IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT
DUPAGE COUNTY, ILLINOIS

CARLA PLOWMAN, on behalf of herself and all others similarly situated, Plaintiff, v. TY INC., Defendant.	Case No. 2024CH000205 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Carla Plowman ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, Ty Inc., ("Defendant"):

INTRODUCTION

1. On April 26, 2023, Ty Inc., the largest manufacturer of stuffed plush toys in the world and best known for its beanie babies craze, lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach perpetrated by cybercriminals ("Data Breach").

2. Due to its intentionally obfuscating language, it is unknown when the Data Breach actually occurred and how long cybercriminals had unfettered access to Plaintiff's and the Class's sensitive and private information. Following discovery of the Breach on April 26, 2023, Ty Inc., conducted an internal investigation and learned cybercriminals gained unauthorized access to thousands of current and former employees' personally identifiable information ("PII") and protected health information ("PHI") (collectively with PII, "Sensitive Information").

3. On or about September 15, 2023–five months after the Data Breach occurred– Ty Inc., finally began notifying Class Members about the Data Breach ("Breach Notice"), an example

of which is attached as Exhibit A. However, notice is ongoing, with Plaintiff not receiving her notice until October 2023.

4. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the Sensitive Information of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's Sensitive Information—rendering them easy targets for cybercriminals.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Defendant five months to begin notifying victims that cybercriminals had gained access to their highly private information.

6. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Sensitive Information misuse.

8. In failing to adequately protect its employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former employees.

9. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant

with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff Carla Plowman is a former Ty Inc. employee and Data Breach victim.

11. The exposure of one's Sensitive Information to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

12. Plaintiff, Carla Plowman, is a natural person and citizen of Illinois, residing in Westmont, Illinois, where she intends to remain.

13. Defendant, Ty Inc., is incorporated in Delaware, with its principal place of business at 280 Chestnut Avenue, Westmont, IL 60559. Defendant can be served through its registered agent Joseph B. Brocato at 1 East Wacker Drive, Suite 1700, Chicago, IL 60601.

JURISDICTION & VENUE

14. This Court has subject-matter jurisdiction over this action under Ill. Const. art. VI, § 9.

15. This Court has general personal jurisdiction over Ty Inc. under 735 ILCS § 5/2-209 because it is headquartered in Illinois.

16. Venue is proper in this Court under 735 ILCS § 5/2-101(2) because some part of the transactions out of which the cause of action arose occurred in DuPage County. Specifically, Plaintiff's injuries arising out of the Data Breach occurred in, and were felt in, DuPage County.

FACTUAL ALLEGATIONS

Ty Inc.

17. Ty Inc. is an Illinois company that touts itself as "an American multinational corporation" with "over 30 years of experience" and is currently the "largest manufacturer of

stuffed plush toys in the world."[1] It boasts over $68.3 million in annual revenue.[2]

18. On information and belief, Ty Inc. accumulates highly private Sensitive Information of its employees.

19. In collecting and maintaining its employees' Sensitive Information, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information.

20. As the largest manufacturer in the stuffed plush toy industry, Ty Inc. understood the need to protect its current and former employees' Sensitive Information and prioritize its data security.

21. Despite recognizing its duty to do so, on information and belief, Ty Inc. has not implemented reasonably cybersecurity safeguards or policies to protect employee Sensitive Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Ty Inc. leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' Sensitive Information.

Ty Inc. Fails to Safeguard Employees' Sensitive Information

22. Plaintiff is a former employee of Ty Inc.

23. As a condition of employment with Ty Inc., Plaintiff provided Defendant with her Sensitive Information, including but not limited to her name, medical information, address, and Social Security number. Defendant used that Sensitive Information to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that Sensitive Information to obtain employment and payment for that employment.

24. On information and belief, Ty Inc. collects and maintains employees' unencrypted

[1] TY Inc., About Us, https://tynordic.com/about/ (last visited November 14, 2023).
[2] TY Inc., Zoominfo, https://www.zoominfo.com/c/ty-inc/39191442 (last visited November 14, 2023).

Sensitive Information in its computer systems.

25. In collecting and maintaining Sensitive Information, Defendant implicitly agreed that it will safeguard the data using reasonable means according to their state and federal law.

26. Indeed, Ty Inc. promises in its privacy policy that it "will not share your personal information with third parties without your consent" and "firmly believes in safety and privacy on the internet and does not collect information about or disclose the identity of children on the Internet without prior parental approval, nor does it disclose the identity of adults without prior approval."[3]

27. According to the Breach Notice, Ty Inc. claims that "on April 26, 2023, Ty Inc. identified suspicious activity in its corporate computer network." Ty Inc. further admits that an internal investigation revealed that "an unauthorized party access or acquired certain files stored on servers in the network." Ex. A.

28. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees' highly private information.

29. Additionally, Defendant admitted that Plaintiff's and the Class's Sensitive Information were actually stolen during the Data Breach, confessing that the information was not just accessed but that the cybercriminals had "**acquired** certain files stored on [its network.]" (Emphasis added) Ex. A.

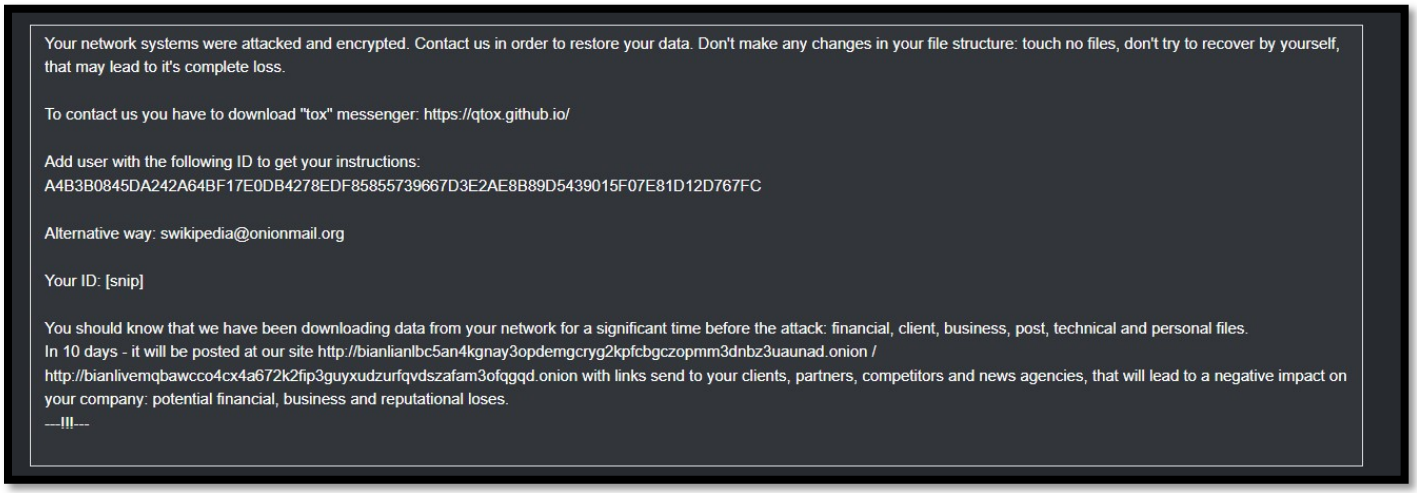
30. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

31. Upon information and belief, the notorious BianLian ransomware gang was

[3] Privacy Policy, Ty Inc., https://shop.ty.com/privacypolicy.html?lang=en (last visited November 14, 2023).

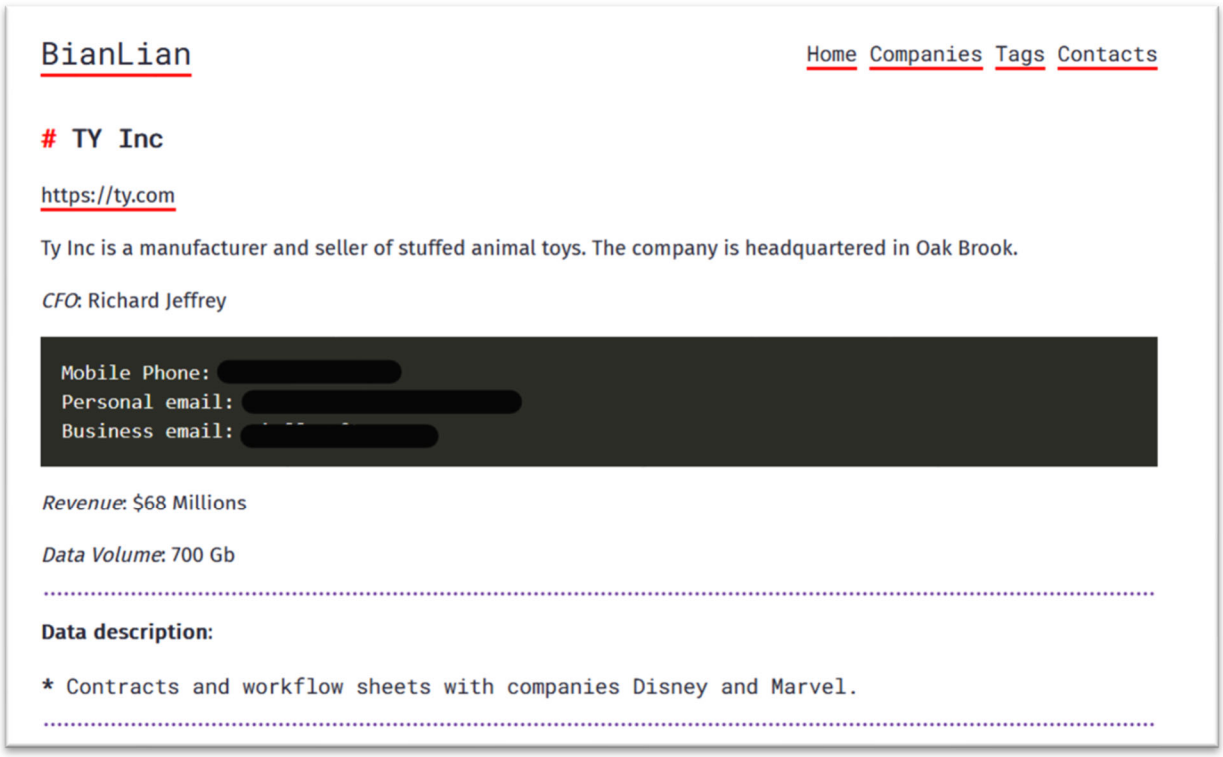
responsible for the cyberattack. Known as one of the most notorious and active ransomware actors, BianLian has perpetrated at least 116 data breaches in the last year alone.[4] Ty Inc. knew or should have known of the tactics that groups like BianLian employ.

32. With the Sensitive Information secured and stolen by BianLian, the hackers then purportedly issued a ransom demand to Ty Inc. However, Ty Inc. has provided no public information on the ransom demand or payment. BianLian's standard ransom demand page is shown below:



33. On September 14,2023, the presumed deadline of BianLian ransom demand, BianLian released information obtained from the Breach on a data leak page. On information and belief, all stolen information was released onto the data leak page[5]:

[4]BianLian Ransomware Pivots from Encryption to Pure Data-Theft Extortion, DarkReading, https://www.darkreading.com/risk/bianlian-ransomware-pivots-encryption-pure-data-theft-extortion (last visited November 14, 2023).
[5] News, HackManac, https://hackmanac.com/news/hacks-of-today-03-04-05-06-2023 (last visited November 14, 2023).



34. On or about September 15, 2023–five months after the Data Breach first occurred–Ty Inc. finally began notifying Class Members about the Data Breach.

35. Despite its duties to safeguard Sensitive Information, Defendant, a self-proclaimed leader in its industry, did not in fact follow industry standard practices in securing employees' Sensitive Information, as evidenced by the Data Breach.

36. In response to the Data Breach, Ty Inc. contends that it has "implemented additional safeguards and security measures." Ex. A. Although Defendant fails to expand on what these alleged "safeguards and measures" are, such actions, if implemented at all, should have been in place before the Data Breach.

37. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for

any unauthorized activity" and if "you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state." Ex. A

38. Ty Inc. further recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards and/or policies to protect its employees' Sensitive Information, insisting that "we wanted to […] assure you that we take this seriously" and "apologize for any concern or inconvenience this incident may cause" acknowledging that as a result of the Breach, Ty Inc. must now try to "relieve concerns and restore confidence following this [Breach.]"Ex. A.

39. On information and belief, Ty Inc. has offered a one year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

40. Even with one year of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Ty Inc. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, Ty Inc. failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures,

causing it to lose control over its employees' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

43. It is well known that Sensitive Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[6]

45. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Ty Inc. knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Sensitive Information private and secure, Defendant failed to take appropriate steps to protect the Sensitive Information of Plaintiff and Class Members from being compromised.

48. In the years immediately preceding the Data Breach, Defendant knew or should

[6] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 4, 2023).

have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

49. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[7]

50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[8]

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[9]

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities

---

[7] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed September 4, 2023).

[8] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed September 4, 2023).

[9] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed September 4, 2023).

such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

53. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Sensitive Information of thousands of its current and former employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Sensitive Information and Defendant's type of business had cause to be particularly on guard against such an attack.

54. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Sensitive Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

55. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees' Social Security numbers and other sensitive data elements within the Sensitive Information to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

56. Plaintiff Carla Plowman is a former employee of Defendant and received a Data Breach notice in October 2023.

57. As a condition of employment, Ty Inc. required Ms. Plowman to provide her Sensitive Information, including at least her name, address, medical information, and Social Security Number.

58. Ms. Plowman provided her Sensitive Information to Ty Inc. and trusted that the

company would use reasonable measures to protect it according to state and federal law.

59. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for six months.

60. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

61. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

62. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information. After all, Sensitive Information is a form of intangible property—property that Defendant was required to adequately protect.

63. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

64. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring her credit information.

65. Plaintiff has already spent at least twelve hours and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the

law contemplates and addresses.

66. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach.

67. Indeed, following the Data Breach, Plaintiff's People's Bank debit account was compromised three times, including at least one fraudulent charge totaling $70.00 from the clothing brand Shein that Plaintiff did not recognize nor authorize, suggesting Plaintiffs' Sensitive Information is now in the hands of cybercriminals. As a result of the numerous compromises to her debit account, Plaintiff was forced close her account entirely.

68. Additionally, following the Data Breach Plaintiff has experienced an increase in spam calls, further suggesting that her Sensitive Information is now in the hands of cybercriminals.

69. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

70. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

71. As a result of Ty Inc.'s failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

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

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

72. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

73. The value of Plaintiff's and the proposed Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

74. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover,

Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

75. It can take victims years to spot identity or Sensitive Information theft, giving criminals plenty of time to use that information for cash.

76. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

77. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

78. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

79. Defendant disclosed the Sensitive Information of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people

engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

80. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

81. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

82. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

83. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

84. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

87. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients, or in this case, employees' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [10]

88. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and

[10] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

PHI is properly maintained.[11]

89. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

[11] See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

90. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrates Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Failed to Follow Industry Standards

91. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

92. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

93. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

95. Plaintiff is suing on behalf of herself and the proposed Class ("Class"), defined as follows:

> **All individuals residing in the United States whose Sensitive Information was compromised in Defendant's Data Breach, including all those who received notice of the breach.**

96. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

97. Plaintiff reserves the right to amend the class definition.

98. This action satisfies the numerosity, commonality, adequacy, and appropriateness requirements under 735 ILCS § 5/2-801(1)- (4):

a. **Numerosity**. Plaintiff's claim is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claim is typical of Class member's claims as each

arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interest does not conflict with Class members' interests, and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. 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;

iii. Whether Defendant was negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

f. **Appropriateness**. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

g. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

99. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

100. Plaintiff and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

101. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards for data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of

Plaintiff's and members of the Class's Sensitive Information by disclosing and allowing access to employee Sensitive Information to unknown third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who made that happen.

102. Moreover, Defendant owed Plaintiff and the Class a fiduciary duty of confidentiality, as Defendant was the employer of the employees affected.

103. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. These duties are required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

104. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's Sensitive Information for employment. Plaintiff and members of the Class needed to provide their Sensitive Information to Defendant as prospective employees, as a condition of employment. Defendant negligently retained this information.

105. The risk that unauthorized persons would try to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would try to access Defendant's

databases containing the Sensitive Information —whether by malware or otherwise.

106. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

107. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Sensitive Information of Plaintiff and members of the Class. These failures actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

108. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

109. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including but not limited to monetary damages, loss of privacy, lost time, loss of value of Sensitive Information, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

110. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by

Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

111. Moreover, pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's Sensitive Information.

112. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's Sensitive Information. 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, of failing to use reasonable measures to protect customers or, in this case, employees' Sensitive Information.

113. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

114. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

115. Defendant had a duty to Plaintiff and the members of the Class to implement and

maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's Sensitive Information.

116. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's Sensitive Information.

117. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and their employees, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

118. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

119. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

120. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach,

including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

121. Defendant's violation of Section 5 of the FTC Act and HIPAA as well as its failure to comply with applicable laws and regulations constitutes negligence *per se*.

122. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

123. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

124. Had Plaintiff and members of the Class known that Defendant did not adequately protect employees' Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

125. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiff and members of the Class paid for that they would not have sought had they known of Defendant's careless approach to cyber security; lost control over the value of Sensitive Information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

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

126. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

127. Defendant offered to employ Plaintiff and members of the Class if, as a condition of that employment, Plaintiff and members of the Class provided Defendant with their Sensitive Information.

128. In turn, Defendant agreed it would not disclose the Sensitive Information it collects to unauthorized persons. Defendant also promised to safeguard employee Sensitive Information.

129. Plaintiff and the members of the Class accepted Defendant's offer by providing Sensitive Information to Defendant in exchange for employment with Defendant.

130. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Sensitive Information.

131. Plaintiff and the members of the Class would not have entrusted their Sensitive Information to Defendant in the absence of such an agreement with Defendant.

132. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Sensitive Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Sensitive

Information that Defendant created, received, maintained, and transmitted.

133. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

134. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

135. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

136. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

137. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

138. In these and other ways, Defendant violated its duty of good faith and fair dealing.

139. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

140. Plaintiff, on behalf of herself and the Class, seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity

theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

141. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

142. This claim is plead in the alternative to the breach of implied contractual duty claim.

143. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate their employment.

144. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

145. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their Sensitive Information.

146. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FOURTH CLAIM FOR RELIEF
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS § 505/1, *et seq.*
(On Behalf of the Plaintiff and the Class)

147. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

148. The Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS § 530/20

provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505/1, et seq. ("ICFA"), which prohibits unfair and deceptive acts or practices in the conduct of trade and commerce.

149. Defendant is a "data collector" under IPIPA. As a data collector, Defendant owns or licenses information concerning Illinois residents.

150. The 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 ILCS § 530/45(a).

151. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." IPIPA, 815 ILCS § 530/10(a).

152. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiff's and the Class's Sensitive Information. Defendant further violated the IPIPA by failing to give Plaintiff and the Class expedient notice without unreasonable delay.

153. As a direct and proximate cause of Defendant's failures, Plaintiff and the Class have suffered actual damages.

154. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of the IPIPA and the ICFA, which includes the costs of future monitoring of their credit

history for identity theft and fraud, plus attorneys' fees, prejudgment interest, and costs.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

155. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

156. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

157. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

158. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Sensitive Information is highly offensive to a reasonable person.

159. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

160. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

161. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

162. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation

efforts.

163. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

164. As a proximate result of Defendant's acts and omissions, the private Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

165. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their Sensitive Information are still maintained by Defendant with its inadequate cybersecurity system and policies.

166. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiff and the Class.

167. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent

the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: August 12, 2024

Respectfully submitted,

By: */s/ Cassandra Miller*

Cassandra Miller (SBN 6290238)
Samuel J. Strauss (SBN 6340331)
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
DuPage Attorney No. 382570
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
cmiller@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

**pro hac vice* anticipated

Attorneys for Plaintiff and the Proposed Class

— EXHIBIT A —

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_2(Subject header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Ty Inc. is writing to notify you of an incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking.

What Happened? On April 26, 2023, Ty Inc. identified suspicious activity in its corporate computer network. Upon detection, we quickly took steps to secure our network and launch an investigation. The investigation determined that an unauthorized party accessed or acquired certain files stored on servers in the network.

What Information Was Involved? To determine if any of the files contained personal information, we reviewed the information contained in the files that may have been involved in the incident. Based on this review, on July 18, 2023, we determined that the data included your <<b2b_text_1(data elements)>>.

What We Are Doing. To help prevent something like this from happening again, we have implemented additional safeguards and security measures. As a precaution, we are offering you a complimentary one-year membership to Kroll's identity monitoring service, which includes Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do. We wanted to let you know this happened and assure you that we take this seriously. For more information on Kroll's identity monitoring services, as well as some additional steps you can take in response, please see the pages that follow this letter.

For More Information. We apologize for any concern or inconvenience this incident may cause. If you have any questions about this incident, please call (866) 731-2920, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

Sincerely,

Ty Inc.

KROLL

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.
To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.
For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That is because most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Ty Inc. is located at 280 Chestnut Avenue, Westmont, IL 60559, and can be reached by telephone at (630) 920-1515.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.