☐ YES ☑ NO

EXHIBITS

CASE NO. 2021 CH 47

DATE: 1/6/2021

CASE TYPE: Class Action

PAGE COUNT: 45

CASE NOTE

_____

_____

_____

Attorney No. 38819

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

ANAND EDKE, individually and on behalf of all others similarly situated,	)	2021CH00047 Case No.
Plaintiff,	)	
v.	)	**JURY TRIAL DEMANDED**
BELDEN, INC.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Anand Edke ("Plaintiff") brings this Class Action Complaint against Belden, Inc. ("Belden" or "Defendant") on behalf of himself and all others similarly situated and alleges, upon personal knowledge as to his own actions and his counsels' investigations and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Belden for its failure to properly secure and safeguard personally identifiable information that Belden required from its employees as a condition of employment, including without limitation, names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers for direct deposit of wages, and dates of birth (collectively, "personally identifiable information" or "PII"). Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former Belden employees ("Class Members") that their PII had been lost and precisely what types of information were unencrypted and are now in the possession of unknown third parties.

2. Belden is a provider of networking, connectivity, and cable products and operates worldwide. Belden's employees entrust Belden with an extensive amount of PII. Belden retains this information on computer hardware—even long after the employment relationship ends.

3. On or before November 12, 2020, Belden learned that a breach of its computer system had occurred, involving "a sophisticated attack by a party outside the company."[1]

4. Belden determined that the unauthorized activity on its network occurred on or before November 12, 2020. This activity involved the access and possible theft of PII, including unauthorized access to files on Belden's servers (the "Data Breach"). These servers contained files that in turn contained information about current and former employees, including Plaintiff, and their beneficiaries and dependents.

5. In a "Notice of Data Incident" published November 24, 2020, Belden advised current and former employees of Belden and their beneficiaries and dependants, of the Data Breach; this included current and former employees of certain of Belden's subsidiaries and former company subsidiaries, including Grass Valley USA, LLC.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII exposed to "unauthorized activity" included names, Social Security numbers or tax identification numbers, financial account numbers provided for direct deposit, home addresses, email addresses, dates of birth, and other, unspecified "general employment-related information."[2]

---

[1] *See Notice of Data Incident*, *available at*: https://oag.ca.gov/system/files/Breach%20Notification%20Template%20-%20%28Belden%29%20%28US%29.pdf, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").

[2] *Id.*

7. The exposed PII of Belden's current and former employees can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Belden's current and former employees and their beneficiaries and dependents face both an imminent and a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and bank account numbers.

8. This PII was compromised due to Belden's negligent and/or careless acts and omissions and the failure to protect PII of its current and former employees and their beneficiaries and dependents. In addition to Belden's failure to prevent the Data Breach, after discovering the breach, Belden waited several weeks to report it to the states' Attorneys General and affected individuals.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes, and is exacerbated by the theft of Plaintiff's and Class Members' Social Security numbers and other highly sensitive PII.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of its current and former employees and their beneficiaries and dependents; (ii) warn its current and former employees and their beneficiaries and dependents of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's

conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the Illinois Consumer Fraud and Deceptive Business Practices Act; and (v) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Belden 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 its current and former 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 are entitled to damages and, because they have a continuing interest in ensuring that their information is and remains safe, and they are also entitled to injunctive and other equitable relief.

PARTIES

13. Plaintiff Anand Edke is a resident of Schaumburg, Illinois. On or about December 16, 2020, Mr. Edke received notice from Belden that it improperly exposed his sensitive PII to unauthorized third parties. Mr. Edke worked for Belden from in or about February 2007 until February 2011 in Schaumburg, Illinois.

14. Defendant Belden, Inc. is a corporation organized under the laws of Delaware, headquartered at 1 North Brentwood Boulevard, 15th Floor, St. Louis, Missouri, 63105, with its principal place of business in St. Louis, Missouri.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

17. This Court has personal jurisdiction over Defendant because it operates within the State of Illinois and derives substantial revenue from its operations, and otherwise seeks the legal benefits and protections afforded by the State of Illinois. Additionally, this Court has jurisdiction over Defendant because Defendant is authorized to do business in the State of Illinois pursuant to 735 ILCS 5/2-102(a).

18. Venue is proper pursuant to 735 ILCS 5/2-101 because a substantial part of the events or omissions giving rise to these claims occurred in this County.

FACTUAL ALLEGATIONS

Background

19. Belden is a leading provider of networking equipment throughout the world. It

currently employs approximately 9,000 people and has thousands of former employees.[3]

20. Plaintiff and Class Members employed by Belden were required to provide some of their most sensitive and confidential information for themselves and their beneficiaries and dependents, including names, dates of birth, Social Security numbers, bank account numbers, and other PII which is often static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and the Class Members, as current and former employees and their beneficiaries and dependents, relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this highly sensitive PII. Current and former employees and their beneficiaries and dependents demand security to safeguard their PII.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure of their PII to third parties.

23. Defendant's headquarters were at one time located in Cook County, Illinois. In or about 2003, however, Defendant moved its headquarters from Cook County to St. Louis, Missouri.

24. However, subsequent to the relocation of its headquarters, Defendant continued to employ persons affected by this data breach in Illinois, including in Cook County, and even hired new employees, such as Plaintiff, to work for Defendant while residing and doing substantively all of their work in Illinois, including in Cook County.

25. On information and belief, Defendant resided in Cook County, Illinois at the time it took possession of the PII of some of the Class Members affected by the events detailed in this

[3] https://investor.belden.com/investor-resources/investor-faq/default.aspx (last accessed Dec. 24, 2020).

complaint.

The Data Breach

26. Beginning on or about November 24, 2020, Belden sent current and former employees and some business partners a *Notice of Data Incident*.[4] Belden informed the recipients of the notice that:

> On the evening of November 12, 2020, Belden IT professionals detected unusual activity involving certain company servers. We immediately triggered our cybersecurity incident response plan, deployed teams of internal IT specialists, and engaged leading third-party cybersecurity forensic experts and other advisors to identify the scope of the incident and move quickly to mitigate the impact. Forensics experts determined that we were the target of a sophisticated attack by a party outside the company. On or about November 15, 2020, we learned that the outside party accessed servers that contained personal information of some current and former employees.
>
> The personal information involved in this incident may have included your: name, birthdate, government-issued identification numbers (for example, social security number), bank account information (for North American employees on Belden payroll), home addresses, email addresses and other general employment-related information.[5]

27. On or about December 14, 2020, Belden sent data breach notifications to various state Attorneys General, including California's Attorney General, Xavier Becerra.[6]

28. Belden admitted in the *Notice of Data Incident* that there was unauthorized access to files that contained information about current and former employees and business partners, including names, birthdates, social security or tax identification numbers, financial accounts numbers provided to Belden for direct deposit, and other "employment-related information."

29. In response to the Data Breach, Belden claims that it notified law enforcement

---

4 *See* Ex. 1.

5 *Id.*

6 *See* https://oag.ca.gov/privacy/databreach/list (last accessed Dec. 29, 2020).

and worked to support the investigation. Defendant also states that it is "continuously monitoring for any suspicious activity on our systems and [has] deployed additional resources to reinforce the security of our systems."[7]

30. Additionally, other companies, former subsidiaries of Belden, such as Grass Valley USA, LLC, had employees or former employees who were affected because Belden held their employees' PII past their divestiture.[8]

31. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the affected current or former employees' approval. Unauthorized individuals can easily access the PII of Belden's current and former employees and their beneficiaries and dependents.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former employees and their beneficiaries and dependents, causing Plaintiff's and Class Members' PII to be exposed.

Belden Acquires, Collects and Stores Plaintiff's and Class Members' PII.

33. Belden has acquired, collected, and stored its current and former employees' PII from at least 2007 to 2020.

34. As a condition of maintaining employment with Belden, it requires its employees to entrust it with highly confidential PII.

35. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Belden

---

[7] *See* Ex. A at 1.

[8] *See* https://oag.ca.gov/system/files/Breach%20Notification%20Template%20-%20%28Grass%20Valley%29%20%28US%29.pdf (last accessed Dec. 30, 2020).

assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

36. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former employees, relied on Belden to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

37. Defendant could have prevented this Data Breach by properly securing and encrypting the files and servers containing Plaintiff's and Class Members' PII. Indeed, Belden could and should have destroyed the data, especially decade-old data from former employees, employees of former companies, and, on information and belief, the dependents and beneficiaries of both.

38. Defendant's negligence in safeguarding its employees', former employees', and their dependents' and beneficiaries' PII is exacerbated in light of the repeated warnings and alerts directed to companies warning them to protect and secure sensitive data.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

40. 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

[9] 17 C.F.R. § 248.201 (2013).

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]

41. The ramifications of Defendant's failure to keep its employees' and former employees' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers and bank account numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

42. Consumers' PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

43. 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. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and

---

[10] *Id*.

[11] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 29, 2020).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, last accessed Dec. 29, 2020.

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

44. 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.

45. 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."[15]

46. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued

---

[14] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 29, 2020).

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Dec. 29, 2020).

identification number, name, and date of birth.

47. This data 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."[16]

48. 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.

49. The fraudulent activity resulting from the Data Breach may not come to light for years.

50. 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.[17]

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding its employees' and former employees' PII, including Social Security numbers, bank account numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 29, 2020).

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Dec. 29, 2020).

significant costs that would be imposed on Defendant's current and former employees and their beneficiaries and dependents as a result of a breach.

52. 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.

53. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

54. To date, Defendant has offered its current and former employees only two years of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the highly sensitive PII at issue here.

55. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of its current and former employees and their beneficiaries and dependents.

Plaintiff Edke's Experience

56. From in or about February 2007 to February 2011, Plaintiff Anand Edke worked for Belden, Inc. and was based in Illinois. As a condition of employment, Belden required that he provide his sensitive PII, including but not limited to his name, date of birth, address, government issued identification numbers (including, for example, his driver's license and Social Security number), financial account information such as bank account numbers, email addresses, and other "general employment-related information," which could include his electronic

signature and personally identifying information for beneficiaries and/or dependents.

57. Mr. Edke received the Notice of Data Breach, dated December 16, 2020, on or about that date.

58. As a result of the Data Breach notice, Mr. Edke has spent time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Belden, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

59. Additionally, Mr. Edke has not been involved in any data breaches in the last five years, and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

60. Mr. Edke stores any documents containing his PII in a safe and secure location, or destroys the documents by shredding them. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

61. Mr. Edke suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Edke entrusted to Defendant for the purpose of his employment, which was compromised in, and as a result of, the Data Breach.

62. Mr. Edke suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

63. Mr. Edke has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

64. Mr. Edke has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

65. This action satisfies the prerequisites for maintenance as a class action pursuant to 735 ILCS 5/2-801, *et seq*., as set forth below.

66. Class Definition. Plaintiff brings this action individually and on behalf of the following class of similarly situated persons (the "Nationwide Class"), of which Plaintiff is a member:

> All individuals whose PII was compromised in the data breach first announced by Belden on or about November 24, 2020 (the "Class").

67. Additionally, Plaintiff brings this action individually and on behalf of the following class of similarly situated persons (the "Illinois Subclass"), of which Plaintiff is a member:

> All Illinois residents whose PII was compromised in the data breach first announced by Belden on or about November 24, 2020 (the "Illinois Subclass").

68. The Nationwide Class and the Illinois Subclass are collectively referred to herein as the "Class." Excluded from the Class and the Illinois Subclass are the presiding judge, Class counsel and any member of their immediate families. Plaintiff hereby reserves the right to amend the class definition based on discovery and the proofs at trial.

69. Numerosity. The members of the Class are so numerous that joinder of all members would be impracticable. The precise number of Class Members is unknown to Plaintiff

but is believed to be at least in the thousands. The true number of Class Members should be known by Defendant, however, and potential Class Members may be notified of the pendency of this action by first class mail, electronic mail, and/or published notice as appropriate and as determined by the court.

70. Commonality. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class Members. These common legal and factual questions include, inter alia, the following:

(1) Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

(2) Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

(3) Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

(4) Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

(5) Whether and when Defendant actually learned of the Data Breach;

(6) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

(7) Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

(8) 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 Breach;

(9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(10) Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct; and

(11) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

71. Typicality. The claims of Plaintiff are typical of the claims of the members of the Class because, *inter alia*, all Class Members were injured through the uniform misconduct described above. Plaintiff is advancing the same claims and legal theories on behalf of himself and all members of the Class.

72. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained highly competent counsel and experienced class action attorneys to represent his interests and that of the Class. Plaintiff and his counsel have the necessary financial resources to adequately and vigorously litigate this class action. Plaintiff has no adverse or antagonistic interests to those of the Class. Plaintiff is willing and prepared to serve the Court and the Class Members in a representative capacity with all of the obligations and duties material thereto and is determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class Members.

73. Appropriateness. A class action is an appropriate method for the fair and efficient adjudication of this controversy. The common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class. Also, the likelihood that individual members of the Class will prosecute separate actions is remote due to the

extensive time and considerable expense necessary to conduct such litigation, especially in view of the relatively modest amount of monetary relief at issue for individual Class Members.

74. A class action will cause an orderly and expeditious administration of the claims of the Class. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

75. Plaintiff does not anticipate any undue difficulty in the management of this litigation.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

76. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 75.

77. As a condition of their employment with Defendant, Defendant's current and former employees were obligated to provide Defendant with certain PII, including their names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, and dates of birth and those of their beneficiaries and dependents.

78. Plaintiff and the Class Members entrusted their PII and that of their beneficiaries and dependents to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

79. Defendant has 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.

80. Defendant knew or reasonably should have known that the failure to exercise due

care in the collecting, storing, and using of their current and former employees' PII, and that of their beneficiaries and dependents, involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

81. 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's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

82. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

83. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

84. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of 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, and the necessity for encrypting PII stored on Defendant's systems.

85. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant.

86. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

87. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

88. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised 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. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

90. Defendant has admitted that the PII of Plaintiff and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

91. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

92. Defendant 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 Breach.

93. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former employees' PII in the face of increased risk of theft.

94. Defendant, 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 and prevent dissemination of its current and former employees' PII.

95. Defendant, 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 Breach.

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

97. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

98. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

99. Additionally, as a direct and proximate result of Belden's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Belden's possession and is subject to further unauthorized disclosures so long as Belden fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Belden from engaging in the wrongful and unlawful acts described herein;

ii. requiring Belden to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Belden to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Belden can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Belden to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Belden from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Belden to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Belden's systems on a periodic basis, and ordering Belden to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Belden to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Belden to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Belden to segment data by, among other things, creating firewalls

and access controls so that if one area of Belden's network is compromised, hackers cannot gain access to other portions of Belden's systems;

x. requiring Belden to conduct regular database scanning and securing checks;

xi. requiring Belden to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Belden to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Belden to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Belden's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Belden to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Belden's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Belden to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Belden to implement logging and monitoring programs sufficient to track traffic to and from Belden's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Belden's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For pre- and post-judgment interest on all amounts awarded; and

F. Such other and further relief as this Court may deem just and proper.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

100. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 75.

101. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC

publications and orders described above also form part of the basis of Defendant's duty in this regard.

102. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue in this case—including Social Security numbers.

103. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

104. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

105. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

106. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud

and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former employees in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

107. Additionally, as a direct and proximate result of Belden's negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Belden's possession and is subject to further unauthorized disclosures so long as Belden fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Belden from engaging in the wrongful and unlawful acts described herein;

ii. requiring Belden to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Belden to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Belden can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Belden to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Belden from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Belden to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Belden's systems on a periodic basis, and ordering Belden to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Belden to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

viii. requiring Belden to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Belden to segment data by, among other things, creating firewalls and access controls so that if one area of Belden's network is compromised, hackers cannot gain access to other portions of Belden's systems;

x. requiring Belden to conduct regular database scanning and securing checks;

xi. requiring Belden to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Belden to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Belden to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Belden's policies, programs, and systems for

protecting personal identifying information;

xiv. requiring Belden to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Belden's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Belden to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Belden to implement logging and monitoring programs sufficient to track traffic to and from Belden's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Belden's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For pre- and postjudgment interest on all amounts awarded; and

F. Such other and further relief as this Court may deem just and proper.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

108. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 75.

109. Plaintiff and Class Members were required to provide their PII, including names, addresses, Social Security numbers, driver's license numbers, financial account numbers, and other personal information, to Defendant as a condition of their employment.

110. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

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

112. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not perform its obligations.

113. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PII, which was disclosed to unauthorized third parties by Defendant's failure to properly secure its sensitive data.

114. Defendant'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.

115. As a direct and proximate result of Defendant'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 Breach, 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of 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 Breach for the remainder of the lives of Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive

and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Belden from engaging in the wrongful and unlawful acts described herein;

ii. requiring Belden to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Belden to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Belden can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Belden to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Belden from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Belden to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Belden's systems on a periodic basis, and ordering Belden to promptly correct any problems or issues detected by such third-party security

auditors;

vii. requiring Belden to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Belden to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Belden to segment data by, among other things, creating firewalls and access controls so that if one area of Belden's network is compromised, hackers cannot gain access to other portions of Belden's systems;

x. requiring Belden to conduct regular database scanning and securing checks;

xi. requiring Belden to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Belden to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Belden to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the

preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Belden's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Belden to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Belden's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Belden to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Belden to implement logging and monitoring programs sufficient to track traffic to and from Belden's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Belden's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

FOURTH CLAIM FOR RELIEF
Violation of Illinois Personal Information ProtectionAct,
815 Ill. Comp. Stat. 530/1, *et seq*.
(On Behalf of Plaintiff and the Illinois Subclass)

116. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 75.

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

118. Defendant is a "data collector" within the meaning of IPIPA.

119. IPIPA requires a data collector that "maintains or stores ... records that contain personal information concerning an Illinois resident" to "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).

120. Defendant violated IPIPA by failing to implement and maintain reasonable security measures to protect the records of Illinois residents from unauthorized access, acquisition, use, or disclosure.

121. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Illinois Subclass members in deviation of standard industry rules, regulations and practices regarding data security and data transmission at the time of the Data Breach.

122. Defendant, through its actions and/or omissions, violated the IPIPA by failing to have appropriate procedures in place to prevent unauthorized access or dissemination of its employees' PII.

123. As a direct and proximate result of the actions alleged above, Plaintiff and Illinois Subclass members have suffered actual damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Illinois Subclass members, requests judgment against the Defendant and the following:

A. For an Order certifying the Illinois Subclass as defined herein, and appointing Plaintiff and his counsel to represent the Illinois Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Illinois Subclass members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Belden from engaging in the wrongful and unlawful acts described herein;

ii. requiring Belden to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Belden to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Belden can provide to

the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Belden to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Belden from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Belden to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Belden's systems on a periodic basis, and ordering Belden to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Belden to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Belden to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Belden to segment data by, among other things, creating firewalls and access controls so that if one area of Belden's network is compromised, hackers cannot gain access to other portions of Belden's systems;

x. requiring Belden to conduct regular database scanning and securing checks;

xi. requiring Belden to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Belden to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Belden to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Belden's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Belden to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Belden's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Belden to meaningfully educate all Class Members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Belden to implement logging and monitoring programs sufficient to track traffic to and from Belden's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Belden's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff, on Behalf of the Nationwide Class)

124. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 75.

125. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their PII with Defendant in such away that saved expense and labor for Defendant.

126. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' PII, as this was used by Defendant to facilitate human resources functions.

127. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

128. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

129. Under principals of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

130. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

the Class Members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Belden from engaging in the wrongful and unlawful acts described herein;

ii. requiring Belden to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Belden to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Belden can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Belden to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Belden from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Belden to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits

on Belden's systems on a periodic basis, and ordering Belden to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Belden to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Belden to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Belden to segment data by, among other things, creating firewalls and access controls so that if one area of Belden's network is compromised, hackers cannot gain access to other portions of Belden's systems;

x. requiring Belden to conduct regular database scanning and securing checks;

xi. requiring Belden to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Belden to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Belden to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Belden's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Belden to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Belden's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Belden to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Belden to implement logging and monitoring programs sufficient to track traffic to and from Belden's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Belden's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For pre- and postjudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial for all matters so triable.

DATED: January 6, 2021

Respectfully Submitted,

By: *Carl V. Malmstrom*

Carl Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Attorney No. 38819
malmstrom@whafh.com
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: 312/984-0000
Facsimile: 212/545-4653
M. ANDERSON BERRY (*Pro Hac Vice Forthcoming*)
LESLIE GUILLON
ARDC No. 6279810
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
aberry@justice4you.com
lguillon@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

whafhch56165