectify all damages caused by its misconduct;
- f. awarding Plaintiff and the other Class members pre-judgment and post-judgment interest on all amounts awarded;
- g. awarding Plaintiff and the other Class members reasonable attorneys’ fees, costs, and expenses; and
- h. granting such other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands that this matter be tried before a jury.

Dated:

Respectfully submitted,

CALCATERRA POLLACK LLP

/s/ Janine Pollack

Janine Pollack
Calcaterra Pollack LLP
1140 Avenue of the Americas, 9th Flr.
New York, NY 10036
212/899-1765 (Direct)
332/206-2073 (Fax)
www.calcaterrapollack.com

LEXINGTON LAW GROUP

Eric S. Somers, (*PHV application forthcoming*)
Mark N. Todzo, (*PHV application forthcoming*)
Meredyth Merrow, (*PHV application forthcoming*)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, CA 94117
Telephone: (415) 913-7800
Facsimile: (415) 759-4112
esomers@lexlawgroup.com
mtodzo@lexlawgroup.com
mmerrow@lexlawgroup.com

Attorneys for Plaintiff
JON HART