

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF NORTH CAROLINA

DAVID LINNINS, KIM WOLFINGTON, )  
And CAROL BLACKSTOCK on behalf of )  
themselves and all others similarly ) Civil Action No.: 16cv486  
situated, )  
)  
)  
Plaintiff, )  
) **AMENDED CLASS ACTION COMPLAINT**  
v. ) **JURY TRIAL DEMANDED**  
)  
)  
)  
TIMCO AVIATION SERVICES, INC., )  
Defendant. )  

---

Plaintiffs, David Linnins, Kim Wolfington and Carol Blackstock, individually and on behalf of all others similarly situated, by and through counsel, bring this action against the Defendant, (hereafter referred to as “Timco” or “Defendant”) and allege as follows based upon personal knowledge, investigation of counsel, and information and belief:

**NATURE OF THE ACTION**

1. On April 29, 2016, Timco acknowledged that in or about March 2016 a Timco employee received a “phishing” or scam email requesting the 2015 W-2 data for all of Timco’s employees. Falling for a well-known scheme which human resources and accounting professionals have been warned to avoid, the Timco employee complied with the request in the email by sending to unknown cyber criminals an unencrypted data file which contained either copies of W-2 statements or all of the sensitive personally identifying information (“PII”) needed to fill out a W-2, including names, mailing addresses, Social Security numbers, and wage and withholding information (the “Data Disclosure”). The compromised data contained PII for every

W-2 employee<sup>1</sup>, as categorized by the Internal Revenue Service (“IRS”), who worked at and received wages from Timco during the time period of January 1, 2015 through December 31, 2015. It is estimated that approximately 3,000 current and former Timco employees had their PII compromised as a result of the Data Disclosure.

2. Almost immediately, the cyber criminals exploited Timco’s wrongful actions and filed fraudulent tax returns in the names of many of the employees. Using the Social Security numbers obtained in the Data Disclosure, the cyber criminals also requested IRS account transcripts for individual employees. These transcripts provide data from most line items on a tax form, including adjusted gross income and tax withholdings, and indicate whether current year tax returns have been filed. But most importantly to cyber criminals, these IRS transcripts will also disclose Social Security numbers and wage information of both spouses for those filing joint tax returns. Thus, using the unlawfully obtained Social Security number of one employee, cyber criminals can request a tax transcript from the IRS to fraudulently obtain the Social Security of the employee’s spouse.

3. No one can know what else the cyber criminals will do with the employees’ PII. However, what is known is that the Timco employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud. Victims of the Data Disclosure have suffered harm repeatedly since their PII was compromised. As set forth in more detail below, false tax returns have been filed using Class Members’ PII, the cyber criminals have posed as Class

---

<sup>1</sup> In simplest terms, the IRS has two categories for workers: employees and independent contractors. For employees, payroll taxes are automatically deducted from paychecks and paid to the government through the employer. The employer reports the wages to the IRS at the end of the year on a W-2 form. Independent contractors are responsible for calculating and submitting their own payroll taxes. Companies report the wages paid to independent contractors on a Form 1099. *See, IRS Publication 15-A, available at <https://www.irs.gov/publications/p15a/ar02.html>* (last visited May 5, 2016).

Members in contacting the IRS in an attempt to gain even more PII, and Class Members have spent hours completing police reports, monitoring credit reports, and placing freezes on their credit. Many Class Members are now paying fees for identity theft and credit monitoring services or insurance. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

4. Plaintiffs bring this class action against Defendant for failing to adequately secure and safeguard the PII of Plaintiffs and the Class, failing to comply with industry standards regarding electronic transmission of PII, and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen and precisely what types of information were stolen.

### **PARTIES**

#### **David Linnins**

5. Plaintiff David Linnins is a citizen and resident of Randolph County, North Carolina.

6. Mr. Linnins is a current employee at the Wallburg, North Carolina facility of Timco.

7. On or about April 13, 2016, Plaintiff David Linnins was using Turbo Tax to complete his 2015 tax return. When he electronically submitted his completed return to the IRS, he received notice that the return had been rejected and was instructed to contact the IRS at the number provided. When Mr. Linnins called the IRS, he was advised that a 2015 tax return using his Social Security number had already been filed. As Mr. Linnins had not filed this prior tax return, he realized that he had been the victim of identity theft. Mr. Linnins was instructed by the IRS to complete a Form 1039 Identity Theft Affidavit, which he did.

8. Mr. Linnins also notified the local police that he was the victim of identity theft and

tax fraud. He spent several hours with a detective completing a police report and working with the assistance of the detective to complete additional paperwork from the IRS, including an authorization for the IRS to release information regarding the incident to the local police department.

9. Mr. Linnins also notified the North Carolina Department of Revenue that he had been a victim of identity theft and tax fraud.

10. Additionally, Mr. Linnins pulled and reviewed his credit reports from each of the three nationwide credit reporting companies.

11. Within days of discovering that he had been the victim of identity theft and tax fraud, Mr. Linnins purchased identity theft and credit protection services through Lifelock at an annual cost of \$109.00.

12. As a result of the Data Disclosure, Plaintiff David Linnins has spent numerous hours making telephone calls and completing paperwork necessary to address this fraud, and his efforts are ongoing. Further, Mr. Linnins has had to take time off from work for these efforts to remediate the tax fraud he experienced, as these telephone calls and meetings had to take place during the normal business day hours.

13. Prior to the Data Disclosure, Plaintiff David Linnins had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

**Kim Wolfington**

14. Plaintiff Kim Wolfington is a citizen and resident of Forsyth County, North Carolina.

15. Mr. Wolfington is a current employee at the Timco facility located in Wallburg, North Carolina.

16. On or about April 15, 2016, when Plaintiff Kim Wolfington attempted to electronically file his tax returns, it was rejected. Mr. Wolfington contacted the IRS and learned that a 2015 tax return using his Social Security Number had been filed previously. Advising the IRS that he had not filed this prior return, Mr. Wolfington was given instructions by the IRS on filing an alternate tax return and steps he needed to take in order to prove his identity, including providing his birth certificate to the IRS.

17. In the weeks preceding April 15, 2016, Mr. Wolfington received notification from the IRS that his Social Security number had been used in an attempt to view his tax information through the IRS's Get Transcript application on [www.irs.gov](http://www.irs.gov). Mr. Wolfington assumed that his accountant has made this inquiry in conjunction with preparing Mr. Wolfington's tax return and, thus, had not been alarmed. After learning that he had been the victim of identity theft, Mr. Wolfington inquired of his accountant and discovered that an unauthorized third party had made this attempt using his PII.

18. To his knowledge, prior to the Data Disclosure, Mr. Wolfington had never been the victim of identity theft or been involved in a data breach incident.

19. As a result of the Data Disclosure, Plaintiff Kim Wolfington has spent several hours remediating the identity theft and tax fraud that he experienced, and it is likely that he will be required to spend additional time protecting himself from future incidents of identity theft and fraud. Additionally, the 2015 federal tax refund that he was expecting is being delayed while the IRS investigates the matter further, verifies Mr. Wolfington's identity, and processes the correct return.

**Carol Blackstock**

20. Plaintiff Carol Blackstock is a citizen and resident of Davidson County, North Carolina.

21. Mrs. Blackstock is a current employee at Timco's Wallburg, North Carolina facility.

22. On or about March 28, 2016, Plaintiff Carol Blackstock received a letter from the IRS addressed to her and her husband. The letter was a response to a March 19, 2016 request made to the IRS for an account transcript. Concerned that neither she nor her husband had made the request for this transcript, which included their Social Security Numbers, 2015 Adjusted Gross Income, 2015 Taxable Income, and tax withholding amounts, Mrs. Blackstock contacted the IRS. She was instructed on the steps to take to report the identity theft and fraud.

23. Because she had not experienced any other issues, Mrs. Blackstock did not feel a sense of urgency to complete the paperwork requested by the IRS. However, weeks later, after learning that her PII had been disclosed by Timco to unknown third parties, she began taking immediate steps to prevent future identity theft and harm. As a result of the Data Disclosure, Mrs. Blackstock has spent, and will continue to spend, numerous hours filing police reports, monitoring her credit reports and completing the IRS paperwork necessary to protect herself from future incidents of identity theft or fraud.

24. Prior to the Data Disclosure, Plaintiff Carol Blackstock had never been the victim of identity theft or been involved in a Data Disclosure.

**Defendant**

25. Defendant Timco Aviation Services, Inc. is a Delaware corporation with its principal place of business in Greensboro, North Carolina.

## **JURISDICTION AND VENUE**

26. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because there are more than 100 Class Members, the class contains members of diverse citizenship from Defendant, and the amount in controversy exceeds \$5,000,000 exclusive of costs and interests.

27. This Court has personal jurisdiction over Defendant because Timco's U.S. headquarters is in this District and each Defendant is authorized to and does conduct substantial business in North Carolina, and in this District.

28. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Timco's U.S. headquarters is in this District, the Defendant regularly conduct business in this District, and a substantial part of the events or omissions giving rise to this action occurred in this District.

## **FACTUAL ALLEGATIONS**

29. On or about April 16, 2016, Timco advised current employees that a Data Disclosure was suspected as several employees had reported experiencing problems when filing their 2015 tax returns.

30. On or about April 18, 2016, representatives of the Human Resources Department held meetings with current employees to advise that W-2s for "some of" Timco's employees had been disclosed to a third party and, as a result, some employees reported having fraudulent tax returns filed using their PII. At no point during this meeting were employees advised that the "third party" to whom the PII had been disclosed were unknown cyber criminals.

31. On or about April 19, 2016, Timco' CEO, Kevin Carter, sent a letter via company email advising that all W-2 forms of Timco' employees had been disclosed to "an outside party."

Once again, Timco did not disclose the identity of the third party, or more appropriately, that the identity was unknown. Acknowledging the importance of the privacy and security of its employee's PII, Mr. Carter further advised that Timco would be offering two years of free identity theft protection through third-party provider ProtectMyId.com to those employees who enrolled on-line.

32. In a letter dated April 29, 2016, and received by most employees on or about May 4, 2016, Timco advised that it had experienced a "data security issue." The letter, signed by CEO Kevin Carter, stated that on April 15, 2016, Timco became aware that W-2 information had been disclosed to an unknown third party in response to a "phishing" email. The letter further stated that the information disclosed was W-2 information, including names, Social Security numbers and wage information. Mr. Carter declared in the letter that no other information had been disclosed. The letter advised again that employees could receive two years of identity theft protection if they went on-line to enroll in the service. This letter was the first notice by Timco that the employees' PII had been given to unknown cyber criminals.

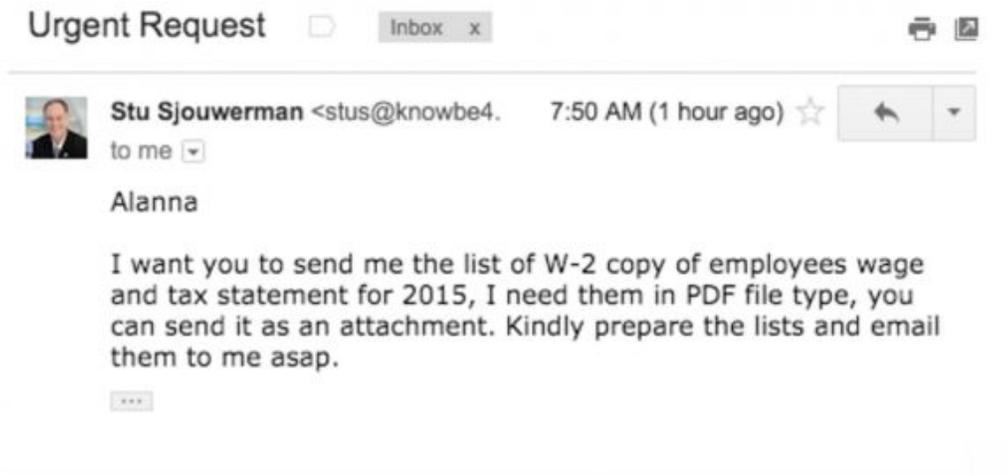
33. This Data Disclosure was caused by Timco's voluntary disclosure of the PII of its current and former employees, ironically at a time in the calendar year when W-2 information is most vital and valuable.

34. Timco was not without warning of this phishing email scam, yet it failed to implement adequate measures to protect its employees' PII.

35. On August 27, 2015, the Federal Bureau of Investigation ("FBI") issued a report warning of the increasingly common scam, known as Business Email Compromise, in which

companies fall victim to phishing emails.<sup>2</sup> Most importantly, this report called attention to the significant spike in scams, also referred to as CEO email schemes, in which cyber criminals send emails that appear to have initiated from the CEO or other top level executive at the target company.

36. On February 24, 2016, noted cybersecurity journalist Brian Krebs warned of this precise scam, which snared Timco, in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.<sup>3</sup> Krebs warned that cyber criminals were attempting to scam companies by sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company:



37. On March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme, which Timco ignored. In precise detail, the alert stated:

<sup>2</sup> See, *Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), available at <https://www.ic3.gov/media/2015/150827-1.aspx> (last visited May 5, 2016.).

<sup>3</sup> Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, available at <http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/> (last visited May 5, 2016).

The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.

The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

“This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments,” said IRS Commissioner John Koskinen. “If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees.”<sup>4</sup>

38. Timco’s negligence in safeguarding its employees’ PII is exacerbated by the repeated warnings and alerts, not only of the increasing risk of general phishing scams, but of the actual W-2 phishing email scam it chose to ignore and thus fell prey to.

39. Timco’s failures handed to criminals the PII of Plaintiffs and other Class Members and put Plaintiffs and the Class at serious, immediate and ongoing risk for identity theft and fraud. The practice with such breaches is that the cyber criminals will use the PII, as they have done here, to file false tax returns immediately but also will continue to use the PII to exploit and injure Class Members by selling the PII to third parties or otherwise using the PII for illicit purposes.

40. The Data Disclosure was caused and enabled by Timco’s violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Timco failed to comply with security standards and allowed its

---

<sup>4</sup> IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (March 1, 2016), available at <https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s> (last visited May 5, 2016)

employees' PII to be compromised by failing to implement security measures that could have prevented or mitigated the Data Disclosure. Timco failed to implement even the most basic of security measures to require encryption of any data file containing PII sent electronically, even within the company.

41. Timco failed to ensure that all personnel in its human resources and accounting departments were made aware of this well-known and well-publicized phishing email scam.

42. Timco failed to timely disclose the extent of the Data Disclosure, failed to individually notify each of the affected individuals in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiffs and the other Class Members of the nature and extent of the Data Disclosure. By failing to provide adequate and timely notice, Timco prevented Plaintiffs and Class Members from protecting themselves from the consequences of the Data Disclosure.

43. The ramifications of Timco's failure to keep its employees' PII secure are severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>5</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

---

<sup>5</sup> 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number.”<sup>6</sup>

45. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

46. The Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.<sup>7</sup>

47. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, as they have done here, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

48. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link

---

<sup>6</sup> *Id.*

<sup>7</sup> Social Security Administration, Identity Theft and Your Social Security Number, *available at* <http://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited May 5, 2016).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>8</sup>

50. Based on the foregoing, the information compromised in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Timco Data Disclosure is difficult, if not impossible, to change—Social Security number, name, date of birth, employment information, income data, etc.

51. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>9</sup>

52. Despite all of the publically available knowledge of the continued compromises of PII, and alerts regarding the actual W-2 phishing email scam perpetrated, Timco’s approach to maintaining the privacy of its employees PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

53. Timco failed to provide compensation to Plaintiffs and Class Members victimized in this Data Disclosure. Timco has not offered to provide any compensation for the costs and

---

<sup>8</sup> *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited May 5, 2016).

<sup>9</sup> *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited May 5, 2016).

burdens associated with the fraudulent tax returns filed as a result of the Data Disclosure. Timco has not offered employees any assistance in dealing with the IRS or state tax agencies. Timco has not offered to reimburse employees for the costs – current and future – incurred as a result of falsely filed tax returns.

54. When current employees requested Timco’s assistance in filing police reports, Timco simply responded that each employee would have to file his or her own report on his or her own time. Timco has not offered to compensate employees for any time off from work taken to deal with the ramifications of the Data Disclosure.

55. To date, Timco has offered its employees only two years of identity theft protection through the Experian ProtectMyId service. Employees and victim of the Data Disclosure have to take their own time to enroll in the service. Timco has not offered to reimburse the cost of identity theft protection services purchased by employees before Timco gave notice that it would pay for such services.

56. In any event, the offered ProtectMyID service is inadequate to protect the Plaintiffs and Class Members from the threats they face, particularly in light of the PII stolen. The ProtectMyID service does nothing to protect against actual identity theft, as its services revolve around credit report monitoring. Instead, it only provides a measure of assistance after the identity theft has been discovered. For example, ProtectMyID monitors credit reports, but fraudulent activity, such as the filing of a false tax return, may not appear on a credit report. Although offers The identity theft insurance coverage provided by ProtectMyID is limited and often duplicative of, or even inferior to, basic protections provided by banks and credit card companies. Additionally and most importantly here, ProtectMyID provides no assistance for pre-existing identity theft and fraud, which Plaintiffs and Class Members experienced before the ProtectMyID

service took effect as a result of the Data Disclosure.

57. Many websites that rank identity theft protection services are critical of ProtectMyID. NextAdvisor ranks ProtectMyID at the bottom of comparable services, noting that it “lacks in protection.”<sup>10</sup> BestIDTheftCompanys.com ranks ProtectMyID at number 29 on its list of companies with a mere score of 4.4 out of 10 (and a “User Score” of only 1.3).<sup>11</sup>

58. As a result of Defendant’ failures to prevent the Data Disclosure, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise, publication and/or theft of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- f. Unauthorized use of compromised PII to open new financial accounts and apply for unemployment benefits;

---

<sup>10</sup>*Identity Theft Protection Reviews & Prices*, NextAdvisor.com, found at [http://www.nextadvisor.com/identity\\_theft\\_protection\\_services/compare.php](http://www.nextadvisor.com/identity_theft_protection_services/compare.php) (last visited May 5, 2016).

<sup>11</sup> See, <https://bestidtheftcompanys.com/company/experian-protectmyid/> (last visited May 5, 2016).

- g. The continued risk to their PII, which remains in the possession of Timco and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the PII in their possession; and
- h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

### **CLASS ACTION ALLEGATIONS**

59. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of the provisions of Rule 23.

60. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All current and former Timco employees whose PII was compromised as a result of the Data Disclosure.

61. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiffs seek to represent the following state class only in the event that the Court declines to certify the Nationwide Class above. Specifically, the state class consists of the following:

All current and former Timco employees who currently reside in North Carolina and whose PII was compromised as a result of the Data Disclosure.

62. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is estimated to be at or above 3,000.

The exact number is generally ascertainable by appropriate discovery as Timco had knowledge of the employees whose PII was in the data file it disclosed.

63. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;
- b. Whether Defendant failed to adequately safeguard the PII of Class Members;
- c. Whether Defendant timely, adequately, and accurately informed Class Members that their PII had been compromised;
- d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;
- e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;
- f. Whether Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant' wrongful conduct;
- i. Whether Plaintiffs and the members of the Classes are entitled to restitution as a result of Defendant' wrongful conduct; and,
- j. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

64. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other class member, was disclosed by

Timco. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct described above and were subject to Defendant' unfair and unlawful conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all Class Members.

65. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class and Subclasses in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Classes and Subclasses. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Classes and Subclasses and the infringement of the rights and the damages they have suffered are typical of other Class members and of other Subclass members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

66. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporate Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical.

67. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each member of the Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

68. The litigation of the claims brought herein is manageable. Defendant' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

69. Adequate notice can be given to Class Members directly using information maintained in Defendant' records and/or through publication.

70. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the scope of the Data Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

71. Defendant have acted, or refused to act, on grounds that apply generally to the Class, making final injunctive and declaratory relief appropriate to the Class as a whole.

Defendant' acts and omissions are the direct and proximate cause of damage described more fully elsewhere in this Complaint.

72. Plaintiffs reserve the right to modify or amend the definition of the proposed classes and to modify, amend or remove proposed subclasses, before the Court determines whether certification is appropriate and as the parties engage in discovery.

**FIRST CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of the Class)**

73. Plaintiffs incorporate by reference the allegations contained in all previous paragraphs as if fully set forth herein.

74. As a condition of their employment, employees were obligated to provide Timco with certain PII, including their date of birth, mailing addresses and Social Security numbers.

75. Plaintiffs and the Class Members entrusted their PII to Timco on the premise and with the understanding that Timco would safeguard their information.

76. Timco had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed.

77. Timco had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

78. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices and procedures.

79. Timco's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Timco's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Timco's misconduct also included

its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiffs and Class Members.

80. Plaintiffs and the Class Members had no ability to protect their PII that was in Timco's possession.

81. Timco was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Disclosure.

82. Timco had and continues to have a duty to timely disclose that the PII of Plaintiffs and Class Members within its possession might have been compromised and precisely the types of information that were compromised and when. Such timely notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

83. Timco had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

84. Timco has admitted that the PII of Plaintiffs and Class Members was wrongfully disclosed as a result of the Data Disclosure.

85. Timco, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Timco's possession or control.

86. Timco improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

87. Timco failed to heed industry warnings and alerts issued by the IRS to provide

adequate safeguards to protect employees' PII in the face of increased risk of a current phishing email scheme being perpetrated.

88. Timco, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its employees' PII.

89. Timco, through its actions and/or omissions, unlawfully breached its duty to timely and adequately disclose to Plaintiff and Class Members the existence, timing and scope of the Data Disclosure.

90. But for Timco's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

91. As a result of Timco's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with addressing false tax returns filed; future out-of-pocket costs in connection with preparing and filing tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure

**SECOND CAUSE OF ACTION**  
**Invasion of Privacy**  
**(On Behalf of the Class)**

92. Plaintiffs incorporate by reference the allegations contained in all previous paragraphs as if fully set forth herein.

93. Defendant invaded the right to privacy of Plaintiffs and Class Members by giving the PII of Plaintiffs and Class Members to unauthorized and unknown third parties.

94. Defendant invaded the right to privacy of Plaintiffs and Class Members by allowing unknown third parties unauthorized access to the PII of Plaintiffs and Class Members.

95. The intrusion was offensive and objectionable to Plaintiffs, Class Members and to a reasonable person of ordinary sensibilities in that the PII of Plaintiffs and Class Members was disclosed without prior authorization.

96. The intrusion was into a place or thing which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Timco as part of their employment, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their authorization.

97. As a proximate result of the above acts and omissions of Timco, the PII of Plaintiffs and Class Members was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

98. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Timco can be viewed, distributed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

**THIRD CAUSE OF ACTION**  
**Violation of the North Carolina Unfair and Deceptive Trade Practices Act**  
**(On Behalf of the Class)**

99. Plaintiffs incorporate by reference the allegations contained in all previous paragraphs as if fully set forth herein.

100. It is appropriate to apply North Carolina law to the nationwide class claims because North Carolina's interest in this litigation exceeds that of any other state.

101. As discussed above, Timco's U.S. headquarters are located in North Carolina. Upon information and belief, the acts leading to the disclosure of employees' PII occurred at a Timco facility in North Carolina. Based upon the foregoing, the policies, practices, acts and omissions giving rise to this Action emanated from Timco's headquarters and facilities in North Carolina.

102. Defendant were engaged in practices affecting commerce by the actions described above within the meaning of N.C.G.S. §75-1.1.

103. The conduct of Defendant alleged above constitutes an unfair and deceptive trade practice in violation of N.C. Gen. Stat. § 75-1.1(a) which provides:

Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

104. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect the PII of Plaintiffs and Class Members constitute unfair or deceptive acts or practices the North Carolina Unfair and Deceptive Trade Practices Act (UDTPA).

105. Defendant further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C.G.S. § 75-60, *et. seq.* (ITPA).

106. Defendant violated ITPA by:

- a. Failing to prevent the personal information of employees from falling into unauthorized hands;
- b. Failing to make reasonable efforts to safeguard and protect the personal information, particularly Social Security numbers, of employees; and

- c. Failing to provide adequate notice of the security breach to affected employees upon discovery that their system had been compromised and personal information had been stolen.

107. Timco violated UDTPA by intentionally communicating and disclosing its employees' Social Security numbers, without written consent, to a third party, which it had reason to believe lacked a legitimate purpose for obtaining the Social Security numbers, in direct violation of N.C.G.S. § 75-62.

108. Defendant willfully concealed, suppressed, omitted and failed to inform Plaintiffs and Class Members of the material facts as described above.

109. Plaintiffs and Class Members have suffered ascertainable losses as a direct result of Defendant' unconscionable acts or practices, and unfair or deceptive acts or practices.

110. As a direct and proximate result of the injury caused by the unfair and deceptive trade practices of the Defendant, Plaintiffs and Class Members are entitled to relief, including actual and treble damages, under N.C.G.S. § 75-1.1 and 75-16. Further, the unlawful acts and omissions as set forth above were willful violations entitling Plaintiffs to attorneys' fees, under N.C.G.S. § 75-16.1. Further, similarly situated members of the proposed classes are likewise entitled to remedies due to the injury they have suffered as a result of the unfair and deceptive trade practices.

### **PRAYER FOR RELIEF**

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;
- B. A mandatory injunction directing Defendant to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;
- C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PII to unauthorized persons;
- D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;
- E. For an award of attorneys' fees and costs;
- F. For treble damages pursuant to N.C. Gen. Stat § 75-16 and for Plaintiffs' costs incurred; and,
- G. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 12, 2017

Respectfully submitted,

/s/ Jean Sutton Martin  
JEAN SUTTON MARTIN  
North Carolina Bar Number 25703  
jean@jsmlawoffice.com  
LAW OFFICE OF JEAN SUTTON  
MARTIN PLLC  
2018 Eastwood Road Suite 225  
Wilmington, NC 28403  
Telephone: (910) 292-6676  
Facsimile: (888) 316-3489  
Email: jean@jsmlawoffice.com

/s/ John A. Yanchunis  
JOHN A. YANCHUNIS\*  
Florida Bar No. 324681  
jyanchunis@ForThePeople.com  
MARCIO W. VALLADARES\*  
Florida Bar No. 986917  
mvalladares@ForThePeople.com  
PATRICK A. BARTHLE II\*  
Florida Bar No. 99286  
pbarthle@ForThePeople.com  
MORGAN & MORGAN  
COMPLEX LITIGATION GROUP  
201 N. Franklin Street, 7th Floor  
Tampa, Florida 33602  
Telephone: (813) 223-5505  
Facsimile: (813) 223-5402

*Attorneys for Plaintiffs and the Proposed Class*

*\* Special Admission to be submitted*

## **CERTIFICATE OF SERVICE**

I hereby certify that on January 12, 2017, a true and correct copy of the foregoing document was filed with the Court utilizing its ECF system, which will send notice of such filing to all counsel of record.

/s/ Jean S. Martin

Jean S. Martin