UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

AUGUSTYN WIACEK, individually and on behalf of all others similarly situated, Plaintiff, v. MONDELEZ GLOBAL LLC, MONDELEZ INTERNATIONAL HOLDINGS LLC, MONDELEZ INTERNATIONAL, INC., and BRYAN CAVE LEIGHTON PAISNER LLP, Defendants.	Case No. 1:23-cv-04023 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Augustyn Wiacek ("Mr. Wiacek" or "Plaintiff") brings this action on behalf of himself, and all others similarly situated against Defendant, Mondelez Global LLC, Mondelez International Holdings LLC, Mondelez International, Inc., (together "Mondelez") and Bryan Cave Leighton Paisner LLP ("BCLP") (collectively with Mondelez, "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. Between February 23, 2023, and March 1, 2023, BCLP, a law firm with "extensive experience handling the full scope of complex privacy and security issues"[1], lost control over its client Mondelez's current and former employees' highly sensitive personal information in a data breach perpetuated by cybercriminals ("Data Breach"). On information and belief, the Data Breach

[1] Data Privacy & Secuirity, BCLP, https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html (last visited March 16, 2023).

affected over 51,000 individuals.[2]

2. Mondelez chose to allow BCLP access and control over its current and formers' employees' highly sensitive personal information.

3. On information and belief, the Data Breach began on or around February 23, 2023, when an unauthorized party gained access to BCLP's network, and was not discovered by BCLP until four days later, on February 27, 2022. Shockingly, despite discovering the Data Breach, BCLP allowed the Data Breach to continue for at least two more days, providing cybercriminals unfettered access to Mondelez former and current employees' highly private information for an entire week.

4. Following an internal investigation, BCLP learned cybercriminals had gained unauthorized access to Mondolez's employees' personally identifiable information ("PII") including but not limited to their names, Social Security number, address, date of birth, gender, employee identification number, and retirement and/or thrift plan information.

5. On information and belief, cybercriminals bypassed BCLP's inadequate security systems to access Mondelez's employees' PII in its computer systems.

6. On or around March 24, 2023, Mondelez, "one of the world's largest snacks companies"[3] was first notified by BCLP that its current and former employees' PII were involved in the Data Breach.

7. On or about June 15, 2023 –almost four months after the unauthorized party first gained access to employees' PII and three months after Mondelez first learned of the Data Breach from BCLP – Mondelez finally notified Class Members about the Data Breach ("Breach Notice")

[2] Mondelēz retirement data breached after hacker targets law firm Bryan Cave, Cybersecurity Dive, https://www.cybersecuritydive.com/news/mondelez-retirement-hacker-targets-law-firm/653600/ (last visited June 23, 2023).
[3] About us, Modelez, https://www.mondelezinternational.com/ (last visited June 23, 2023).

an example of which is attached as **Exhibit A**. However, notification is ongoing, with Plaintiff not receiving his notice until June 21, 2023.

8. Mondelez's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Mondelez almost three months to begin notifying victims that hackers had gained access to highly sensitive PII.

9. Defendants' failure to timely detect and 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 PII.

10. Defendants 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 PII misuse.

11. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of its current and former employees.

12. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their PII. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff Augustyn Wiacek is a Data Breach victim.

14. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in

Defendants' possession.

PARTIES

15. Plaintiff, Augustyn Wiacek, is a natural person and citizen of New York, where he intends to remain. Plaintiff Wiacek is a Data Breach victim, receiving the Breach Notice on June 21, 2023.

16. Defendant, Mondelez Global LLC, is a Delaware LLC with its principal place of business at 905 West Fulton Market Ste 200, Chicago, IL 60607-1308.

17. Defendant, Mondelez International Holdings LLC, is a Delaware LLC, with its principal place of business at 905 West Fulton Market Ste 200, Chicago, IL 60607-1308.

18. Defendant, Mondelez International, Inc., is a Virginia Corporation with its principal place of business at 208 South Lasalle St, Suite 814 Chicago, IL 60604.

19. Defendant, BCLP, is a Missouri Corporation, with its principal place of business at 221 Bolivar Street Jefferson City, MO 65101. Defendant can be served through its registered agent, CSC- Lawyers Incorporating Service Company, at 221 Bolivar Street Jefferson City, MO 65101.

JURISDICTION & VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and Defendants are citizens of different states.

21. This Court has personal jurisdiction over Defendants because at least one Defendant maintains its principal place of business in this District and does substantial business in this District.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

BCLP

23. BCLP is a law firm that touts itself as "groundbreakers and innovators"[4] that has "extensive experience handling the full scope of complex privacy and security issues."[5] BCLP boasts a total annual revenue of 900 million.[6]

24. BCLP's services are specialized for companies "including 35% of the Fortune 500"[7] who manage highly sensitive data. BCLP thus must oversee, manage, and protect the PII of its clients' consumers, including Mondelez's current and former employees.

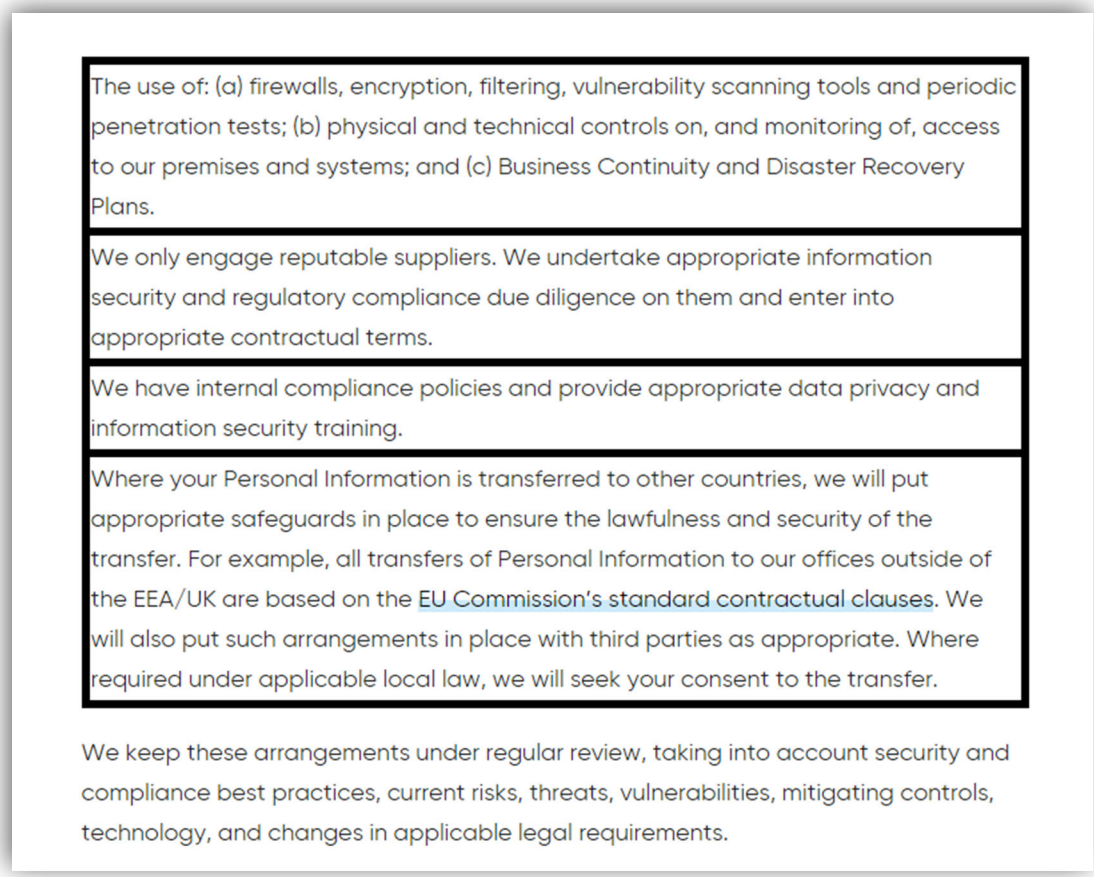
25. Indeed, BCLP advertises that it "routinely advise clients in a variety of sectors, including hospitality, consumer services, healthcare, software and technology, financial services, travel, manufacturing, and retail" about how "to achieve the most streamlined international data privacy strategy as possible, and we excel at helping companies achieve their business goals while balancing and addressing privacy and security obligations".[8]

26. On information and belief, these third-party employees, whose PII was collected by BCLP, do not do any business with BCLP.

---

[4] About us, BCLP, https://www.bclplaw.com/en-US/about/about-bclp.html (last visited June 23, 2023).
[5] Data Privacy & Security, BCLP, https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html (last visited March 16, 2023).
[6] BCLP Revenue, Zippia, https://www.zippia.com/bryan-cave-careers-17522/revenue/ (last visited June 23, 2023).
[7] About us, BCLP, https://www.bclplaw.com/en-US/about/about-bclp.html (last visited June 23, 2023).
[8] Data Privacy and Security, BCLP, https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html#overview (last visited June 23, 2023).

27. In working with third party employees' highly sensitive data, BCLP assures that it "understand the importance of keeping your Personal Information secure"[9], boasting that it employs a plethora of ways to ensure the security of PII:



The use of: (a) firewalls, encryption, filtering, vulnerability scanning tools and periodic penetration tests; (b) physical and technical controls on, and monitoring of, access to our premises and systems; and (c) Business Continuity and Disaster Recovery Plans.

We only engage reputable suppliers. We undertake appropriate information security and regulatory compliance due diligence on them and enter into appropriate contractual terms.

We have internal compliance policies and provide appropriate data privacy and information security training.

Where your Personal Information is transferred to other countries, we will put appropriate safeguards in place to ensure the lawfulness and security of the transfer. For example, all transfers of Personal Information to our offices outside of the EEA/UK are based on the EU Commission's standard contractual clauses. We will also put such arrangements in place with third parties as appropriate. Where required under applicable local law, we will seek your consent to the transfer.

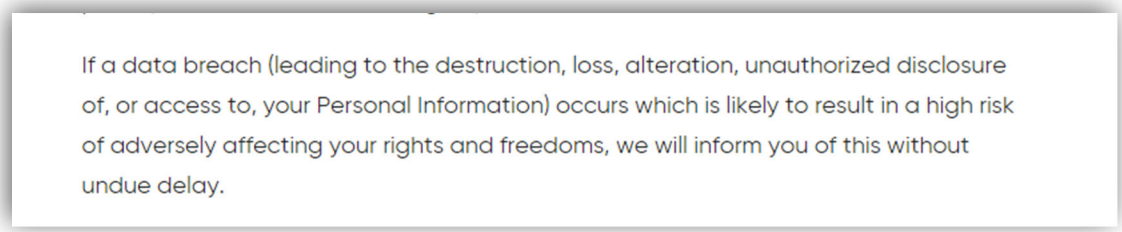
We keep these arrangements under regular review, taking into account security and compliance best practices, current risks, threats, vulnerabilities, mitigating controls, technology, and changes in applicable legal requirements.

28. BCLP also claims that it has "a world class incident response practice that has helped clients navigate major security incidents and data breaches, including ransomware attacks", stating that it "leverage[s] that experience to help companies identify and remediate gaps in their readiness and to train companies how to respond to breaches effectively."[10]

[9] Privacy Notice, BCLP, https://www.bclplaw.com/en-US/legal-notices/privacy-notice.html(last visited June 23, 2023).

[10] Data Privacy & Security, BCLP, https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html (last visited March 16, 2023).

29. BCLP promises that, in the event of a data breach, it will "inform you of this without undue delay".[11]



30. As a self-proclaimed "leader" in data Privacy and Security firm and handling highly sensitive aspects of its clients' business, BCLP understood the need to protect its client's employee's data and prioritize its data security. In fact, BCLP advertises that its "experience and practical approach to data breach response uniquely equip us to assist organizations by understanding both the law and the business implications of data breaches."[12]

31. But, on information and belief, BCLP fails to strictly adhere to these policies in maintaining its client's employees' PII.

Mondelez

32. Mondelez is "one of the world's largest snacks companies"[13] that "[has] operations in more than 80 countries and employ[s] approximately 91,000 diverse and talented employees [] around the world."[14] Mondelez boasts a total revenue of 31 billion.[15]

33. In its privacy policy, Mondelez promises that "protecting your personal information is important to us" and that it "maintain[s] administrative, technical, and physical safeguards

[11] *Id*.
[12] *Id*.
[13] About us, Mondelez, https://www.mondelezinternational.com/About-Us (last visited June 23, 2023).
[14] *Id*.
[15] Investor Release Details, Mondelez, https://ir.mondelezinternational.com/news-releases/news-release-details/mondelez-international-reports-q4-and-fy-2022-results (last visited June 23, 2023).

designed to help protect against unauthorized use, disclosure, alteration, or destruction of the personal information we collect on our Sites." [16]

34. As part of its business, Mondelez receives and maintains the PII of thousands of current and former employees. In doing so, Mondelez implicitly promises to safeguard their PII.

35. In collecting and maintaining its current and former employees' PII, Mondelez agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

36. Despite recognizing its duty to do so, on information and belief, Mondelez has not implemented reasonably cybersecurity safeguards or policies to protect its employees' PII or supervised its IT or data security agents and employees, including BCLP, to prevent, detect, and stop breaches of its systems. As a result, Mondelez left significant vulnerabilities in its storage of Plaintiff's and the Class's PII for cybercriminals to exploit and gain access to employees' PII.

The Data Breach

37. Plaintiff is a former employee of Mondelez.

38. As a condition of employment with Mondelez, Defendant requires its employees to disclose PII including but not limited to, their names, Social Security number, address, date of birth, and gender. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

39. On information and belief, Mondelez provided BCLP with Plaintiff's PII as part of the legal services BCLP provided to Mondelez, including data and privacy advice. Thus, BCLP was

[16]Privacy Policy, Mondelez, https://www.uchealth.org/privacy-policy/#:~:text=UCHealth%20may%20use%20your%20precise,UCHealth%20website%20or%20mobile%20application. (last visited June 23, 2023).

granted access and custody of Plaintiff's PII including but not limited to his name, address, Social Security Number, date of birth, and gender.

40. On information and belief, Defendants collect and maintain employees' PII in their computer systems.

41. In collecting and maintaining the PII, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies and federal law.

42. According to the Breach Notice, BCLP first detected suspicious activity within its network on February 27, 2023. Following an internal investigation, BCLP discovered the Data Breach had occurred between February 23, 2023, and March 1, 2023. Ex. A. In other words, BCLP's investigation revealed that not only had its network been hacked by cybercriminals at least four days before it discovered the Breach, but the Data Breach actually continued for another two days after BCLP first became aware of it.

43. Despite touting itself to be a "leader" in data Privacy and Security firm, BCLP's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its clients' employees' highly sensitive PII. Mondelez knew or should have known that granting BCLP access to Plaintiff's PII would result in a Data Breach given BCLP's inadequate cybersecurity practices.

44. Additionally, Defendants admitted that PII was actually stolen during the Data Breach confessing that the information was not just accessed, but that the "unauthorized third party **acquired** certain data" that Defendants are still struggling to identify. Ex. A.

45. BCLP did not notify Mondelez about the breach until March 24, 2022, an entire month after the breach first began.

46. On or around June 15, 2023 –four months after the Breach first occurred and almost three months after Mondelez first learnt of the Breach – Mondelez finally began to notify Class Members about the Data Breach. However, Plaintiff did not receive a Notice Letter from Mondelez until June 21, 2023.

47. Despite their duties and alleged commitments to safeguard PII, Defendants do not in fact follow industry standard practices in securing employees' PII, as evidenced by the Data Breach.

48. In response to the Data Breach, Defendants contend that BCLP has or will be taking "taken steps to address the incident and prevent a similar occurrence in the future." Ex. A. Although Defendants fail to expand on what these alleged "steps" are, such steps should have been in place before the Data Breach.

49. Through the Breach Notice, Defendants also recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to "remain vigilant by reviewing account statements and monitoring free credit reports. You should regularly change your passwords. You may want to temporarily freeze your credit. You should be on guard for schemes where malicious actors may pretend to represent Mondelēz or reference this incident." Ex. A.

50. 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 PII. 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.

51. On information and belief, Mondelez has offered only two years 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 PII that cannot be changed, such as Social Security numbers. Further, the breach exposed employees' nonpublic, highly private information, a disturbing harm in and of itself.

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

53. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over their employees' PII. Defendants' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

54. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in similar industries preceding the date of the breach.

55. In light of recent high profile data breaches at other law firm advising and food industry companies[17], Defendants knew or should have known that their electronic records and employees' PII would be targeted by cybercriminals.

---

[17] *See* https://abovethelaw.com/2023/04/major-biglaw-firm-suffers-cyber-security-breach-of-mergers-acquisitions-data/ (last visited June 23, 2023); https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/ (last visited June 23, 2023); *see also* https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/ (last visited June 23, 2023).

56. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[18] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[19]

57. Indeed, cyberattacks against the both the legal and food industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [20]

58. Cyberattacks on the food industry and legal partner and advisers like Defendants 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 prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly." [21]

59. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including BCLP and Mondelez.

Plaintiff Wiacek's Experience

---

[18] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 23, 2023).

[19] *Id.*

[20] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 23, 2023).

[21] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

60. Plaintiff Wiacek is former Mondelez employee.

61. As a condition of employment with Mondelez, Plaintiff was required to provide his PII, including but not limited to his full name, Social Security number, date of birth, gender, and address.

62. Plaintiff provided his PII to Mondelez and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

63. On information and belief, Mondelez shared Plaintiff's PII with BCLP as part of its provision of management legal services and advice to Mondelez. Mondelez provided BCLP with Plaintiff's PII, including but not limited to his full name, Social Security number, date of birth, gender, and address.

64. Plaintiff provided his PII to Defendants and trusted that they would use reasonable measures to protect it according to their internal policies and state and federal law.

65. Defendants deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over four months.

66. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

67. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

68. 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.

69. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

70. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

71. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

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

72. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendants.

73. As a result of Defendants' 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. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

e. Lost opportunity costs and lost wages associated with 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 PII; and

h. The continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

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

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

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

77. One such example of criminals using PII for profit is the development of "Fullz" packages.

78. Cyber-criminals can cross-reference two sources of PII 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.

79. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed 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 PII 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 members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

80. Defendants disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII 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 PII.

81. Defendants' failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

82. 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 Defendants, should employ to protect against the unlawful exposure of PII.

83. 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 sensitive consumer information that they keep;

b. properly dispose of PII 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.

84. 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.

85. 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.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

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

CLASS ACTION ALLEGATIONS

88. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class") defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **All individuals residing in the United States whose PII was compromised in the Data Breach, including all those who received a notice of the Data Breach.**

Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

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

90. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 51,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, 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. His interests do not conflict with the Class's interests, and he 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 the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendants 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 Defendants were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's PII;

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

vi. Whether Defendants' 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.

91. 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.

COUNT I
Negligence
(Against Defendants On Behalf of Plaintiff and the Class)

92. Plaintiff realleges all previous paragraphs as if fully set forth below.

93. Plaintiff and members of the Class entrusted their PII to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII 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.

94. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

95. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants 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. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, 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.

96. Defendants 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 Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's PII.

97. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII — whether by malware or otherwise.

98. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

99. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their 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. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

100. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(Against Defendants On Behalf of Plaintiffs and the Class)

101. Plaintiff realleges all previous paragraphs as if fully set forth below.

102. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

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

104. Defendants breached their respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

105. Defendants' 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 Defendants are bound by industry standards to protect confidential PII.

106. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants 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.

107. 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 the Class.

108. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

109. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

110. Had Plaintiff and the Class known that Defendants did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendants with their PII.

111. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

112. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and 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; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

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

COUNT III
Breach of an Implied Contract
(Against Defendant Mondelez On Behalf of Plaintiff and the Class)

114. Plaintiff realleges all previous paragraphs as if fully set forth below.

115. Plaintiff and Class Members were required to provide their PII Defendant Mondelez as a condition of receiving employment from Defendant Mondelez. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's employment.

116. Plaintiff and the Class Members accepted Defendant Mondelez's offers by disclosing their PII to Defendant in exchange for employment.

117. Plaintiff and Class Members entered into implied contracts with Defendant Mondelez under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

118. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant Mondelez whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

119. In delivering their PII to Defendant Mondelez, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

120. Plaintiff and the Class Members would not have entrusted their PII to Defendant Mondelez in the absence of such an implied contract.

121. Defendant Mondelez accepted possession of Plaintiff's and Class Members' PII.

122. Had Defendant Mondelez disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure employees' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

123. Defendant Mondelez recognized that employees' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

124. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant Mondelez.

125. Defendant Mondelez breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

126. Defendant Mondelez breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

127. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' PII.

Count IV
Breach of Contract
(Against BCLP On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

129. Defendant BCLP entered into various contracts with its clients, including Defendant Mondelez, to provide legal services to its clients.

130. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant BCLP agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

131. Defendant BCLP knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

132. Defendant BCLP breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

133. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant BCLP's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

134. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Unjust Enrichment
(Against Defendants On Behalf of Plaintiff and the Class)

135. Plaintiff realleges all previous paragraphs as if fully set forth below.

136. This claim is pleaded in the alternative to the breach of implied contractual duty claims.

137. Plaintiff and members of the Class conferred a benefit upon Defendants in providing the PII to Defendants.

138. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate the services it sold to Plaintiff and the Class.

139. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's PII because Defendants failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendants had they known Defendants would not adequately protect their PII.

140. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Invasion of Privacy
(Against Defendants On Behalf of Plaintiff and the Class)

141. Plaintiff realleges all previous paragraphs as if fully set forth below.

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

143. Defendants owed a duty to Plaintiff and Class Member to keep their PII confidential.

144. Defendants affirmatively and recklessly disclosed Plaintiff's and Class Members' PII to unauthorized third-parties.

145. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

146. Defendants' reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' 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.

147. Defendants' failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

148. Defendants knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

149. Because Defendants failed to properly safeguard Plaintiff's and Class Members' PII, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

150. As a proximate result of Defendants' acts and omissions, Plaintiff's and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

151. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendants with their inadequate cybersecurity system and policies.

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

153. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

154. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VII
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"),
815 Ill. Comp. Stat. §§ 505/1, et seq.
(On behalf of Plaintiff and the Class)

155. Plaintiff realleges all previous paragraphs as if fully set forth below.

156. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

157. Defendants engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

158. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiff and

the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (iii) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

159. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

160. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

161. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

162. Defendants also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

163. As a result of Defendants' wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendants, or purchased Defendants' services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

164. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Class have suffered harm: (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, 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 identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their 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.

165. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the CFA.

PRAYER FOR RELIEF

Plaintiff and 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 representatives, and appointing their 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 Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

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: June 23, 2023

Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
Samuel J. Strauss
Brittany Resch
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com

ClassAction.org
