E-FILED
Tuesday, 10 September, 2019 03:43:27 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS

LYNN MCGLENN, on behalf of herself and all others similarly situated, Plaintiff, v. DRIVELINE RETAIL MERCHANDISING, INC., Defendant.	)	Civil Action No.: 2:18-cv-02097-CSB-EIL **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Lynn McGlenn, individually and on behalf of all others similarly situated, by and through counsel, bring this first amended complaint against Defendant Driveline Retail Merchandising, Inc. ("Defendant" or "Driveline"), and alleges as follows based upon personal knowledge, investigation of counsel, and information and belief:

PARTIES

1. Plaintiff Lynn McGlenn is a citizen and resident of Charlotte, North Carolina.

2. Defendant Driveline Retail Merchandising, Inc. is a resident of Illinois.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class members, and at least one class member is a citizen of a state different from Defendant as Plaintiff McGlenn is a citizen of Georgia and Defendant is a citizen of Illinois.

4. This Court has personal jurisdiction over Defendant because Driveline maintains its principal place of business in this District, regularly conducts business in this District, and is authorized to and does conduct substantial business in this District.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Driveline's principal place of business is in this District and a substantial part of the events or omissions giving rise to this action, particularly decisions related to data security and the acts which lead to the Data Disclosure, occurred in this District.

FACTUAL ALLEGATIONS

6. Defendant Driveline Retail Merchandising provides retail merchandising services, setting up product displays and or shelve products at big-box retail establishments in the continental United States, Alaska, Hawaii, Puerto Rico, the Virgin Islands, and Guam. Driveline's clients are national and regional companies across the country, including: Dollar General, Johnson and Johnson, Kraft, Walgreens, Nestle, StoreBoardMedia, BiLo, Unilever, WinnDixie, Kimberly-Clark, and ConAgra Foods.

7. As a condition of employment, Driveline requires that employees entrust it with certain personal information. In its ordinary course of business, Driveline maintains personal and tax information, including the name, address, zip code, date of birth, wage and withholding information, and Social Security number, of each current and former employee.

8. Plaintiff and members of the proposed Class, as current and former employers, relied on Driveline to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

9. On or about February 14, 2017, Defendant sent a letter to its current and former

employees advising that their 2016 W-2 tax form information had been subjected to "a data breach." [1]

10. The "data breach" was, in reality, a data disclosure by a Driveline employee responding to an email "that *appeared* to be sent from Driveline management." In response to the email, that employee provided "a file containing the 2016 W-2s of Driveline employees."

11. Ignoring a well-known "phishing" or scam email scheme, which human resources and accounting professionals have been warned about repeatedly, the Driveline employee complied with an email request to send unknown cyber criminals a data file containing copies of W-2 statements for W-2 employees[2] (as categorized by the Internal Revenue Service ("IRS")) who worked at and received wages from Driveline during the time period of January 1, 2016 through December 31, 2016 (the "Data Disclosure"). These W-2 statements contain sensitive personally identifying information ("PII") including names, mailing addresses, Social Security numbers, and wage and withholding information.

12. This case does not involve a *breach* of a computer system *by* a third party, but rather a voluntary, unauthorized *disclosure* of the PII of Plaintiffs and Class members by the Defendant *to* a third party.

13. The Data Disclosure occurred at a time in the calendar year when W-2 information is most vital and valuable.

14. Plaintiff Lynn McGlenn is a former employee at Driveline whose PII was disclosed

[1] A true and correct copy of the February 14, 2017 letter (the "Notice") is attached hereto as Exhibit A.

[2] 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 November 8, 2017).

without her authorization to an unknown third party as a result of the Data Disclosure.

15. Before the Data Disclosure, Ms. McGlenn had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

16. It was not until on or after February 14, 2017, that Ms. McGlenn learned from the Notice that a Driveline employee had been responsible for emailing Ms. McGlenn's PII to an unknown, unauthorized third party.

17. Shortly after receiving the notice from Driveline, Plaintiff McGlenn was alerted that someone used her personally identifiable information to open a new credit card account with Capital One, which required the use of her Social Security Number and other data found on her W-2.

18. As a result of this fraudulent use of her personal information, Plaintiff McGlenn alerted the credit reporting agencies and placed a freeze on her credit. She was required to spend time working with Capital One to close the fraudulent account. She spent approximately 10 hours resolving and mitigating the issues arising from the misuse of her personal information. Concerned that this type of theft could easily happen again given that her personal information remains in the hands of criminals due to the Data Disclosure, Plaintiff McGlenn now spends time weekly checking her credit reports.

19. As a result of the Data Disclosure, Ms. McGlenn has spent, and will continue to spend, numerous hours monitoring her bank accounts, and credit reports and taking other actions necessary to protect herself from future incidents of identity theft or fraud.

20. Without question, the PII of Plaintiff and Class members, particularly their Social Security numbers and wage and tax information, was taken for purposes of identity theft, and unfortunately, Driveline's current and former employees are now, and for the rest of their lives

will be, at a heightened risk of further identity theft and fraud.

21. Plaintiff brings this class action against Driveline for failing to adequately secure and safeguard the PII of Plaintiff and the Class, for failing to comply with industry standards regarding electronic transmission of PII, and for failing to provide timely accurate and adequate notice to Plaintiff and other Class members as to precisely how and when their sensitive personal information had been given to unknown persons.

22. Driveline disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that employees' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

23. Driveline could have prevented this Data Disclosure. Driveline was not without warning of this phishing email scam, yet it failed to implement adequate measures to protect its employees' PII.

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

25. 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 had fallen victim to phishing emails.[3] Most importantly, this report called attention to the significant spike in scams, also referred to as spoofing, in which cyber criminals send emails that appear to have initiated from the CEO or other top-level executive at the target company.

26. Business Email Compromise or phishing or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an "urgent" request from a company "executive" requesting that confidential information be provided via email.

27. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name." [4]

28. Spoofing fraud has been steady increasing in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received reports from over 17,000 victims of "spoofing" scams, which resulted in more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.[5]

---

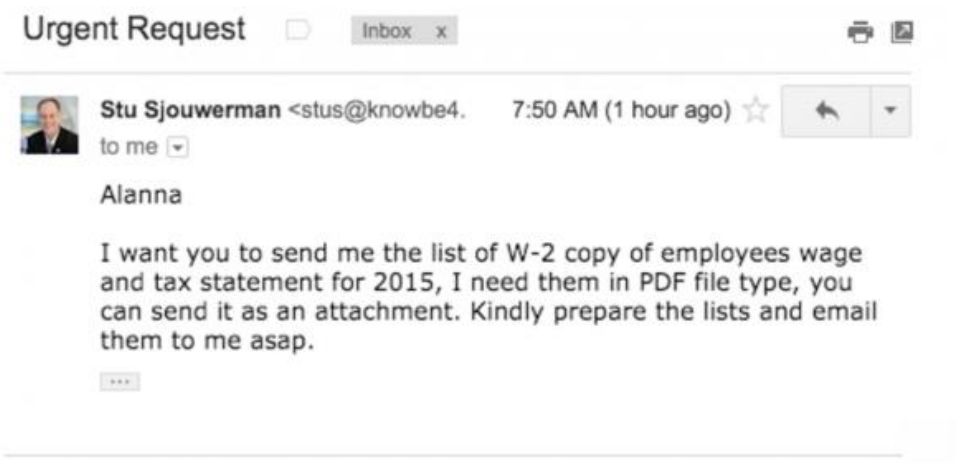
[3] *See, Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx (last visited November 8, 2017).
[4] Brian Krebs, *FBI: $2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), *available at* http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/ (last visited November 8, 2017).
[5] *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), *available at* https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-email-scams (last visited November 8, 2017).

29. Companies can mount several defenses to spoofing scams. These defenses include employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal and tax information.

30. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

31. On February 24, 2016, a well-respected and followed cybersecurity journalist Brian Krebs warned of the precise scam which snared Driveline in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.[6] Krebs warned that cybercriminals 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:

[6] Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, KREBS ON SECURITY *available at* http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/ (last visited November 8, 2017).



32. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. In precise detail, the alert stated:

> 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." [7]

33. Again, on January 25, 2017—the very day the phishing email was sent to

[7] 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 November 8, 2017).

Driveline—the IRS renewed the alert specifically cautioning, "company payroll officials to double check any executive-level or unusual requests for lists of Forms W-2 or Social Security number."[8]

34. A simple phone call to the purported sender of the email to verify this request would have prevented the Data Disclosure.

35. Encrypting the file containing the PII would have prevented the Data Disclosure.

36. Despite the widespread prevalence of spoofing aimed at obtaining confidential information from employers and despite the warnings of the W-2 email scam from the 2015 tax season and renewed alerts for the 2016 tax season, Driveline provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure.

37. Driveline failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and

[8] IRS, *IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments*, IR-2017-10 (Jan. 25, 2017), *available at*: https://www.irs.gov/uac/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w2-scam-targeting-payroll-human-resource-departments (last visited November 8, 2017).

f. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

38. Driveline's decisions handed criminals the PII of Plaintiff and other Class members and put Plaintiff and the Class at serious, immediate and ongoing risk for identity theft and fraud.

39. Access to W-2 information permits identity thieves to quickly and easily file fraudulent tax returns, using the victim's information to obtain a fraudulent refund. The IRS will direct deposit the refund to the bank account or prepaid debit card (which are virtually untraceable) provided by the thief.

40. The Data Disclosure was caused by Driveline's violation of its obligation to abide by best practices and industry standards concerning the security of highly confidential employee data and the storage, use, and transmission of that data. Driveline decided not to comply with accepted security standards and allowed its employees' PII to be disclosed and compromised by choosing not to implement security measures that could have prevented or mitigated the Data Disclosure. Driveline failed to implement even the most basic of data security practices to require encryption of any data file containing PII sent electronically, even internally within the company.

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

42. Upon discovery, Driveline failed to take reasonable steps to clearly and conspicuously inform Plaintiff and the other Class members of the nature, timing and extent of the Data Disclosure. By failing to provide adequate timely notice, Driveline prevented Plaintiff and Class members from protecting themselves from the consequences of the Data Disclosure.

43. Driveline was well aware of the risk of identity theft and other damage to its employees if their PII was disclosed to unauthorized third parties or otherwise compromised. The ramifications of Driveline's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, 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."[9] 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, employer or taxpayer identification number."[10]

45. The data compromised in the Driveline Data Disclosure, particularly, Social Security numbers, 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. Indeed, the information compromised in the Driveline Data Disclosure is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

46. 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

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id.*

information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

47. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

48. 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.[12]

49. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, 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.

50. 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.

---

[11] *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 November 8, 2017).

[12] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 30, 2016).

51. 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 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."[13]

52. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

53. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

54. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

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

---

[13] *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 November 8, 2017).

[14] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited November 8, 2017).

56. Even reimbursing a consumer for certain financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims." [15]

57. To date, Driveline has offered its employees only 12 months of credit monitoring service through AllClear ID. The offered service is inadequate in to protect the Plaintiff and Class members from the threats they face, particularly in light of the PII stolen.

58. As a result of Driveline's failures to prevent the Data Disclosure, Plaintiff 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. Unauthorized use and misuse of their PII;

b. The loss of the opportunity to control how their PII is used;

c. The diminution in value of their PII;

d. The compromise, publication and/or theft of their PII;

e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

f. 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

[15] Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited November 8, 2017).

fraud;

g. Delay in receipt of tax refund monies;

h. Lost opportunity and benefits of electronically filing of income tax returns;

i. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

j. The continued risk to their PII, which remains in the possession of Driveline and is subject to further breaches so long as Driveline fail to undertake appropriate measures to protect the PII in their possession; and

k. 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 Plaintiff and Class members.

59. As a direct and proximate result of Driveline's wrongful actions and inaction and the resulting Data Disclosure, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Disclosure reach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

60. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiff and Class members should be free of having to deal with the consequences of Driveline's carelessness.

61. The injuries to the Plaintiff and Class members were directly and proximately caused by Driveline's failure to implement or maintain adequate data security measures for its employees' PII.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

63. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

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

64. Excluded from the Classes are the officers, directors and legal representatives of Driveline and the judges and court personnel to whom this case may be assigned and any members of their immediate families.

65. 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 Plaintiff at this time, based on information and belief, it is estimated to be at or above 10,000. The exact number is generally ascertainable by appropriate discovery as Driveline had knowledge of the employees whose PII was in the data file it disclosed.

66. 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 Driveline had a duty to protect the PII of Class members;

b. Whether Driveline had a duty to not disclose the PII of Class members to unauthorized third parties;

c. Whether Driveline had a duty to not use the PII of Class members for non-business purposes;

d. Whether Driveline failed to adequately safeguard the PII of Class members;

e. Whether Driveline adequately, promptly, and accurately informed Class members their PII had been compromised;

f. Whether Driveline failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed without authorization in the Data Disclosure;

g. Whether Driveline engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class members;

h. Whether Class members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Driveline' wrongful conduct;

l. Whether Plaintiff and the members of the Class are entitled to restitution as a result of Driveline' wrongful conduct; and,

m. Whether Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

67. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff' claims are typical of those of other Class members because Plaintiff's PII, like that of every other class member, was disclosed by Driveline. Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members,

and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

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

69. 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 Driveline. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical.

70. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff 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 Plaintiff 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.

71. 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.

72. Adequate notice can be given to Class members directly using information maintained in Driveline's records.

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

74. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

75. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, transmitting, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, transmitting, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately, and accurately informed Class members that their PII had been disclosed without authorization;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed and compromised in the Data Disclosure;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard and disclosing without authorization the PII of Class members; and,

g. Whether Class members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

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

76. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

77. As a condition of their employment, employees were obligated to provide Driveline

with certain PII, including their date of birth, mailing addresses and Social Security numbers.

78. Plaintiff and the Class members entrusted their PII to Driveline on the premise and with the reasonable expectation and understanding that Driveline would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

79. Driveline's obligation under federal law to collect PII from its employees was accompanied by a duty to use reasonable care in the protection, use, transmission, and safeguarding of this PII.

80. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII were wrongfully disclosed.

81. Driveline knew or reasonably should have known that the failure to exercise due care in the collecting, storing, transmitting, and using of its employees' PII involved an unreasonable risk of harm to Plaintiff and Class members, even if the harm occurred through the acts of a third party.

82. Driveline knew or reasonably should have known of the IRS, government, and industry warnings regarding the prevalence of phishing email scams seeking W-2 information of employees and that the failure to heed these warnings would create an unreasonable risk of harm to Plaintiff and Class members.

83. Defendant 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. This duty includes, among other things, designing, maintaining and testing Defendant security protocols to ensure that Plaintiff and Class members' information in its possession was adequately secured and protected and that employees tasked with maintaining such

information were adequately training on cyber security measures regarding the security of employees' personal and tax information, particularly in the transmission of such data.

84. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Driveline knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

85. Driveline's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Driveline misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Driveline misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class members.

86. Plaintiff and the Class members had no ability to protect their PII that was in Driveline's possession.

87. Driveline was in the sole position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Disclosure.

88. Driveline had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class members within its possession was disclosed without authorization, might have been compromised, how it was disclosed and/or compromised and precisely the types of information that were disclosed and when. Such notice was necessary to allow Plaintiff 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.

89. Driveline had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiff and Class members.

90. Driveline has acknowledged that the PII of Plaintiff and Class members was voluntarily, wrongfully disclosed to unauthorized third persons as a result of the Data Disclosure.

91. Driveline, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class members during the time the PII was within Driveline possession or control.

92. Driveline improperly and inadequately safeguarded the PII of Plaintiff and Class members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

93. Driveline 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.

94. Driveline, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect phishing scams and prevent unauthorized dissemination of its employees' PII.

95. Driveline, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class members the existence, and scope of the Data Disclosure.

96. But for Driveline's wrongful and negligent breach of duties owed to Plaintiff and Class members, the PII of Plaintiff and Class members would not have been disclosed and compromised.

97. There is a close causal connection between Driveline's decision not to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

98. As a result of Driveline's negligence, Plaintiff and the Class members have suffered and will continue to suffer damages and injury including, but not limited to: identity theft, out-of-pocket expenses associated with addressing false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed 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 Plaintiff and the Class)

99. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

100. Plaintiff and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

101. Because of the nature of the relationship between Defendant and its employees, including that Defendant is required by law to obtain certain PII of its employees and employees are required to provide such data to Defendant, Defendant owed a duty to its employees, including Plaintiff and Class members, to keep their PII confidential and prevent unauthorized disclosures of such PII.

102. Defendant made an active, voluntary decision to release an unencrypted file containing the PII of Plaintiff and Class members through an email transmission, knowing that

whoever came into possession of that email and/or file would have unfettered and unlimited access to, examination of, and use of highly confidential PII of Plaintiff and Class members.

103. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiff and Class members, especially where the information includes Social Security numbers and wage information, would be highly offensive to a reasonable person.

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

105. The Data Disclosure at the hands of Defendant constitutes an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

106. As a proximate result of the above acts and omissions of Driveline, the PII of Plaintiff and Class members was disclosed to and used by third parties without authorization, causing Plaintiff and Class members to suffer damages.

107. Unless and until enjoined, and restrained by order of this Court, Driveline wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Driveline can be viewed, distributed and used by unauthorized persons. Plaintiff 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 Plaintiff and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

108. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

109. Plaintiff and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to Driveline as a condition of their employment.

110. Implicit in the employment agreement between the Driveline and its employees was the obligation that Driveline would use the PII of its employees for business purposes only and not make unauthorized disclosures of the information.

111. Driveline had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses.

112. Additionally, by accepting the PII of its employees, Driveline implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

113. Plaintiff and Class members fully performed their obligations under the implied contract with Driveline. Driveline did not.

114. Driveline breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff' and Class members' PII, which was disclosed to unauthorized third parties by Driveline's decision to send an unencrypted file containing its employees' PII through an email communication.

115. Driveline's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their PII as a condition of employment in exchange for compensation and benefits.

116. As a direct and proximate result of Driveline's breach of its implied contacts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the control over how their PII is used and who has access to same; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity 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 tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remain in Driveline possession and is subject to further unauthorized disclosures so long as Driveline fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiff and Class members.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

117. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

118. In light of the special relationship between Driveline and its employees, whereby Driveline required Plaintiff and Class members to provide highly sensitive, confidential, personal and financial information as a condition of their employment, Driveline was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including

Plaintiff and Class members, for the safeguarding of employees' PII and wage information.

119. Driveline had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure income records and the PII of its employees.

120. Driveline breached its duty of care to Plaintiff and Class members to ensure that their PII and W-2 data was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by voluntarily disclosing the information, in an unencrypted format, to an unknown and unauthorized third party.

121. As a direct and proximate result of the Driveline actions alleged above, the Plaintiff and Class members have suffered actual damages.

FIFTH CAUSE OF ACTION
Violation of Illinois Personal Information Protection Act,
815 Ill. Comp. Stat. 530/1 *et seq*.
(On Behalf of Plaintiff and the Class)

122. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

123. By being headquartered in Illinois, employing Illinois residents, and collecting and storing the PII of those Illinois residents, Driveline is obligated to comply with the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. 530/1 *et seq*. ("IPIPA").

124. Driveline is a "data collector" under the provisions of IPIPA.

125. IPIPA requires a data collector that "maintains or stores… records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, … use, … or disclosure." IPIPA, 815 Ill. Comp. Stat. 530/45(a).

126. As detailed above, Driveline violated the IPIPA by disclosing its employees' PII to

unauthorized third parties.

127. As detailed above, Driveline violated the IPIPA by making the voluntary decision not to implement and maintain reasonable security measures to prevent the unauthorized disclosure of its employees' PII.

128. Driveline improperly and inadequately safeguarded the PII of Plaintiff and Class members in deviation of standard industry rules, regulations and practices regarding data security and data transmission at the time of the Data Disclosure.

129. Driveline 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.

130. Driveline, through its actions and/or omissions, violated the IPIPA by failing to have appropriate procedures in place to detect phishing scams and prevent unauthorized dissemination of its employees' PII.

131. As a direct and proximate result of the Driveline actions alleged above, the Plaintiff and Class members have suffered actual damages.

SIXTH CAUSE OF ACTION
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act,
815 Ill. Comp. Stat. 505/1 *et seq*.
(On Behalf of Plaintiff and the Class)

132. Plaintiff restates and realleges paragraphs 1- 75 above as if fully set forth herein.

133. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 530/20 ("ICFA") provides that a violation of the IPIPA "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

134. As detailed above, through its acts and omissions, Driveline violated the IPIPA by

failing to implement and maintain reasonable security measures to prevent the unauthorized disclosure of its employees' PII. Accordingly, Driveline's violation of the IPIPA constitutes a violation of the ICFA.

135. Further, Plaintiff and the other members of the Class were deceived by Driveline's failure to properly implement adequate, commercially reasonable security measures to protect its employees' PII.

136. Driveline intended for its employees, including Plaintiff and other members of the Class, to rely on Driveline to protect the PII furnished to it in connection with their employment and to store, use, and transmit the PII for business purposes only and only as authorized.

137. Instead, Driveline made an unauthorized disclosure of its employees' PII to unknown third parties.

138. Driveline failed to follow industry best practices concerning security in the storage, use, and transmission of PII or was negligent in preventing the Data Disclosure from occurring.

139. By transmitting an unencrypted file containing its employees' PII, it was foreseeable to Driveline that whoever came into possession of that email and/or file would have unfettered and unlimited access to, examination of, and use of highly confidential PII of Plaintiff and Class members.

140. It was foreseeable to Driveline that its willful indifference or negligent course of conduct in handling its employees' PII would put that information at risk of compromise or unauthorized disclosure.

141. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Defendant's deception that their PII information was secure and protected and would only be disclose as authorized when providing

Driveline this personal data as a condition of employment.

142. Driveline violated the ICFA by failing to properly implement adequate, commercially reasonable security measures to protect its employees' PII from unauthorized disclosure, by failing to warn its employees that their information was at risk of being compromised or disclosed without authorization, and by failing to discover and immediately notify its employees of the nature and extent of the Data Disclosure.

143. Driveline violated the ICFA by its voluntary decision to release an unencrypted file containing the PII of Plaintiff and Class members through an email transmission.

144. Plaintiff and members of the Class have suffered injury in fact and actual damages as a result of Driveline's violations of the ICFA.

PRAYER FOR RELIEF

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

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

B. A mandatory injunction directing Driveline to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Driveline 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 damages, in an amount to be determined;

E. For an award of attorneys' fees and costs;

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: September 10, 2019

Respectfully submitted,

/s/ *John A. Yanchunis*

JOHN A. YANCHUNIS*
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JEAN SUTTON MARTIN*
jeanmartin@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (813) 559-4908
Facsimile: (888) 316-3489

KEVIN S. HANNON*
khannon@hannonlaw.com
THE HANNON LAW FIRM, LLC
1641 Downing Street
Denver, CO 80218
Telephone: (303) 861-8800
Facsimile: (303) 861-8855

Shannon M. McNulty (Il. Bar. No. 6281984)
smm@cliffordlaw.com
CLIFFORD LAW OFFICES
120 N. LaSalle Street, Suite 3100
Chicago, IL 60602
Telephone: (312) 899-9090

Attorneys for Plaintiff and the Proposed Class

** admitted pro hac vice*