UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No.: 18-cv-61836

JEFFERY ROBERTS, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

COMPLYRIGHT, INC., a Minnesota corporation,

Defendant.
_____/

CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiff JEFFERY ROBERTS ("Plaintiff"), by and through his attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant COMPLYRIGHT, INC. ("Defendant"), a Minnesota corporation, and make the following allegations based upon knowledge as to himself and his own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This is a class action brought by Plaintiff individually and on behalf of all other individuals similarly situated whose personal information, including names, addresses, phone numbers, email addresses, and social security numbers (hereinafter "Personal Information" or "PI") was stolen from Defendant's computer servers beginning on or around April 20, 2018, and lasting until May 22, 2018 (the "Data Breach").

2. Defendant is a cloud-based human resources and tax preparation company whose services are used by thousands of organizations and businesses.

3. Defendant held itself out as an entity that had implemented several layers of data protection.

4. Contrary to these claims, however, Defendant did not adequately safeguard the data entrusted to it. Instead, Defendant's failure to implement and maintain adequate data security measures for its customers' information, including the PI, directly and proximately caused injury to Plaintiff and the Class as defined below.

5. On July 13, 2018, Defendant sent letters to Plaintiff and Class Members informing them that their Personal Information had been accessed and viewed by unauthorized individuals while being maintained on Defendant's Website. The letter further stated that Plaintiff's and Class Members' PI "may have been downloaded or otherwise acquired, by an unauthorized user." The letter admits that the Data Breach occurred from April 20, 2018 to May 22, 2018, but it may have gone on much longer.

6. The Data Breach was caused by Defendant's inadequate data security measures and failure to implement and maintain reasonable security measures to properly protect sensitive PI.

7. As a result of Defendant's misconduct, a massive amount of information was stolen from Defendant. The Data Breach compromised the Personal Information of hundreds of thousands of Personal Information entrusted to it. Victims have had their PI compromised, their privacy violated, an increased risk of exposure to fraud and identity theft, a loss of control over their personal and financial information, and have otherwise been injured.

8. Customers like Plaintiff seek damages caused by Defendant's negligence, breach of implied contract, breach of fiduciary duty, and violations of state consumer protection statutes.

Plaintiff further seeks injunctive and declaratory relief on behalf of himself and similarly situated Class Members.

PARTIES

9. Plaintiff Jeffery Roberts is an adult over the age of eighteen. He is a resident of New Port Richey, Florida. On or about July 17, 2018, Plaintiff received a letter from Defendant informing him that Defendant was subject to a "recent security incident involving some of [his/her] Personal Information that was maintained on [Defendant's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user" including his "name, address, telephone number, email address, and Social Security number." As a result of Defendant's failure to adequate safeguard Plaintiff's Personal Information, Plaintiff has been injured.

10. Defendant ComplyRight is a Minnesota corporation with a principal executive office at 1725 Roe Crest Drive, North Mankato, Minnesota 56003. Defendant lists its "main office" in Florida at 3300 Gateway Drive, Pompano Beach, Florida 33069. Defendant offers a variety of legal compliance and human resources services for businesses to ensure that they comply with federal, state, and local employment laws.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant because Defendant is authorized to do business and does conduct business in Florida, maintains its "main office" in Pompano Beach, Florida, and has sufficient minimum contacts with this state and/or sufficiently avail itself of the markets of this state through the promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

13. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant does business in this District, has intentionally availed itself of the laws and markets within this District by maintaining an office and conducting substantial business in this District, and a significant portion of the facts and circumstances giving rise to this Complaint occurred in or emanated from this District.

FACTUAL ALLEGATIONS

A. Defendant's Background

14. Defendant offers a suite of legal compliance and human resources services for small businesses. On its website, it states: "At ComplyRight, our mission is to free employers from the burden of tracking and complying with the complex web of federal, state, and local employment laws, so they can stay focused on managing and growing their businesses."[1] Defendant claims that it, among other things, "talk[s] to employers every day," "track[s] federal, state and local regulatory activity," and "consult[s] with [its] in-house legal research team to understand how employment regulations affect employers day-to-day." Its services range "[f]rom hiring and training, to time tracking and recordkeeping, to labor law posting and tax information reporting…."

[1] https://www.complyright.com/about/who-we-are (last accessed Aug. 1, 2018).

15. On its website, Defendant advertises that maintaining its customers' security is one of its top priorities. Indeed, on its Tax Solutions Products page,[2] Defendant states that it is "Tackling Security From Every Angle," and "take[s] a multi-pronged approach to data protection":

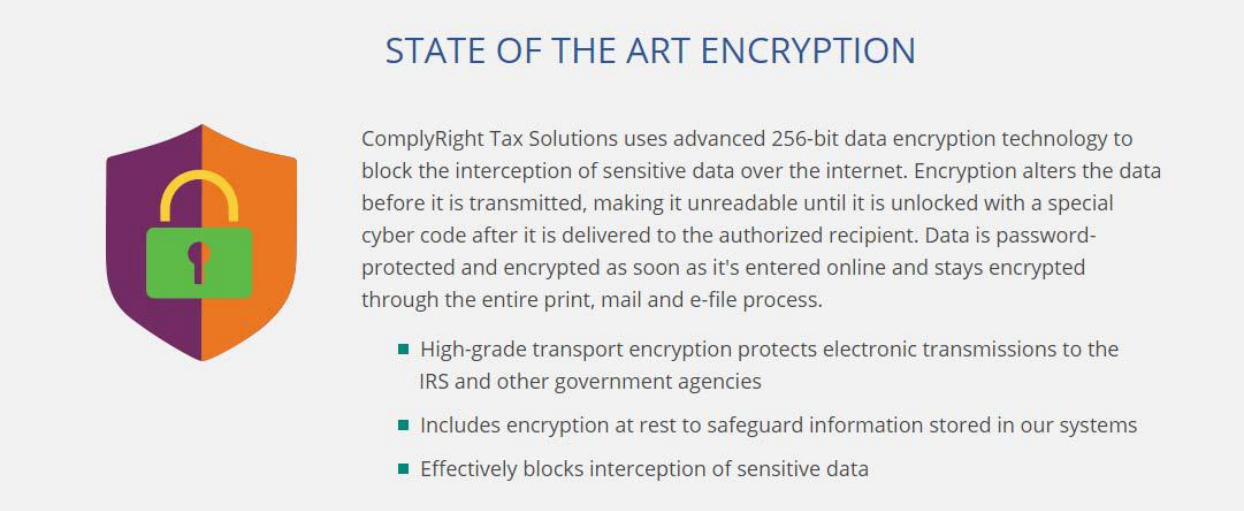
16. On its "Security Standards" page,[3] Defendant touts that it "employ[s] the latest, most sophisticated technologies and best practices to ensure [that] your sensitive data is protected end-to-end. These exacting measures and adherence to strict security standards ensure a superior level of data security and protection."

17. Such "exacting measures and adherence to strict security standards" Defendant asserts to keep its customers' data safe include "State of the Art Encryption":[4]

[2] https://www.complyright.com/products/tax-solutions (last accessed Aug. 1, 2018).

[3] https://www.complyright.com/products/security (last accessed Aug. 1, 2018).

[4] *Id.*



18. Another measure Defendant boasts to customers to "ensure a superior level of data security and protection" includes "SOC Certification"[5]:

19. Defendant also claims that it is HIPAA compliant[6]:

[5] *Id.*

[6] *Id.*

20. Despite the assurances and security practices enumerated above, which Defendant claims it met, Defendant failed to adequately protect Plaintiff's and Class Members' Personal Information.

B. <u>The Data Breach</u>

21. In late May 2018, Defendant was alerted that it had suffered from a criminal cyberattack, in which the Personal Information of employees of its various business customers was accessed and/or obtained by unauthorized persons, including but not limited to their names, addresses, phone numbers, email addresses, and social security numbers. News outlets reported that the Data Breach occurred between April 20, 2018 and May 22, 2018.[7]

22. However, it was not until July 13, 2018 that Defendant sent a letter out to Plaintiff and others, stating in part:

[7] *See, e.g.*, *Human Resources Firm ComplyRight Breached*, KREBS ON SECURITY (July 19, 2018, 5:08 PM), https://krebsonsecurity.com/2018/07/human-resources-firm-complyright-breached/; Ron Hurtibise, *Pompano-based HR services company says clients' personal info accessed in data breach*, SUN SENTINEL (July 18, 2018, 12:00 PM), http://www.sun-sentinel.com/business/fl-bz-complyright-data-breach-20180718-story.html.

> We are writing with important information about a recent security incident involving some of your personal information that was maintained on our website. Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2. We wanted to provide you with information regarding the incident, share the steps we have undertaken since discovering the incident, and provide guidance on what you can do to protect yourself.
>
> *What Happened?*
>
> On or about May 22, 2018 we initially learned of a potential issue involving our website. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website.
>
> *What We Are Doing*
>
> In addition, we commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to our website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of our website, and analysis of potentially impacted individuals, on June 14, 2018 we discovered that some of your personal information was accessed and/or viewed. Although the forensic investigation determined that your information was accessed and/or viewed on the website, it could not confirm if your information was downloaded or otherwise acquired by an unauthorized user. We are not aware of any report of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution we wanted to make you aware of the incident.
>
> *What Information Was Involved?*
>
> Your personal information that was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user included your name, address, telephone number, email address, and Social Security number.

23. And, it was not until July 18, 2018 that Defendant posted on its website the following "ComplyRight Data Security Incident Notice"[8] (the "Notice"), which states in part as follows:

> ComplyRight was the victim of a criminal cyberattack. In late May 2018, ComplyRight was alerted to a potential issue affecting the tax form preparation

[8] https://www.complyright.com/data-security-notice (last accessed Aug. 1, 2018).

websites[9] using our platform. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website. In consultation with third-party forensic cybersecurity experts, we took swift action to secure the data of our partners, business customers and the individuals potentially impacted.

The forensic investigators concluded that there was unauthorized access to our website resulting in compromise of Personal Information for some individual recipients of tax forms such as 1099 or W-2 forms. Although the forensic investigation determined the information was accessed and/or viewed, the investigators were unable to confirm whether the information was downloaded or otherwise acquired by the unauthorized user.

24. Defendant further described the Data Breach as follows:[10]

What happened?

On May 22, 2018, ComplyRight initially learned of a potential issue involving our tax reporting web platform. After investigation, we concluded that a criminal cyberattack had targeted some of the Personal Information maintained on the websites using our platform.

How did this happen?

The investigation determined there was unauthorized access to the ComplyRight web platform that is used by various websites to prepare tax-related forms for individuals (for example, 1099 and W-2 forms). Upon learning of the issue, we disabled the platform, remediated the issue on the website, and commenced a prompt and thorough investigation using external cybersecurity professionals to determine who was potentially affected and what information was accessed or viewed. Although the investigation determined the information was accessed and/or viewed, it could not confirm if the information was downloaded or otherwise acquired by an unauthorized user.

Who is affected?

[9] Defendant does not detail what "tax form preparation websites" were involved in the Data Breach. However, one of Defendant's "family of brands" includes the website efile4biz.com, a "leading IRS-authorized e-file provider" that "offers comprehensive front-to-back process of tax information returns" and is "certified by the American Institute of Certified Public Accountants (AICPA) to be SOC2-compliant, ensuring that the sensitive data you entrust us is guarded against tampering and identity theft using the latest technologies and stringent business practices." *See About Us*, efile4biz.com, at https://www.efile4biz.com/about-us.html (last visited Aug. 2, 2018).

[10] https://www.complyright.com/data-security-notice.

> A portion (less than 10%) of individuals with tax forms prepared on the ComplyRight web platform were impacted by this incident. All affected individuals have been sent notifications via U.S. Mail to their last known addresses. This letter included information to help safeguard them against identity fraud, including 12 months of free credit monitoring and identity theft protection services through TransUnion.
>
> **What information was involved?**
>
> The investigation confirmed that the portion of the website that was accessed contained names, addresses, phone numbers, email addresses, and Social Security numbers of individual tax form recipients.
>
> **Why did I receive a letter from ComplyRight?**
> ComplyRight provides a web platform used by a number of different tax form preparation websites. On behalf of those organizations and our clients, we executed the communication plan to advise those affected as promptly as possible. This is not a scam, and we apologize for any confusion that may have arisen due to your lack of familiarity with our company.
>
> **Why did ComplyRight have my information?**
>
> Tax reporting forms (such as 1099s or W-2s) sent to you were prepared on a site using the ComplyRight web platform.
>
> **How am I affected if I am a site user or employer (payer)?**
>
> The investigation found no evidence that any user or payer information was compromised. No credit card or bank account information of users or payers was involved.

25. Based on the foregoing, upon information and belief, Plaintiff's and Class Members' Personal Information was stolen, acquired, accessed, downloaded, and/or viewed by unauthorized persons from Defendant's website.

26. The link to the Notice is not found anywhere on Defendant's homepage. A customer could find this information only by scouring Defendant's website and finding a link to the Notice on its "Newsroom" page.[11]

[11] https://www.complyright.com/about/newsroom

27. Furthermore, Defendant withheld disclosure of the Data Breach from Plaintiff and Class Members for nearly two months. The letter and Notice are insufficient to comply with Defendant's obligations to provide adequate and timely notification of the Data Breach.

28. While Defendant states in its Notice that "less than 10% … were impacted," in its notice of breach to the Wisconsin Department of Agriculture, Trade and Consumer Protection, Defendant states that 662,000 individuals were affected by the Data Breach.[12]

29. Although Defendant is offering impacted individuals complimentary 12-month credit monitoring and identity protection services, that does not sufficiently protect those individuals from the number of threats such data breaches impose and is not long enough to eliminate all potential damage from the Data Breach.

30. Indeed, Defendant concedes that consumers will be subjected to continued, future risk of identity theft and other damages, stating in its letters informing consumers of the Data Breach that consumers must "remain vigilant in reviewing … financial account statements and credit reports for fraudulent and irregular activity."

C. Industry Standards, Identity Theft, and Protection of Personal Information

31. It is well known that customer Personal Information is an invaluable commodity and a frequent target by hackers. However, despite this widespread knowledge and industry alerts regarding other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached.

32. According to Javelin Strategy & Research, in 2017 alone, over 16.7 million individuals have been affected by identity theft, causing $16.8 billion stolen.[13]

[12] *Data Breaches*, STATE OF WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION, https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx (last accessed Aug. 1, 2018).

33. Defendant is, and at all relevant times has been, aware that the PI it maintains is highly sensitive and could be used for illegal purposes by third parties. Indeed, Defendant's website pages acknowledge that its customers expect adequate safeguards of their employees' Personal Information.

34. Consumers place a high value not only on their PI, but also on the privacy of that data. That is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[14]

35. This is especially the case with social security numbers, the "secret sauce" that is "as good as your DNA to hackers."[15] There are long-term consequences to data breach victims whose social security numbers are taken and utilized. However, Plaintiff and Class Members would not be able to obtain a new number unless they become a victim of social security number misuse. And, even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[16]

36. In light of the multiple high-profile data breaches targeting companies such as Target, Neiman Marcus, eBay, Anthem, Equifax, and Yahoo Inc., Defendant is, or reasonably

---

[13] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited Aug. 1, 2018).

[14] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf (last visited Aug. 1, 2018).

[15] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, KIPLINGER, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited Aug. 1, 2018).

[16] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 1, 2018).

should have been, aware of the importance of safeguarding its customers' Personal Information, as well as of the foreseeable consequences that would occur if its systems were breached.

37. However, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach that occurred. Had Defendant maintained its systems and adequately protected them, it could have prevented the Data Breach.

38. Defendant, at all relevant times, had a duty to Plaintiff and Class Members to properly secure Personal Information, encrypt and maintain such PI using industry standard methods, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harms to Plaintiff and Class Members, and promptly notify customers when Defendant became aware of the potential that its customers' PI may have been compromised.

39. Plaintiff and Class Members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of their Personal Information, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and identity fraud, and a deprivation of the value of their Personal Information.

40. Plaintiff and Class Members have suffered and will continue to suffer additional damages based on the opportunity cost and time Plaintiff and Class Members are forced to expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

CLASS ACTION ALLEGATIONS

41. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and a Nationwide class defined as (the "Class"):

> All persons whose Personal Information was compromised in the ComplyRight Data Breach that occurred from at least April 20, 2018 through May 22, 2018.

42. Plaintiff further brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and members of the following class (the "Florida Subclass"):

> All persons residing in Florida whose Personal Information was compromised in the ComplyRight Data Breach that occurred from at least April 20, 2018 through May 22, 2018.

Excluded from the Class and Florida Subclass are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest, and their current or former employees, officers, and directors; (3) counsel for Plaintiff and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

43. Though the exact number and identities of Class and Florida Subclass members are unknown at this time, Defendant has confirmed through its notice to the Wisconsin Department of Agriculture, Trade and Consumer Protection that at least 662,000 individuals were affected by the Data Breach. Accordingly, the Class and Florida Subclass are so numerous that joinder of all members is impracticable.

44. Common questions of law and fact exist as to all Class members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether Defendant engaged in wrongful conduct as alleged herein;

(b) Whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their Personal Information and to provide timely and

accurate notice of breach to Plaintiff and Class Members, and whether it willfully, recklessly, or negligently breached these duties;

(c) Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to its data security networks and to Plaintiff and Class Members' Personal Information;

(d) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

(e) Whether Defendant failed to inform Plaintiff and Class Members of the Data Breach in a timely and accurate manner;

(f) Whether Defendant continues to breach its duties to Plaintiff and Class Members;

(g) Whether Defendant has sufficiently addressed, remedied, or protected Plaintiff and Class Members following the Data Breach and has taken adequate preventive and precautionary measures to ensure that Plaintiff and Class Members will not experience further harm;

(h) Whether Plaintiff and Class Members suffered damages as a proximate result of Defendant's conduct or failure to act; and

(i) Whether Plaintiff and Class Members are entitled to damages, equitable relief, and other relief.

45. Plaintiff's claims are typical of the claims of the respective Class and Florida Subclass he seeks to represent, in that Plaintiff and all members of the proposed Class and Florida Subclass have suffered similar injuries as a result of the same practices alleged herein.

Plaintiff has no interests adverse to the interests of the other members of the Class and Florida Subclass.

46. Plaintiff will fairly and adequately protect the interests of the Class and Florida Subclass, and has retained attorneys experienced in class actions and complex litigation as their counsel.

47. Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

48. The prerequisites for class action treatment apply to this action and that questions of law or fact common to the Class and Florida Subclass predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. The interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class and Florida Subclass will not be difficult.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

49. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

50. Defendant obtained sensitive Personal Information from Plaintiff and Class Members in its providing of legal compliance and human resources services.

51. Defendant owed a duty to Plaintiff and Class Members to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their Personal Information in

Defendant's possession from being compromised by unauthorized persons. This duty included, *inter alia*, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiff's and Class Members' Personal Information was adequately protected both in the process of collection and after collection.

52. Defendant further owed a duty to Plaintiff and Class Members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks adequately protected the Personal Information of Plaintiff and Class Members whose confidential data Defendant obtained and maintained.

53. Defendant holds itself out as an expert in legal compliance, and thus knew, or should have known, of the risks inherent in collecting and storing Personal Information and of the critical importance of provide adequate security for that information.

54. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. This conduct included but was not limited to Defendant's failure to take reasonable steps and opportunities to prevent and stop the Data Breach described above. Defendant's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of Plaintiff's and Class Members' Personal Information.

55. Defendant knew or should have known that it had inadequate data security practices to safeguard such information, and Defendant knew or should have known that hackers were and would attempt to access the Personal Information in databases such as Defendant's.

56. Defendant breached its duties to Plaintiff and Class Members by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiff and Class Members. This breach was a proximate cause of injuries and damages suffered by Plaintiff and Class Members.

57. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members suffered injury and are entitled to damages in an amount to be proven at trial. Defendant's violations of its duties of care were conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

COUNT II
GROSS NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

58. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

59. Plaintiff and Class Members entrusted Defendant with highly-sensitive and inherently personal private data subject to confidentiality.

60. In requiring, obtaining and storing Plaintiff's and Class Members' Personal Information, Defendant owed a duty of reasonable care in safeguarding this PI.

61. Defendant's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Member's Personal Information were secured from release, disclosure, and publication.

62. Defendant's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiff's and Class Member's private data.

63. Upon learning of the Data Breach, Defendant should have immediately disclosed the Data Breach to Plaintiff and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiff and Class Members as a result of the Data Breach.

64. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PI were secured from release, disclosure, and publication, Defendant ignored the inadequacies and was oblivious to the risk of release, disclosure, and publication it had created.

65. Defendant's behavior establishes facts evidencing a reckless disregard for Plaintiff's and Class Members' rights.

66. Defendant was thus grossly negligent.

67. The negligence is directly linked to Plaintiff's and Class Members' injuries.

68. As a result of Defendant's reckless disregard for Plaintiff's and Class Members' rights by failing to secure their Personal Information despite knowing its networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiff and Class Members suffered injury, which includes, but is not limited to, impermissible release, disclosure, and publication—both directly and indirectly by Defendant as well as unauthorized parties—of their Personal Information as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently. Plaintiff and Class Members have also incurred, and will continue to incur, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The impermissible release, disclosure, and publication of Plaintiff's and Class Members' PI has also diminished the value of their PI.

69. The harm to Plaintiff and the Class Members was a proximate and reasonably foreseeable result of Defendant's breach of its duty of reasonable care in safeguarding Class Members' Personal Information.

70. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT III
NEGLIGENT MISREPRESENTATION
(On behalf of Plaintiff and the Nationwide Class)

71. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

72. Defendant negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' Personal Information from impermissible release, disclosure, and publication.

73. Prior to making these representations, Defendant knew or should have known that its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PI were adequately secured from release, disclosure, and publication.

74. Plaintiffs and other reasonable consumers, including the Class Members, reasonably relied on Defendant's representations set forth herein, and, in reliance thereon, engaged, utilized, and purchased Defendant's services.

75. The reliance by Plaintiffs and Class members was reasonable and justified in that Defendants appeared to be, and represented themselves to be, a reputable business, and they sold legal compliance and human resources services.

76. Plaintiff and Class Members would not have entrusted their Personal Information or otherwise purchase or utilize Defendant's legal compliance and human resources services had they known that Defendant's data privacy and security practices and procedures were inadequate.

77. As a direct and proximate result of these misrepresentations, Plaintiff and Class Members suffered injury, which includes, but is not limited to, release, disclosure, and publication of their Personal Information as well as exposure to a heightened, imminent risk of fraud, identity theft, financial, and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently. Plaintiff and Class Members also have incurred, and will continue to incur, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The impermissible release, disclosure, and publication of Plaintiff's and Class Members' PI has also diminished the value of their PI.

78. Therefore, Plaintiff and Class Members are entitled to damages to be determined at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

79. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

80. Plaintiff and Class Members whose Personal Information is obtained by Defendant in connection with its provision of human resources services have valid, binding, and enforceable implied contracts with Defendant.

81. Specifically, Plaintiff and Class Members agreed to release their sensitive Personal Information to Defendant to be used in connection with Defendant's legal compliance and human resources services. In exchange, Defendant agreed, among other things: (1) to provide third-party legal compliance and human resources services to Plaintiff and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' Personal Information; and (3) to protect Plaintiff's and Class Members' Personal Information in compliance with federal and state laws and regulations and industry standards.

82. Protection of Personal Information is a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand.

83. Plaintiff and Class Members consented—implicitly or explicitly—to the release of their sensitive Personal Information to Defendant. Had Plaintiffs and Class members known that Defendant would not adequately protect their Personal Information, they would not have consented to or protested their Personal Information being provided Defendant. Defendant did not satisfy its promises and obligations to Plaintiff and Class Members under the implied contracts because it did not take reasonable measures to keep Plaintiff's and Class Member's Personal Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

84. Defendant materially breached its implied contracts with Plaintiff and Class members by failing to implement adequate data security measures.

85. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

86. Defendant's failure to satisfy its obligations led directly to the successful intrusion of its computer servers and stored Personal Information and led directly to unauthorized parties' access and extraction of Plaintiff's and Class Members' sensitive Personal Information.

87. Defendant breached these implied contracts as a result of its failure to implement adequate data security measures.

88. As a result of Defendant's failure to implement the security measures, Plaintiff and Class Members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

89. Alternatively, Plaintiff and each of the members of the Class are intended third party beneficiaries of any contracts between Defendant, on the one hand, and the employers or entities that utilized Defendant's legal compliance and human resources services and provided Plaintiff's and Class members Personal Information to Defendant, on the other hand.

90. Plaintiffs and the Class were injured as a direct and proximate result of Defendant's breach and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT V
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class)

91. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

92. Defendant owed a fiduciary duty to Plaintiff and the Class as guardians of their PI to (a) protect the PI belonging to Plaintiff and Class Members; and (b) timely notify them of the Data Breach.

93. Defendant breached its fiduciary duty to Plaintiff and the Class by (a) failing to adequately secure their Personal Information from impermissible release, disclosure, and publication; (b) failing to take adequate actions to prevent release, disclosure, and publication of Plaintiff's and Class Members' PI in a manner that would be highly offensive to a reasonable person; (c) failing to take adequate actions to prevent release, disclosure, and publication of Plaintiff's and Class Members' PI to unauthorized parties without the informed and clear consent of Plaintiff and the Class; and (d) notifying Plaintiff and the Class of the Data Breach four months after it had occurred and two months after Defendant had knowledge of the Data Breach.

94. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members suffered an injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendant from its conduct.

COUNT VI
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

95. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

96. Plaintiff and the Class have stated claims against Defendant based on negligence, gross negligence, negligent misrepresentation, breach of implied contract, and breach of fiduciary duty.

97. Defendant failed to fulfill its obligations to provide adequate and reasonable data security measures for the Personal Information of Plaintiff and the Class, as evidenced by the Data Breach.

98. As a result of the Data Breach, Defendant's systems are more vulnerable to access by unauthorized parties and require more stringent measures to be taken to safeguard the Personal Information of Plaintiff and Class Members going forward.

99. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide data security measures adequate to protect the Personal Information of Plaintiff and the Class.

100. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to the Personal Information of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant must implement and maintain reasonable data security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

COUNT VII
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
FLA. STAT. §§ 501.201, *et seq.*
(On behalf of Plaintiff and the Florida Subclass)

101. Plaintiff repeats and realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Florida Subclass.

102. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Fla. Stat. §§ 501.201, *et seq.* The express purpose of the FDUPTA is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

103. Plaintiff is a "consumer" as defined by the FDUTPA. Fla. Stat. § 501.203. Defendant is engaged in trade or commerce within the meaning of the FDUTPA. *Id.* Plaintiff's Personal Information is a "thing of value" within the meaning of the FDUTPA. *Id.*

104. The FDUTPA declares as unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

105. Defendant's deceptive practices are likely to mislead -- and have misled -- the consumer acting reasonably under the circumstances. Fla. Stat. § 500.204. As set forth above, Defendant's claims are deceptive and misleading to reasonable consumers because: (1) Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Florida Subclass Members' Personal Information, which was a direct and proximate case of the Data Breach; (2) Defendant failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach; and (3) misrepresenting its adequate and strong data security measures when in fact its systems were vulnerable to unauthorized access.

106. Defendant has violated the FDUPTA by engaging in the unfair and deceptive practices described above, which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers.

107. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and the Florida Subclass members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information and damages.

108. Plaintiff and the Florida Subclass seek a declaratory judgment and court order enjoining the above described wrongful acts and practices of Defendant. Fla. Stat. § 501.211(1).

109. Additionally, Plaintiff and the Florida Subclass make claims for actual damages, attorney's fees and costs. Fla. Stat. §§ 501.2105, 501.211(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and on behalf of the Class and Florida Subclass, prays for relief as follows:

A. For an Order certifying this case as a class action against Defendant and appointing Plaintiff as Representative of the Class and Florida Subclass;

B. Awarding monetary and actual damages and/or restitution, as appropriate;

C. Awarding punitive damages, as appropriate;

D. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class and Florida Subclass have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

E. Prejudgment interest to the extent allowed by the law;

F. Awarding all costs, including experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

G. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff, individually and on behalf of all others similarly situated, demand a trial by jury on all issues so triable.

DATED: August 7, 2018

By: */s/ Marc A. Wites*

Marc A. Wites (Fla. Bar No. 24783)
WITES LAW FIRM
4400 North Federal Highway
Lighthouse Point, FL 33064
Telephone: (954) 933-4400
mwites@witeslaw.com
Laurence D. King (*pro hac vice* to be sought)
Matthew George (*pro hac vice* to be sought)
Mario M. Choi (*pro hac vice* to be sought)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com
mchoi@kaplanfox.com

Attorneys for Plaintiff Jeffery Roberts and the Proposed Class

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

JEFFERY ROBERTS, Individually and on Behalf of All Others Similarly Situated,

Plaintiff(s)

v.

COMPLYRIGHT, INC., a Minnesota Corporation,

Defendant(s)

Civil Action No.: 18-cv-61836

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* COMPLYRIGHT, INC.,
Through its Registered Agent, C T Corporation System
1200 South Pine Island Road
Plantation, FL 33324

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Marc A. Wites
WITES LAW FIRM
4400 North Federal Highway
Lighthouse Point, FL 33064
Telephone: (954) 933-4400
mwites@witeslaw.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

JS 44 (Rev. 06/17) FLSD Revised 06/01/2017

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)* **NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.**

I. (a) PLAINTIFFS JEFFERY ROBERTS, Individually and on Behalf of All Others Similarly Situated

DEFENDANTS COMPLYRIGHT, INC., a Minnesota corporation

(b) County of Residence of First Listed Plaintiff Pasco
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Broward
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Marc A. Wites, Wites Law Firm, 4400 North Federal Highway, Lighthouse Point, FL 33064, (954) 933-4400

Attorneys *(If Known)*

(d) Check County Where Action Arose: ☐ MIAMI- DADE ☐ MONROE ☑ BROWARD ☐ PALM BEACH ☐ MARTIN ☐ ST. LUCIE ☐ INDIAN RIVER ☐ OKEECHOBEE ☐ HIGHLANDS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☑ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☑ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☑ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence

Other:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee – Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Re-filed (See VI below) ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation Transfer ☐ 7 Appeal to District Judge from Magistrate Judgment ☐ 8 Multidistrict Litigation – Direct File ☐ 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

(See instructions): a) Re-filed Case ☐ YES ☑ NO b) Related Cases ☑ YES ☐ NO

JUDGE: Beth Bloom DOCKET NUMBER: 18-cv-61730

VII. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. sec. 1332(d)(2); 28 U.S.C. sec. 1367

LENGTH OF TRIAL via 5-7 days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☑ Yes ☐ No

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE August 7, 2018

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT IFP JUDGE MAG JUDGE