

# Exhibit B

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

ERIC D. FLORES, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

BRYAN CAVE LEIGHTON PAISNER LLP,  
MONDELEZ GLOBAL LLC, MONDELEZ  
INTERNATIONAL HOLDINGS LLC, and  
MONDELEZ INTERNATIONAL, INC.,

Defendants.

Case No.

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

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

**I. 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,”<sup>1</sup>

---

<sup>1</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html>.

lost control over its client Mondelez’s current and former employees’ highly sensitive personally identifiable information (“PII”) in a data breach perpetuated by cybercriminals (“Data Breach”). On information and belief, the Data Breach affected **over 51,000 individuals.**<sup>2</sup>

2. Mondelez chose to allow BCLP access and control over its current and former employees’ highly sensitive PII without first ensuring BCLP maintained adequate data security, infrastructure, procedures, and protocols in compliance with law and industry standards. To make matters worse, Mondelez failed to oversee and monitor BCLP and its data security after providing it with Plaintiff and the Class’s PII.

3. According to information and belief, the Data Breach began on or around February 23, 2023, when an unauthorized party gained access to BCLP’s inadequately protected network, and was not discovered by BCLP until **four (4) 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’s former and current employees’ highly private information for an entire week.

4. Following an internal investigation, BCLP learned cybercriminals had gained unauthorized access to Mondelez’s employees’ PII, including but not limited to,

---

<sup>2</sup> 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/>.

<sup>3</sup> About us, Mondelez, <https://www.mondelezinternational.com/>.

their names, Social Security numbers, addresses, dates of birth, genders, employee identification numbers, 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,"<sup>3</sup> was first notified by BCLP that its current and former employees' PII was compromised 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 Plaintiff and Class Members of the Data Breach ("Breach Notice").

8. Mondelez's Breach Notice obscured the nature of the breach and the threat it posed—failing to tell its former and current 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 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.

13. Mondelez failed to ensure the third party it hired, BCLP, maintained adequate data security before entrusting it with Plaintiff's and the Class's PII. Moreover, Mondelez failed to oversee and monitor BCLP to ensure Plaintiff's and the Class's PII was protected during the course of the relationship.

14. Moreover, BCLP failed to properly use up-to-date security practices to prevent the Data Breach.

15. Plaintiff Eric D. Flores is a Data Breach victim.<sup>3</sup>

16. 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.

## **II. PARTIES**

17. Plaintiff, Eric D. Flores, is a natural person and citizen of California, where he intends to remain. Plaintiff Flores is a Data Breach victim, receiving the Breach

---

<sup>3</sup> See *id.*

Notice dated June 15, 2023.<sup>4</sup>

18. 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.

19. 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.

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

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

### **III. JURISDICTION & VENUE**

22. 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.

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

---

<sup>4</sup> *Id.*

business in this District.

24. 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.

#### IV. BACKGROUND FACTS

##### *BCLP*

25. BCLP is a law firm that touts itself as “groundbreakers and innovators”<sup>5</sup> that has “extensive experience handling the full scope of complex privacy and security issues.”<sup>6</sup> BCLP boasts a total annual revenue of 900 million.<sup>7</sup>

26. BCLP’s services are specialized for companies “including 35% of the Fortune 500”<sup>8</sup> 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.

27. Indeed, BCLP advertises that it “routinely advise[s] 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

---

<sup>5</sup> About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html>.

<sup>6</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html>.

<sup>7</sup> BCLP Revenue, Zippia, <https://www.zippia.com/bryan-cave-careers-17522/revenue/>.

<sup>8</sup> About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html>.

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.”<sup>9</sup>

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

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

---

<sup>9</sup> Data Privacy and Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html#overview>.



29. In working with third party employees' highly sensitive data, BCLP assures that it "understand the importance of keeping your Personal Information secure,"<sup>10</sup> 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.

30. 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

---

<sup>10</sup> Privacy Notice, BCLP, <https://www.bclplaw.com/en-US/legal-notices/privacy-notice.html>.

breaches effectively.”<sup>11</sup>

31. BCLP promises that, in the event of a data breach, it will “inform you of this without undue delay.”<sup>12</sup>

If a data breach (leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Information) occurs which is likely to result in a high risk of adversely affecting your rights and freedoms, we will inform you of this without undue delay.

32. 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.”<sup>13</sup>

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

---

<sup>11</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html>.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

***Mondelez***

34. Mondelez is “one of the world’s largest snacks companies”<sup>14</sup> that “[has] operations in more than 80 countries and employ[s] approximately 91,000 diverse and talented employees [] around the world.”<sup>15</sup> Mondelez boasts a total revenue of 31 billion dollars.<sup>16</sup>

35. 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 designed to help protect against unauthorized use, disclosure, alteration, or destruction of the personal information we collect on our Sites.”<sup>17</sup>

36. 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.

37. 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

---

<sup>14</sup> About us, Mondelez, <https://www.mondelezinternational.com/About-Us>.

<sup>15</sup> *Id.*

<sup>16</sup> Investor Release Details, Mondelez, <https://ir.mondelezinternational.com/news-releases/news-release-details/mondelez-international-reports-q4-and-fy-2022-results>.

<sup>17</sup> Privacy Policy, Mondelez, <https://www.uchealth.org/privacy-policy/#:~:text=UCHealth%20may%20use%20your%20precise,UCHealth%20website%20or%20mobile%20application>.

reasonable steps to secure their PII.

38. Despite recognizing its duty to protect Plaintiff's and the Class's PII Mondelez handed over Plaintiff and the Class's PII to a third-party (BCLP) with inadequate data security, infrastructure, procedures, and protocols. Mondelez also failed to monitor and oversee BCLP. As a result, Defendants failed to protect the PII of Plaintiff and the Class.

### ***The Data Breach***

39. Plaintiff is a former employee of Mondelez.

40. As a condition of employment with Mondelez, Mondelez required Plaintiff and the Class to disclose their PII including but not limited to, their names, Social Security numbers, addresses, dates of birth, and gender. Defendant used that PII to facilitate its employment of Plaintiff and the Class, including payroll, and required Plaintiff and the Class to provide that PII to obtain employment and payment for that employment.

41. On information and belief, Mondelez provided BCLP with Plaintiff's and the Class's PII as part of the legal services BCLP provided to Mondelez, including data and privacy advice. Thus, BCLP was granted access and custody of Plaintiff's and the Class's PII. As such, Plaintiff's and the Class's PII was in BCLP's possession before, during, and after the Data Breach.

42. Defendants collect and maintain employees' PII in their computer systems. In collecting and maintaining Plaintiff's and the Class's PII, Defendants implicitly agreed that they would protect and safeguard that PII by complying with state and federal

laws and regulations and applicable industry standards.

43. 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. 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.

44. 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.

45. 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.<sup>18</sup>

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

47. On or around June 15, 2023 –four months after the Breach first occurred and

---

<sup>18</sup> *Id.* (emphasis added).

almost three months after Mondelez first learned of the Breach – Mondelez finally began to notify Class Members about the Data Breach.<sup>19</sup>

48. 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.

49. 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.”<sup>20</sup> Although Defendants fail to expand on what these alleged “steps” are, such steps should have been in place before the Data Breach.

50. 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.**”<sup>21</sup>

51. 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

---

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.* (emphasis added).

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.

52. According to information and belief, Mondelez has offered only two (2) 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 and dates of birth. Further, the Breach exposed employees’ nonpublic, highly private information, disturbing harm in and of itself.

53. 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.

54. 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.***

55. 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.

56. In light of recent high profile data breaches at other law firms and food

industry companies,<sup>22</sup> Defendants knew or should have known that their electronic records and employees' PII would be targeted by cybercriminals.

57. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>23</sup> 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.<sup>24</sup>

58. 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."<sup>25</sup>

---

<sup>22</sup> See <https://abovethelaw.com/2023/04/major-biglaw-firm-suffers-cyber-security-breach-of-mergers-acquisitions-data/>; <https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/>; 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).

<sup>23</sup> 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](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf).

<sup>24</sup> *Id.*

<sup>25</sup> Gordon M. Snow Statement, FBI <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.



59. 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.”<sup>26</sup>

60. 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 Flores’s Experience***

61. Plaintiff Flores is former Mondelez employee.

62. As a condition of receiving 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.

63. 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. Plaintiff also reasonably and justifiably believed that Mondelez would not give his PII to third parties with inadequate data security, such as BCLP.

---

<sup>26</sup> Secret Service Warn of Targeted, Law360, <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

64. On information and belief, Mondelez shared Plaintiff's PII with BCLP as part of its provision of 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.

65. 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.

66. 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**.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

72. 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***

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

74. 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.

75. 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.

76. 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.

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

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

79. 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.

80. 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.

81. 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.

82. 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.*

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

#### V. CLASS ACTION ALLEGATIONS

89. 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 discovered on or around February 27, 2023 and received a Notice of Data Breach letter from Mondelez.**

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.

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

91. 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.

92. 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.

**VI. CAUSES OF ACTION**

**COUNT I**

**Negligence**

**(Against Defendants On Behalf of Plaintiff and the Class)**

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

94. 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.

95. Mondelez had a duty to protect Plaintiff's and the Class's PII was protected. This duty to protect Plaintiff's and the Class's PII did not end when it gave Plaintiff and the Class's PII to BCLP. Mondelez had a duty to ensure that any third party it gave Plaintiff's and the Class's PII to maintained adequate data security, procedures, practices, protocols, and infrastructure. Mondelez also had the continuing duty to ensure that any third-party it hired maintained the data security, procedures, practices, protocols, and infrastructure needed to protect Plaintiff's and the Class's PII throughout the course of the relationship.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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.

101. Defendants breached their duties by failing to exercise reasonable care in protecting the PII of Plaintiff and the Class, supervising and monitoring 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.

102. 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)**

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

104. 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.

105. 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.

106. 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.

107. 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.

108. 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.

109. 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.

110. 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.

111. 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.

112. 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.

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

114. 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.

115. 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)**

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

117. 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.

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

119. 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.

120. 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.

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

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

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

124. 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.

125. 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.



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

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

128. 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.

129. 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 V**  
**Unjust Enrichment**  
**(Against Defendants On Behalf of Plaintiff and the Class)**

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

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

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

133. 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.

134. 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.

135. 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)**

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

137. 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.

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

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

140. 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.

141. 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.

142. 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.

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

144. 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.

145. 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.

146. 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.

147. 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.

148. 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.

149. 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)**

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

151. 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).

152. 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).

153. 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.

154. 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.

155. 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.

156. 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.

157. 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.*

158. 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.

159. 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.

160. 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.

**COUNT VIII**  
**NEGLIGENT HIRING, TRAINING, AND SUPERVISION**  
**(On behalf of Plaintiff and the Class)**

161. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

162. At all relevant times, BCLP was Mondelez's agent. Mondelez granted BCLP access to the PII of Plaintiff and the Class without properly vetting BCLP, inquiring about/ investigating BCLP's data security, training BCLP, advising BCLP of its duties owed to Plaintiff and the Class under the InfoSecPPG, and/or advising BCLP of the confidential nature of Plaintiff' and the Class's PII.

163. Mondelez was negligent and failed to exercise the requisite standard of care in the hiring, supervision, and retention of BCLP – who disclosed Plaintiff' and the Class's PII without authorization and caused the damages delineated herein by virtue of the Data Breach.

164. At all times relevant hereto, Defendant Mondelez owed a duty to Plaintiff and the Class to train and supervise its agents and third parties handling sensitive PII in its possession to ensure they recognized the duties owed to Plaintiff' and the Class to keep their PII safe from data breaches.

165. Mondelez owed a duty to Plaintiff and the Class to ensure BCLP had adequate data security, procedures, and protocols sufficient to protect Plaintiff' and the Class's PII from data breaches prior to hiring BCLP.



166. Mondelez also owed a continuing duty to Plaintiff and the Class to ensure BCLP continued to employ adequate data security, procedures, and protocols sufficient to protect Plaintiff' and the Class's PII from data breaches after hiring BCLP.

167. Mondelez breached this duty by failing to ensure BCLP possessed the requisite data security, procedures, practices, infrastructure, and protocols to protect Plaintiff' and the Class's PII from data breaches prior to hiring BCLP and while BCLP worked for Mondelez.

168. Mondelez was on notice of the importance of data security because of well publicized data breaches occurring throughout the United States. Despite knowledge of prior data breaches, Mondelez failed to ensure BCLP possessed the adequate security posture to protect Plaintiff' and the Class's PII from unauthorized disclosure.

169. Mondelez knew or should have known that the failure to ensure BCLP employed adequate data security, procedures, and protocols would create an unreasonable risk of danger to persons and property.

170. As a direct and proximate result of Mondelez's breach of its duties, and its negligent hiring, training, selection, and supervision, of BCLP, which resulted in the disclosure of Plaintiff' and Class members' confidential PII in the Data Breach, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, diminution in value of their PII, and actual misuse of their PII.

171. Mondelez was advised of the Data Breach, but continued to employ BCLP, putting Plaintiff and the Class at risk of more data breaches in the future.

172. The acts and omissions of Mondelez in negligently hiring, retaining, training, and/or supervising BCLP are such as to show gross negligence and reckless disregard for the safety of others and, therefore, punitive damages are appropriate.

**VII. 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.

**VIII. JURY DEMAND**

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

Dated: June 30, 2023

Respectfully submitted,

By: s/ Thomas A. Zimmerman, Jr.

Thomas A. Zimmerman, Jr. (IL #6231944)

*tom@attorneyzim.com*

Sharon A. Harris

*sharon@attorneyzim.com*

Matthew C. De Re

*matt@attorneyzim.com*

Jeffrey D. Blake

*jeff@attorneyzim.com*

**ZIMMERMAN LAW OFFICES, P.C.**

77 W. Washington Street, Suite 1220

Chicago, Illinois 60602

(312) 440-0020 telephone

(312) 440-4180 facsimile

[www.attorneyzim.com](http://www.attorneyzim.com)

William B. Federman\*

**FEDERMAN & SHERWOOD**

10205 N. Pennsylvania Ave.

Oklahoma City, Oklahoma 73120

(405) 235-1560

(405) 239-2112 (facsimile)

[wbf@federmanlaw.com](mailto:wbf@federmanlaw.com)

\**pro hac vice* application forthcoming

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

ROCK MEYER, individually and on  
behalf of all others similarly situated,

Plaintiff,

vs.

BRYAN CAVE LEIGHTON PAISNER,  
LLP,

Defendant.

CASE NO. 1:23-CV-04954

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Rock Meyer (“Mr. Meyer” or “Plaintiff”) brings this action on behalf of himself, and all others similarly situated against Defendant, Bryan Cave Leighton Paisner LLP (“BCLP” or “Defendant”), and alleges as follows:

**I. 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,”<sup>1</sup> lost control over the highly sensitive personally identifiable information (“PII”) of Plaintiff and other similarly situated individuals (the “Class” or “Class Members”) in a massive and preventable data breach perpetrated by cybercriminals (the “Data Breach” or “Breach”). According to information and belief, the Data Breach affected **at least**

---

<sup>1</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html>.

**51,110 individuals.**<sup>2</sup>

2. According to information and belief, the Data Breach began on or around February 23, 2023, when an unauthorized party gained access to BCLP's inadequately protected network and was not discovered by BCLP until **four (4) days later**, on February 27, 2022.<sup>3</sup> Shockingly, despite discovering the Data Breach on February 27, 2023, BCLP allowed the Data Breach to continue for **at least two more days**, providing cybercriminals unfettered access to Plaintiff and the Class's highly private information **for an entire week.**<sup>4</sup>

3. Following an internal investigation, BCLP learned cybercriminals had gained unauthorized access to Plaintiff's and the Class's PII, including but not limited to, their names, Social Security numbers, addresses, dates of birth, genders, employee identification numbers, and retirement and/or thrift plan information.<sup>5</sup>

4. On information and belief, cybercriminals bypassed BCLP's inadequate security systems to access Plaintiff and the Class's PII in its computer systems.

5. On or about June 15, 2023 – **almost four months after the unauthorized party first gained access to Plaintiff and the Class's PII** – victims of the Data Breach were finally notified via letter that their highly sensitive and

---

<sup>2</sup> See <https://apps.web.maine.gov/online/aeviewer/ME/40/ca25f29f-db60-4baf-ba53-8bae79da4d97.shtml>.

<sup>3</sup> See Exhibit 1.

<sup>4</sup> See *id.*

<sup>5</sup> See *id.*

confidential PII was exposed (“Notice of Data Breach Letter”).<sup>6</sup>

6. The Notice of Data Breach Letter obscured the nature of the breach and the threat it posed—failing to notify Plaintiff and the Class how many people were impacted, how the Breach happened, or why it took so long to begin notifying victims that hackers had gained access to highly sensitive PII.

7. Defendant’s 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.

8. 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 PII misuse.

9. In failing to adequately protect Plaintiff’s and the Class’s PII, failing to adequately notify them of the Breach, and by obfuscating the nature of the breach, Defendant violated state and federal laws and harmed Plaintiff and the Class.

10. Plaintiff and members of the proposed Class are victims of Defendant’s negligence and inadequate cyber security measures.

11. Moreover, BCLP failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff Rock Meyer is a Data Breach victim.<sup>7</sup>

---

<sup>6</sup> *See id.*

<sup>7</sup> *See id.*

13. 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 Defendant's possession.

## **II. PARTIES**

14. Plaintiff, Rock Meyer, is a natural person and citizen of Kentucky, where he intends to remain. Plaintiff Meyer is a Data Breach victim and received a Notice of Data Breach Letter.<sup>8</sup>

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

## **III. JURISDICTION & VENUE**

16. 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 Defendant are citizens of different states.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

---

<sup>8</sup> *Id.*

18. 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.

#### IV. FACTUAL ALLEGATIONS

##### *BCLP*

19. BCLP is a law firm that touts itself as “groundbreakers and innovators”<sup>9</sup> that have “extensive experience handling the full scope of complex privacy and security issues.”<sup>10</sup> BCLP boasts a total annual revenue of \$900 million.<sup>11</sup>

20. BCLP’s services are specialized for companies “including 35% of the Fortune 500”<sup>12</sup> who manage highly sensitive data. BCLP thus must oversee, manage, and protect the PII of its clients’<sup>13</sup> consumers, including that of Plaintiff and the Class.

21. Indeed, BCLP advertises that it “routinely advise[s] 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

---

<sup>9</sup> About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html>.

<sup>10</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html> .

<sup>11</sup> BCLP Revenue, Zippia, <https://www.zippia.com/bryan-cave-careers-17522/revenue/>.

<sup>12</sup> About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html>.

<sup>13</sup> “Mondelez Global LLC retained the legal services of the law firm Bryan Cave Leighton Paisner LLP (“Bryan Cave”) to provide advice on customary legal matter of a company of its size. To provide these services, Bryan Cave obtained some PII of current and former Mondelez employees.” Exhibit 1.



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.”<sup>14</sup>

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

23. In working with third-party employees’ highly sensitive data, BCLP assures that it “understand the importance of keeping your PII secure,”<sup>15</sup> 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.

---

<sup>14</sup> Data Privacy and Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html#overview>.

<sup>15</sup> Privacy Notice, BCLP, <https://www.bclplaw.com/en-US/legal-notices/privacy-notice.html>.

24. 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.”<sup>16</sup>

25. BCLP promises that, in the event of a data breach, it will “inform you of this without undue delay.”<sup>17</sup>

If a data breach (leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Information) occurs which is likely to result in a high risk of adversely affecting your rights and freedoms, we will inform you of this without undue delay.

26. 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 Plaintiff’s and the Class’s data and prioritize 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.”<sup>18</sup>

---

<sup>16</sup> Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html>.

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

27. But, according to information and belief, BCLP failed to strictly adhere to these policies in maintaining Plaintiff's and the Class's PII.

***The Data Breach***

28. Defendant collected and maintained Plaintiff and the Class's PII in its computer systems. In collecting and maintaining Plaintiff's and the Class's PII, Defendant implicitly agreed that it would protect and safeguard that PII by complying with state and federal laws and regulations and applicable industry standards. Defendant was in possession of Plaintiff and the Class's PII before, during, and after the Data Breach.

29. According to the Notice of Data Breach Letter, BCLP first detected suspicious activity within its network on February 27, 2023.<sup>19</sup> Following an internal investigation, BCLP discovered the Data Breach occurred between February 23, 2023, and March 1, 2023.<sup>20</sup> 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.

30. 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 individuals

---

<sup>19</sup> See Exhibit 1.

<sup>20</sup> See *id.*

highly sensitive PII, including Plaintiff and the Class.

31. Additionally, Defendant 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 Defendant is still struggling to identify.<sup>21</sup>

32. On or around June 15, 2023 – **four months after the Breach first occurred** – Plaintiff and Class Members were finally notified of the Data Breach.<sup>22</sup>

33. Despite BCLP’s duties and alleged commitments to safeguard PII, BCLP did not follow industry standard practices in securing Plaintiff and the Class’s PII, as evidenced by the Data Breach.

34. In response to the Data Breach, BCLP contends it has or will be taking “taken steps to address the incident and prevent a similar occurrence in the future.”<sup>23</sup> Although BCLP failed to expand on what these alleged “steps” are, such steps should have been in place before the Data Breach.

35. Through the Notice of Data Breach Letter, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach and encouraged Data Breach victims to “remain vigilant by reviewing account statements and monitoring free credit reports. You should regularly change your passwords. You may

---

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

want to temporarily freeze your credit.”<sup>24</sup>

36. Even though Social Security numbers were exposed here, 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.

37. Plaintiff and the Class were only offered two (2) 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 and dates of birth. Further, the Breach exposed nonpublic, highly private information, disturbing harm in and of itself.

38. 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.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over Plaintiff and the Class’s PII. Defendant’s negligence is evidenced by its failure to

---

<sup>24</sup> *Id.*

prevent the Data Breach and stop cybercriminals from accessing the PII.

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

40. Defendant's 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.

41. In light of recent high profile data breaches at other law firms,<sup>25</sup> Defendant knew or should have known that their electronic records and Plaintiff and the Class's PII would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>26</sup> 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.<sup>27</sup>

43. Indeed, cyberattacks against the both the legal industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that

---

<sup>25</sup> See <https://abovethelaw.com/2023/04/major-biglaw-firm-suffers-cyber-security-breach-of-mergers-acquisitions-data/>; <https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/>; see also <https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/>.

<sup>26</sup> 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](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf).

<sup>27</sup> *Id.*

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.”<sup>28</sup>

44. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including BCLP.

***Plaintiff Meyer’s Experience***

45. Plaintiff received a Notice of Data Breach Letter, dated June 15, 2023, notifying him that an unauthorized third-party “acquired certain data” which included his PII. BCLP was in possession of Plaintiff’s PII before, during, and after the Data Breach.

46. Defendant 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**.

47. As a result of the Data Breach, Plaintiff spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts and credit reports to monitor suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff has spent and will continue to spend considerable time and

---

<sup>28</sup> Gordon M. Snow Statement, FBI <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.

effort monitoring his accounts to protect himself from additional identity theft for the rest of his life.

48. Plaintiff fears for his personal financial security and uncertainty over what PII 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.

49. As a result of the Data Breach, Plaintiff has suffered **actual misuse** of his PII. Plaintiff received a fraud alert from PNC Bank after the Data Breach, notifying him of a fraudulent transaction. Due to the proximity of the fraud to the Data Breach, Plaintiff reasonably believes it was caused by the Data Breach.

50. 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 Defendant, which was compromised in and as a result of the Data Breach.

51. 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.

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

53. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and



certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant; (f) actual misuse of his PII.

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

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

55. As a result of Defendant'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. 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 Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

56. 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.

57. 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.

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

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

60. 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.

61. 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.

62. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant 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.

63. Defendant’s 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.

***Defendant failed to adhere to FTC guidelines.***

64. 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 PII.

65. In 2016, the FTC updated its publication, Protecting PII: 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.

66. 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.

67. 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.

68. 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.

69. Defendant’s 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.

#### V. CLASS ACTION ALLEGATIONS

70. 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 discovered by BCLP on or around February 27, 2023, and received a Notice of Data Breach Letter.**

Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant’s officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

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

72. 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 Defendant's 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 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. 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 Defendant had a duty to use reasonable care in

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

73. 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.

**VI. CAUSES OF ACTION**

**COUNT I**  
**Negligence**

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

75. Plaintiff and members of the Class's PII was entrusted to Defendant. Defendant 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.

76. 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 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. Defendant 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.

77. Defendant 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. 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. 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.

78. 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 the Class's PII.

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

80. PII is highly valuable, and Defendant 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. Especially with multiple other law firms experiencing data breaches.

81. Defendant breached its duties by failing to exercise reasonable care in protecting the PII of Plaintiff and the Class, supervising and monitoring its 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. 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. As a direct and traceable result of Defendant's 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.

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

**COUNT II**  
**Negligence Per Se**

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

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

85. 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’ PII. 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 members of the Class’s PII.

86. Defendant breached its 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.

87. 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 PII.

88. Defendant violated its 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. Defendant’s conduct was particularly unreasonable given the nature and amount of PII 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.

89. 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.

90. But for Defendant's 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.

91. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it 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 PII.

92. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have allowed Defendant to access their PII.

93. Defendant's various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

94. As a direct and proximate result of Defendant's 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.

95. Additionally, as a direct and proximate result of Defendant's negligence

*per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

**COUNT III**  
**Unjust Enrichment**

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

97. This claim is pleaded in the alternative to the breach of contract claim(s).

98. Plaintiff and members of the Class conferred a benefit upon Defendant in providing their PII to Defendant.

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

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

101. Defendant 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 IV**  
**Invasion of Privacy**

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

103. 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.

104. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

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

106. 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.

107. Defendant's 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.

108. Defendant's 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.

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

110. Because Defendant failed to properly safeguard Plaintiff's and Class

Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

111. As a proximate result of Defendant's 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.

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

113. Plaintiff and Class Members 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 Plaintiff's and the Class's PII.

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

115. Plaintiff, on behalf of himself and Class Members, 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.

**COUNT V**  
**Violations of the Illinois Consumer Fraud and**  
**Deceptive Business Practices Act (“CFA”), 815 Ill. Comp. Stat. §§ 505/1, et seq.**

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

117. Plaintiff and the Class are “consumers” as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are “persons” as defined in 815 Ill. Comp. Stat. § 505/1(c).

118. Defendant engaged in “trade” or “commerce,” including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

119. Defendant 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 material 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 material facts to Plaintiff and the Class about Defendant’s 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 PII from further unauthorized disclosure, release, data breaches, and theft.

120. These actions also constitute deceptive and unfair acts or practices because Defendant 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.

121. 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 Defendant's offering of goods and services.

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

123. Defendant 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 PII Protection Act, 815 ILCS 530/1, *et seq.*

124. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's 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.

125. As a direct and proximate result of Defendant's 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant 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.

126. 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 Defendant's violations of the CFA.

## **VII. 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 Defendant 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.

#### **VIII. JURY DEMAND**

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

Dated: July 28, 2023

Respectfully submitted,

/s/: Thomas A. Zimmerman

Thomas A. Zimmerman, Jr.

(IL #6231944)

tom@attorneyzim.com

Sharon A. Harris

sharon@attorneyzim.com

Matthew C. De Re

matt@attorneyzim.com

Jeffrey D. Blake

jeff@attorneyzim.com

**ZIMMERMAN LAW  
OFFICES, P.C.**

77 W. Washington Street

Suite 1220

Chicago, Illinois 60602

(312) 440-0020 telephone

(312) 440-4180 facsimile

www.attorneyzim.com

M. Anderson Berry

*(pro hac vice application forthcoming)*

**CLAYEO C. ARNOLD,  
A PROFESSIONAL CORP.**

865 Howe Avenue

Sacramento, CA 95825

Telephone: (916) 239-4778

Facsimile: (916) 924-1829

aberry@justice4you.com

# Exhibit 2

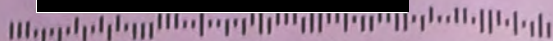
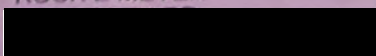


Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

June 15, 2023



J5767-L01-0019224 T0004B P003 \*\*\*\*\*ALL FOR AADC 450  
ROCK E MEYER



Re: NOTICE OF DATA BREACH

Dear Rock E Meyer:

Mondelēz Global LLC (“Mondelēz,” “we,” “us,” “our”) is writing to inform you of an incident that involved some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you can take to protect your personal information. Mondelēz takes this incident and the security of your personal information very seriously, and we sincerely regret any concern or issue this incident may cause.

**WHAT HAPPENED?** Mondelēz retained the legal services of the law firm Bryan Cave Leighton Paisner LLP (“Bryan Cave”) to provide advice on customary legal matters of a company its size. To provide these services, Bryan Cave obtained some personal information of current and former Mondelēz employees.

Bryan Cave has stated that on February 27, 2023, it detected unauthorized access to its systems, including an area it used to store certain customer files. This access occurred from February 23, 2023 until March 1, 2023. Bryan Cave initiated a robust investigation with the assistance of an outside cybersecurity forensics firm and notified law enforcement. Bryan Cave informed us of unauthorized access on March 24, 2023, while continuing to investigate the incident, and later confirmed that an unauthorized third party acquired certain data, which was still being determined. On May 22, 2023, based upon additional information received from Bryan Cave, Mondelēz determined that it finally had enough information to determine who was impacted and that affected individuals should be notified. Mondelēz proceeded to conduct a thorough review of impacted information to identify affected current and former employees, which was just completed, and is now providing notification. Please know that this incident did not occur on or affect Mondelēz systems or networks in any way.

**WHAT INFORMATION WAS INVOLVED?** The investigation determined that the personal information which was included in the impacted data may include your: social security number, first and last name, address, date of birth, marital status, gender, employee identification number, and Mondelēz retirement and/or thrift plan information. Financial information, such as account information or credit card numbers, were not involved in this incident.

**WHAT WE ARE DOING.** Please know that protecting your personal information is something that Mondelēz takes very seriously. Bryan Cave conducted an investigation with an outside cybersecurity forensic firm to confirm the nature and scope of the incident. Bryan Cave also notified law enforcement. Bryan Cave informed us that they have taken steps to address the incident and prevent a similar occurrence in the future. Mondelēz is providing notice and offering credit monitoring services to individuals based on the personal information that was potentially impacted.

**WHAT YOU CAN DO:** We encourage you to remain vigilant by reviewing account statements and monitoring your 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 mailpiece. If you have questions, please contact us at the number described below.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> Credit Plus 1B for 24 months. This helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

To enroll in this credit monitoring service, please contact Experian by calling the phone number listed below. If you have internet access, you may also enroll by visiting the website listed below. You will need the Activation Code provided below to complete your enrollment.

**Enrollment URL:** <https://www.experianidworks.com/plus>  
**Your Activation Code:** [REDACTED]  
**Enrollment Deadline:** September 30, 2023 (Please be sure to enroll by this date, your code will not work after the deadline.)

If you have questions about the product or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-901-4621 by September 30, 2023. Be prepared to provide engagement number B096059 for Experian.

**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

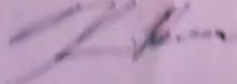
- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only. \*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Internet Surveillance: Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE<sup>TM</sup>: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$1 Million Identity Theft Insurance<sup>\*\*</sup>: Provides coverage for certain credit and unauthorized electronic fund transfers.

\* Offline members will be eligible to call for additional reports quarterly after enrolling

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an American company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**FOR MORE INFORMATION,** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-901-4621 toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide engagement number B096059.

Sincerely,



Kevin Brennan  
Chief Counsel Litigation (US)

B096059

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

**IN RE: BRYAN CAVE LEIGHTON  
PAISNER, LLP DATA BREACH  
LITIGATION**

Master File No. 1:23-CV-04249

**JURY TRIAL DEMANDED**

This Document Relates to: All Actions

**CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Eric D. Flores and Rock Meyer (collectively, “Plaintiffs”) bring this class action lawsuit on behalf of themselves, and on behalf of all others similarly situated (the “Class” or “Class Members”) against Defendant, Bryan Cave Leighton Paisner LLP (“BCLP” or “Defendant”), and allege as follows:

**I. INTRODUCTION**

1. This lawsuit stems from a massive and preventable data breach spanning from February 23, 2023, through March 1, 2023, during which cybercriminals infiltrated BCLP’s inadequately protected data systems and **acquired** the highly sensitive personally identifiable information (“PII”) of approximately **51,110 individuals** (the “Data Breach” or “Breach”). As a result of BCLP’s negligence and failure to provide adequate data security, Plaintiffs’ and the Class’s PII is in the hands of cybercriminals who will misuse their PII for nefarious purposes for years to come.

2. According to BCLP, on February 27, 2023, BCLP “detected unauthorized



access to its systems, including an area it used to store certain customer files.”<sup>1</sup>

3. Despite discovering the unauthorized access to its systems on February 27, 2023, BCLP allowed the Data Breach to continue for days—until March 1, 2023.<sup>2</sup>

4. Although BCLP discovered the Data Breach on February 27, 2023, the Data Breach actually began February 23, 2023.<sup>3</sup> Thus, the Data Breach spanned at least six (6) days.

5. In other words, cybercriminals had unfettered access to Plaintiffs’ and the Class’s highly sensitive PII for nearly an entire week.

6. There is no question that sensitive PII was stolen in the Data Breach. Indeed, BCLP admits point-blank that Plaintiffs’ and the Class’s Private Information is in the hands of cybercriminals. Following an investigation, BCLP confirmed an unauthorized third-party “**acquired certain data**,” including but not limited to PII such as: names, marital statuses, Social Security numbers, addresses, dates of birth, genders, employee identification numbers, and retirement and/or thrift plan information (the “Private Information” or “Personal Information”).<sup>4</sup>

7. On or about June 15, 2023—almost four (4) months after the unauthorized

---

<sup>1</sup> See Exhibits 1–2 (Notice of Data Breach Letters).

<sup>2</sup> See *id.*

<sup>3</sup> See *id.*

<sup>4</sup> See *id.*

party first gained access to Plaintiffs’ and the Class’s PII—victims of the Data Breach were finally notified via letter that their highly sensitive and confidential PII was exposed (“Notice of Data Breach Letter” or “Notice Letter”).<sup>5</sup>

8. The Notice Letter obscured the nature of the breach and the threat it posed—failing to notify Plaintiffs and the Class how many people were impacted, how the Breach happened, why it took BCLP so long to discover the Breach, and why there was such a delay in notifying victims of the Breach.

9. Defendant’s failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warning to monitor their credit reports to prevent unauthorized use of their PII.

10. 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 PII misuse.

11. In failing to adequately protect Plaintiffs’ and the Class’s PII, failing to adequately notify Plaintiffs and the Class of the Breach, failing to use up-to-date data security practices/infrastructure to prevent the Data Breach, and by obscuring the nature of the Breach, Defendant violated state and federal laws and harmed Plaintiffs and the Class.

12. Plaintiffs and members of the Class are victims of Defendant’s negligence

---

<sup>5</sup> See *id.*

and inadequate cyber security measures and are victims of Defendant's Data Breach.

13. Accordingly, Plaintiffs, on behalf of themselves and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees.

## **II. THE PARTIES**

14. Plaintiff **Rock Meyer** ("Plaintiff Meyer") is a natural person and citizen of the State of Kentucky, where he intends to remain. Plaintiff Meyer is a Data Breach victim and received a Notice of Data Breach Letter.<sup>6</sup>

15. Plaintiff **Eric D. Flores** ("Plaintiff Flores") is a natural person and citizen of the State of California, where he intends to remain. Plaintiff Flores is a Data Breach victim and received a Notice of Data Breach Letter.<sup>7</sup>

16. Defendant, **BCLP**, is registered in the State of Illinois as a foreign LLP. BCLP has multiple partners in the State of Illinois and within this District.<sup>8</sup>

## **III. JURISDICTION & VENUE**

17. 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

---

<sup>6</sup> See Exhibit 1.

<sup>7</sup> See Exhibit 2.

<sup>8</sup> See generally, People (Chicago), BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/people/index.html?of=2169> (last visited Oct. 19, 2023).

members in the proposed class,<sup>9</sup> and Plaintiffs and Defendant are citizens of different states.

18. This Court has personal jurisdiction over the Defendant because Defendant does substantial business in this District, has partners located in the District, has an office located in this District, and is registered to do business in the State of Illinois.

19. 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.

#### **IV. FACTUAL ALLEGATIONS**

##### ***Bryan Cave Leighton Paisner LLP's Business and the Collection of Plaintiffs' and the Class's Private Information***

20. BCLP is a law firm that touts itself as “groundbreakers and innovators”<sup>10</sup> who have “extensive experience handling the full scope of complex privacy and security issues.”<sup>11</sup>

---

<sup>9</sup> See Data Breach Notification, OFFICE OF THE MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aeviewer/ME/40/ca25f29f-db60-4baf-ba53-8bae79da4d97.shtml> (last visited Oct. 19, 2023) (reporting 51,110 individuals were affected by the Data Breach).

<sup>10</sup> About us, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/about/about-bclp.html> (last visited Oct. 19, 2023).

<sup>11</sup> Data Privacy & Security, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html> (last visited Oct. 19, 2023).

21. BCLP boasts a total annual revenue of \$900 million in 2022.<sup>12</sup> As such, BCLP had more than sufficient funds to implement adequate data security, infrastructure, training, procedures, and protocols.

22. BCLP's services are specialized for companies "including 35% of the Fortune 500"<sup>13</sup> who manage highly sensitive data. As such, BCLP is routinely entrusted with PII from its clients, which BCLP must oversee, manage, and protect.

23. Indeed, BCLP advertises that it "routinely advise[s] 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 [it] excel[s] at helping companies achieve their business goals while balancing and addressing privacy and security obligations."<sup>14</sup>

24. Plaintiffs', and the Class's PII was acquired by BCLP through BCLP's relationship with one of BCLP's clients, Mondelez International ("Mondelez").<sup>15</sup>

---

<sup>12</sup> BCLP Revenue, ZIPPIA, <https://www.zippia.com/bryan-cave-careers-17522/revenue/> (last visited Oct. 19, 2023).

<sup>13</sup> About us, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/about/about-bclp.html> (last visited Oct. 19, 2023).

<sup>14</sup> Data Privacy & Security, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html> (last visited Oct. 19, 2023).

<sup>15</sup> See Exhibits 1–2.

Mondelez retained the legal services of BCLP.<sup>16</sup>As one of Mondelez's legal services providers, Bryan Cave had copies of and access to sensitive Private Information belonging to current and former Mondelez employees, including that of Plaintiffs and the Class.<sup>17 18</sup>

25. Defendant collected and maintained Plaintiffs' and the Class's PII in its computer systems. In collecting and maintaining Plaintiffs' and the Class's PII, Defendant implicitly agreed that it would protect and safeguard that PII by complying with state and federal laws and regulations and applicable industry standards.

26. Indeed, Defendant states on its website, "[w]e understand the importance of keeping your Personal Information secure."<sup>19</sup>

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

---

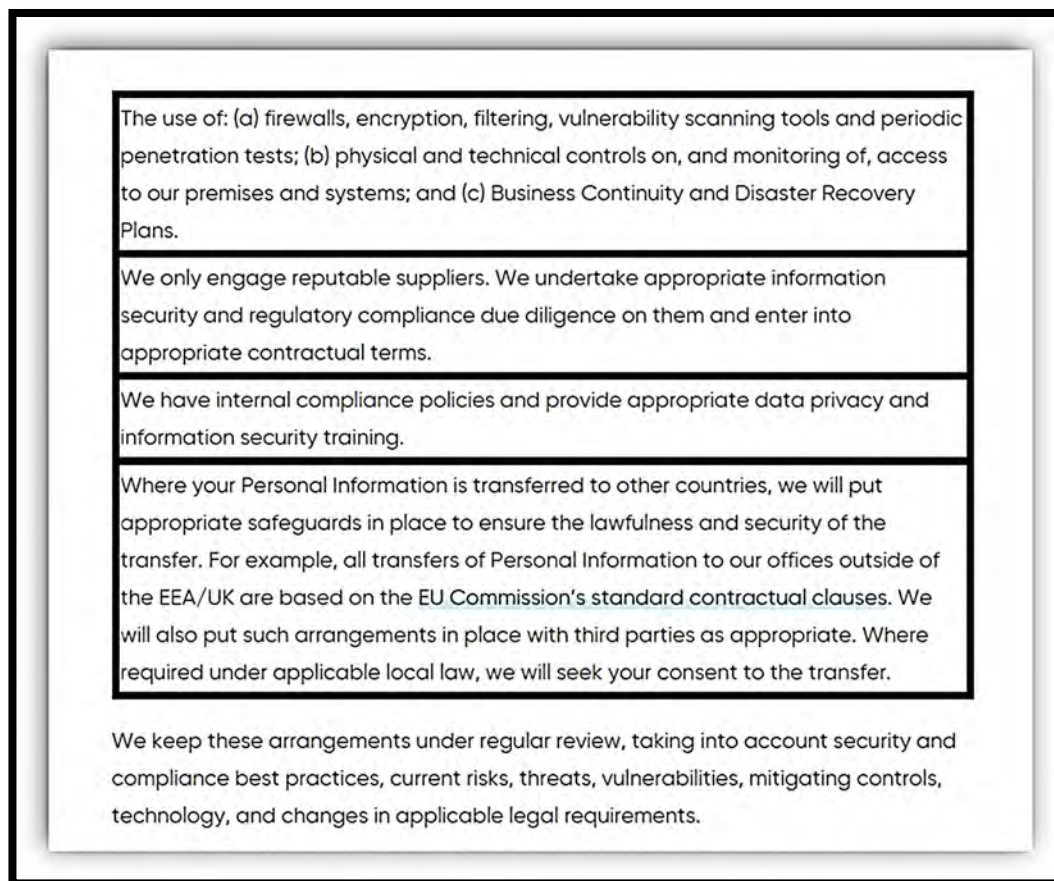
<sup>16</sup> "Mondelez Global LLC retained the legal services of the law firm Bryan Cave Leighton Paisner LLP ("Bryan Cave") to provide advice on customary legal matter of a company of its size. To provide these services, Bryan Cave obtained some PII of current and former Mondelez employees." Exhibits 1–2.

<sup>17</sup> *See id.*

<sup>18</sup> According to the Notice Letter, the Data Breach did not affect Mondelez's systems or networks. *See id.*

<sup>19</sup> Privacy Notice, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en-US/legal-notices/privacy-notice.html> (last visited Oct. 19, 2023).

27. In working with highly sensitive PII, BCLP assures that it “understand[s] the importance of keeping your PII secure,”<sup>20</sup> gloating that it employs a plethora of ways to ensure the security of PII:



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.”<sup>21</sup>

---

<sup>20</sup> *Id.*

<sup>21</sup> Data Privacy & Security, BRYAN CAVE LEIGHTON PAISNER LLP,

29. BCLP promises that, in the event of a data breach, it will “inform you of this without undue delay.”<sup>22</sup>

If a data breach (leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Information) occurs which is likely to result in a high risk of adversely affecting your rights and freedoms, we will inform you of this without undue delay.

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 Plaintiffs’ and the Class’s PII and the need to prioritize data security.

31. 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.”<sup>23</sup>

32. Despite the promises explicitly and implicitly made by BCLP, BCLP failed to employ industry standard data security that would have prevented the Data Breach and the subsequent theft of Plaintiffs’ and the Class’s PII.

***BCLP’s Massive and Preventable Data Breach***

33. Between February 23, 2023, and March 1, 2023, BCLP, a law firm who claims to have “extensive experience handling the full scope of complex privacy and

---

<https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html> (last visited Oct. 19, 2023).

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*



security issues,” and who also claims to “understand the importance of keeping [] personal information secure” failed to adequately secure and protect the Private Information of Plaintiffs and the Class, resulting in a massive and preventable data breach, reported to have affected at least 51,110 individuals.

34. According to BCLP, on February 27, 2023, BCLP first detected unauthorized access to its systems, including an area that stored the Private Information of Plaintiffs and the Class.<sup>24</sup>

35. Although the Breach was discovered by BCLP on February 27, 2023, the Data Breach actually began days earlier on February 23, 2023.<sup>25</sup>

36. BCLP failed to timely detect the Data Breach, giving cybercriminals several days of unfettered access to Plaintiffs’ and the Class’s PII.

37. To make matters worse, following an investigation, BCLP discovered the Data Breach spanned from February 23, 2023, through March 1, 2023—nearly an entire week.<sup>26</sup>

38. In other words, BCLP’s investigation revealed that not only had its network been hacked by cybercriminals at least four (4) days before it discovered the Breach, but the Data Breach actually continued for at least another two (2) days after BCLP first became

---

<sup>24</sup> See Exhibits 1–2.

<sup>25</sup> See *id.*

<sup>26</sup> See *id.*

aware of the intrusion.

39. Despite BCLP self-proclaiming itself as a “leader” in data privacy and security, BCLP’s cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of highly sensitive PII, including the PII of Plaintiffs and the Class.

40. BCLP’s investigation revealed that during the Data Breach, the unauthorized third-party “**acquired certain data,**” of Plaintiffs and the Class, including Social Security numbers, first and last names, addresses, dates of birth, marital statuses, genders, employee identification numbers, and Mondelez retirement and/or thrift plan information.<sup>27</sup>

41. Based on this information from BCLP, Plaintiffs’ and the Class’s Private Information was **stolen** by cybercriminals in the Data Breach.

42. Nearly four (4) months after the Breach began, victims were finally notified of the Data Breach via Notice of Data Breach Letters.<sup>28</sup>

43. This belated notice is despite BCLP’s public assertion in its privacy policy that “[i]f a data breach (leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your personal information) occurs which is likely to result in a high risk of adversely affecting your rights and freedoms, we will inform you of this without undue delay.”<sup>29</sup>

---

<sup>27</sup> *See id.* (emphasis added).

<sup>28</sup> *See id.*

<sup>29</sup> Privacy Notice, BRYAN CAVE LEIGHTON PAISNER LLP, <https://www.bclplaw.com/en->

44. Despite BCLP’s duties and alleged commitments to safeguard PII, BCLP did not follow industry standard practices in securing Plaintiffs’ and the Class’s Private Information, as evidenced by the Data Breach.

45. In response to the Data Breach, BCLP contends it has “taken steps to address the incident and prevent a similar occurrence in the future.”<sup>30</sup> Although BCLP failed to expand on what these alleged “steps” are, such steps should have been in place *before* the Data Breach.

46. Through the Notice of Data Breach Letter, Defendant also recognized the actual imminent harm and injury flowing from the Data Breach and admonished victims of the Data Breach to “remain vigilant by reviewing account statements and monitoring free credit reports.”<sup>31</sup> The Notice of Data Breach Letter also advised victims to “change your passwords” and that they may want to temporarily freeze their credit.<sup>32</sup>

47. Even though highly sensitive information such as Social Security numbers were accessed here, cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity theft, fraud, or misuse Plaintiffs’ and the Class’s PII. Cybercriminals can cross-reference the data stolen from the Data

---

US/legal-notices/privacy-notice.html (last visited Oct. 19, 2023).

<sup>30</sup> Exhibits 1–2.

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

Breach and combine it with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiffs’ and the Class’s financial accounts.

48. Although the Notice Letter claims financial information was not exposed in the Breach, cybercriminals need not harvest a person’s financial account information in order to gain access to pre-existing financial accounts. Cybercriminals can use an individual’s Social Security Number, which was exposed here, to access and drain existing financial accounts.<sup>33</sup>

49. Plaintiffs and the Class were only offered two (2) years of complimentary credit monitoring services, which *does not* adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the Breach involves PII that cannot be easily changed, such as Social Security numbers and information that cannot be changed, such as dates of birth. The Breach exposed nonpublic, highly private information, which is disturbing harm in and of itself and an utter invasion of privacy.

---

<sup>33</sup> See <https://www.gobankingrates.com/retirement/social-security/what-hackers-can-do-with-ssn/> (“Armed with your SSN, hackers could access your bank accounts,” says O’Brien. “They could pose as you to customer support, perform fraudulent transactions, transfer funds, or drain your accounts.”); see also <https://surfshark.com/blog/what-can-someone-do-with-your-ssn/> (“An identity thief can use your SSN together with your PII to open new bank accounts or access existing ones, take out credit cards, and apply for loans all in your name.”); <https://www.moneytalksnews.com/slideshows/heres-what-hackers-can-do-with-your-social-security-number/> (“A criminal with your Social Security number and other data about you could potentially gain access to your existing bank, credit card, loan and other accounts.”); <https://www.washingtonpost.com/creativegroup/discover/is-your-social-security-number-at-risk/> (“The financial cost of a compromised Social Security number can be profound. If someone gets a hold of your Social Security number, ‘they can make unauthorized withdrawals, purchases, and transfers. They can get government documents.’”).

50. Defendant acknowledged the imminent future risk of harm to Plaintiffs and the Class by offering complimentary credit monitoring services.

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

52. Additionally, credit monitoring services do not prevent fraud and identity theft from occurring. It only alerts the individual once the fraud and identity theft has *already* occurred. Thus, it does nothing to prevent future harm to Plaintiffs and the Class.

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

***The Data Breach was a Foreseeable Risk and BCLP was on Notice.***

54. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches affecting law firms preceding the date of the Breach.<sup>34</sup>

---

<sup>34</sup> See *Law Firm Cyberattacks Grow, Putting Operations in Legal Peril*, BLOOMBERG LAW (July 7, 2023, 4:30AM), <https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril> (last visited Oct. 19, 2023); see also *Law Firm Data Breaches Surge In 2023*, Above the Law (Aug. 1, 2023, 11:42 AM), <https://abovethelaw.com/2023/08/law-firm-data-breaches-surge-in-2023/> (last visited Oct.

55. In light of recent high profile data breaches at other law firms,<sup>35</sup> Defendant knew or should have known that their electronic records containing Plaintiffs’ and the Class’s PII would be targeted by cybercriminals.

56. According to Bloomberg, “[n]ews of data breaches at prominent firms has become close to a weekly occurrence.”<sup>36</sup> In fact, “[m]ore than a quarter of law firms in a 2022 American Bar Association survey said they had experienced a data breach, up 2% from the previous year.”<sup>37</sup>

57. “The diversity of client data that law firms handle—financial statements, medical data, and criminal records—makes them a valuable target for cybercriminals.”<sup>38</sup>

---

19, 2023).

<sup>35</sup> See *Law Firm Data Breaches Surge In 2023*, Above the Law (Aug. 1, 2023, 11:42 AM), <https://abovethelaw.com/2023/08/law-firm-data-breaches-surge-in-2023/> (last visited Oct. 19, 2023); *Cyberattacks ‘Inevitable for Law Firms, Highlighting Need for Comprehensive Incident Response Plans*, THE AMERICAN LAWYER (Jan. 10, 2023, 11:41 AM) <https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/#:~:text=Cyberattacks%20on%20law%20firms%20have,business%20data%20compromised%20by%20hackers> (last visited Oct. 19, 2023); *Hacked and Smacked: the Lurking Danger and Costly Ramifications of a Data Breach for Attorneys*, AON ATTORNEYS ADVANTAGE, <https://www.attorneys-advantage.com/Resources/Data-Breach-For-Attorneys>, (last visited Oct. 19, 2023); *Massive Cybersecurity Breach Hits Biggest US Law Firms*, New York Post (July 8, 2023, 4:20 PM), <https://nypost.com/2023/07/08/large-global-law-firms-affected-by-massive-data-brach/>, (last visited Oct. 19, 2023).

<sup>36</sup> *Law Firm Cyberattacks Grow, Putting Operations in Legal Peril*, BLOOMBERG LAW (July 7, 2023, 4:30AM), <https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril> (last visited Oct. 19, 2023)

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

58. “Experts have consistently noted that many law firms fall short of best cybersecurity practices.”<sup>39</sup>

59. The BCLP Data Breach “underscores the increasing frequency of cyber attacks on law firms, which has seen a worrying escalation in recent years. Such breaches often involve sensitive data of both the firms and their clients, highlighting the need for improved security protocols within the industry.”<sup>40</sup>

60. Indeed, cyberattacks against the both the legal industry and other industries 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.”<sup>41</sup>

61. In 2021, a record 1,862 data breaches occurred, resulting in approximately

---

<sup>39</sup> *Law Firm Data Breaches Surge In 2023*, Above the Law (Aug. 1, 2023, 11:42 AM), <https://abovethelaw.com/2023/08/law-firm-data-breaches-surge-in-2023/> (last visited Oct. 19, 2023).

<sup>40</sup> *Law Firm Bryan Cave Leighton Painer Victim of Major Cyberattack*, ONE2CALL, <https://www.one2call.net/law-firm-bryan-cave-leighton-paisner-bclp-victim-of-major-cyber-attack/> (last visited Oct. 19, 2023).

<sup>41</sup> *Gordon M. Snow Statement*, FBI <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.

293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>42</sup> 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.<sup>43</sup>

62. “[E]arlier this year, Proskauer Rose confirmed a similar breach that exposed its clients’ sensitive financial information to hackers. In 2021, data from Goodwin Procter and Jones Day was exposed through a breach at tech provider Accellion, now known as Kiteworks. The firms confirmed the breach resulted in confidential client data exposure. Covington & Burling faced an attack in 2020 that possibly exposed nonpublic information involving about 300 corporate clients. And only recently the Australian law firm HWL Ebsworth announced that it has been the target of a Cyber Attack which resulted in the breach of government data. These incidents highlight a clear pattern of persistent security threats facing law firms and the need for comprehensive cyber security measures to ensure the protection of sensitive client data.”<sup>44</sup>

63. Therefore, the increase in such attacks, and attendant risk of future attacks,

---

<sup>42</sup> *2021 Data Breach Annual Report*, ITRC, [chrome-extension://efaidnbnmnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124\\_ITRC-2021-Data-Breach-Report.pdf](https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf).

<sup>43</sup> *Id.*

<sup>44</sup> *Law Firm Bryan Cave Leighton Painer Victim of Major Cyberattack*, ONE2CALL, <https://www.one2call.net/law-firm-bryan-cave-leighton-paisner-bclp-victim-of-major-cyber-attack/> (last visited Oct. 19, 2023).



was widely known to the public and to anyone in Defendant's industry, including BCLP.

***Plaintiff Rock Meyer's Experience***

64. Plaintiff Meyer received a Notice of Data Breach Letter, dated June 15, 2023, notifying him that an unauthorized third-party "**acquired certain data**" which included his Social Security number, first and last name, date of birth, address, marital status, gender, employee identification number, and retirement and/or thrift plan information.<sup>45</sup>

65. Defendant deprived Plaintiff Meyer of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over four (4) months.

66. As a result of the Data Breach, Plaintiff Meyer spent *hours* dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts and credit reports to monitor any suspicious and/or fraudulent activity, and researching the inadequate credit monitoring services offered to him. This time has been lost forever and cannot be recaptured. Plaintiff Meyer has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft and fraud for the rest of his life.

67. Plaintiff Meyer fears for his personal financial security because his PII was accessed, acquired, and stolen by criminals during the Data Breach. Plaintiff Meyer 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

---

<sup>45</sup> See Exhibit 1.

inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

68. Since the Data Breach, Plaintiff Meyer has been burdened by an influx of spam calls and emails. Plaintiff Meyer reasonably attributes these spam calls and emails to the Data Breach because they have increased significantly after the Data Breach. He was not receiving spam emails and calls of this volume before the Data Breach.

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

70. Plaintiff Meyer has suffered an extreme invasion of his privacy because cybercriminals not only accessed his confidential and personal PII but acquired it as well.

71. Plaintiff Meyer has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being accessed, acquired, and stolen by criminals. The fact that Defendants offered Plaintiffs and the Class credit monitoring services confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Meyer is at an imminent and impending risk of harm because cybercriminals already have or will post his Private Information on the dark web.

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

73. Plaintiff Meyer also suffered injury directly and proximately caused by the

Data Breach, including: (i) theft of Plaintiff Meyer’s valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Meyer’s PII being placed in the hands of cyber criminals; (iii) damages to and diminution in value of Plaintiff Meyer’s PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Meyer should have received from Defendant and Defendant’s defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Meyer’s PII; (v) continued risk to Plaintiff Meyer’s PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant; and (vi) invasion of privacy due to cybercriminals taking possession of his PII and likely posting it on the dark web (if they have not done so already).

***Plaintiff Eric D. Flores’ Experience***

74. Plaintiff Flores received a Notice of Data Breach Letter, dated June 15, 2023, notifying him that an unauthorized third-party “**acquired certain data**” which included his Social Security number, first and last name, date of birth, address, marital status, gender, employee identification number, and retirement and/or thrift plan information.<sup>46</sup>

75. Defendant deprived Plaintiff Flores of the earliest opportunity to guard himself against the Data Breach’s effects by failing to notify him about it for over four (4) months.

---

<sup>46</sup> See Exhibit 2.

76. As a result of the Data Breach, Plaintiff Flores spent *hours* dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts and credit reports to monitor suspicious and fraudulent activity, and researching the inadequate credit monitoring services offered to him. This time has been lost forever and cannot be recaptured. Plaintiff Flores has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft and fraud for the rest of his life.

77. Plaintiff Flores fears for his personal financial security because his PII was accessed, acquired, and stolen by criminals during the Data Breach. Plaintiff Flores 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.

78. Plaintiff Flores suffered actual injury in the form of damages to and diminution in the value of Plaintiff Flores's PII—a form of intangible property that was compromised as a result of BCLP's Data Breach.

79. Plaintiff Flores has suffered an extreme invasion of his privacy because cybercriminals not only accessed his confidential and personal PII but acquired it as well.

80. Plaintiff Flores has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. The fact that Defendants offered Plaintiffs and the Class

credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Flores is at an imminent and impending risk of harm because cybercriminals already have or will post his Private Information on the dark web.

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

82. Plaintiff Flores also suffered injury directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Flores' valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Flores' PII being placed in the hands of cyber criminals; (iii) damages to and diminution in value of Plaintiff Flores' PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Flores should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Flores' PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Flores' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

***Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft***

83. Plaintiffs and members of the proposed Class have suffered injuries from

the Data Breach that can be directly traced to Defendant.

84. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and/or 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 Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

85. 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.

86. The value of Plaintiffs' 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.

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

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

89. Cybercriminals 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.

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

91. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs 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.

92. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' 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.

***Defendant Failed to Adhere to FTC Guidelines.***

93. 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 PII.

94. In 2016, the FTC updated its publication, Protecting PII: 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.

95. 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.

96. 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.

97. 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.

98. Defendant's 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.

## V. CLASS ACTION ALLEGATIONS

99. Plaintiffs sue on behalf of themselves and the proposed classes defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

### Nationwide Class

All individuals residing in the United States whose PII was compromised in the Data Breach discovered by BCLP on or around February 27, 2023, and received a Notice of Data Breach Letter.

### California Subclass

All individuals residing in the State of California whose PII was compromised in the Data Breach discovered by BCLP on or around February 27, 2023, and received a Notice of Data Breach Letter.

Excluded from the Class(es) is Defendant, Mondelez, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

100. Plaintiffs reserve the right to amend the class definitions above.

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

- a. **Numerosity**. Plaintiffs are 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 Defendant's possession, custody, and control;

- c. **Typicality**. Plaintiffs' claims are typical of class 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**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiffs' interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.
- e. **Commonality**. Plaintiffs' 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 Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;
  - 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 PII;

- iv. Whether Defendant breached contractual promises to safeguard Plaintiffs' and the Class's PII;
- 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 Plaintiffs' and the Class's injuries;
- viii. What the proper damages measure is; and
- ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

102. 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.

## **VI. CAUSES OF ACTION**

### **COUNT ONE**

#### **Negligence**

#### **(On Behalf of Plaintiffs and the Nationwide Class)**

103. Plaintiffs reallege all previous paragraphs as if fully set forth below.

104. Plaintiffs' and Class Members' PII was entrusted to Defendant. Defendant owed to Plaintiffs 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, protocols, and infrastructure sufficient to protect the information from a data breach, and to promptly detect attempts at unauthorized access.

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

106. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs 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.

107. Defendant owed these duties to Plaintiffs 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 Plaintiffs' and the Class's PII.

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

109. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and the Class and the importance of exercising reasonable care in handling it. Especially with multiple other law firms experiencing data breaches in recent years.

110. Defendant breached its duties by failing to exercise reasonable care in protecting the PII of Plaintiffs and the Class, supervising and monitoring its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm,

embarrassment, humiliation, frustration, and emotional distress.

111. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs 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 Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

**COUNT TWO**  
**Negligence *Per Se***  
**(On Behalf of Plaintiffs and the Nationwide Class)**

112. Plaintiffs reallege all previous paragraphs as if fully set forth below.

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

114. 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, its customer's current and former employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's PII.

115. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

116. 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 PII.

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

118. 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 Plaintiffs and the Class.

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



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

121. Had Plaintiffs and the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have allowed Defendant to access their PII.

122. Defendant's various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

123. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs 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.

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

**COUNT THREE**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and the Nationwide Class)**

125. Plaintiffs reallege all previous paragraphs as if fully set forth below.

126. This claim is pled in the alternative to the breach of contract claim(s).

127. Plaintiffs and members of the Class conferred a benefit upon Defendant.

Defendant benefited from the receipt of Plaintiffs' and the Class's PII, as this was used to facilitate the services it sold to businesses. Without Plaintiffs' and the Class's PII, Defendant would not be able to provide services and would not be able to obtain profit and revenue therefrom.

128. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class.

129. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

130. Under the principles of equity and good conscience, Defendant should not

be permitted to retain the monetary benefit, because Defendant failed to implement appropriate data management and security measures.

131. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

132. If Plaintiffs and the Class had known that Defendant would not secure the PII it was entrusted with, they would not allow their PII be provided to Defendant.

133. Plaintiffs and Class Members have no adequate remedy at law.

134. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails 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 Plaintiffs and Class Members.

135. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

136. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received for business services on their behalf.

#### **COUNT FOUR**

#### **Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.* (On Behalf of Plaintiffs and the Nationwide Class)**

137. Plaintiffs reallege all previous paragraphs as if fully set forth below.

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

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

140. Defendant 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 its services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiffs' 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 material facts regarding their lack of adequate data security and

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

141. These actions also constitute deceptive and unfair acts or practices because Defendant 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 Plaintiffs and the Class and defeat their reasonable expectations about the security of their PII.

142. Defendant intended reliance on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's goods and services.

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

144. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Class of the nature and extent of the Data Breach pursuant to the Illinois

PII Protection Act, 815 ILCS 530/1, *et seq.*

145. As a result of Defendant's wrongful conduct, Plaintiffs and the Class were injured in that they never would have allowed their PII to be provided to Defendant 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.

146. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant 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 Plaintiffs and Class Members.

147. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as

a result of Defendant's violations of the CFA.

**COUNT FIVE**  
**Violations of the California Unfair Competition Law,**  
**Cal. Bus. & Prof. Code § 17200 *et seq.***  
**(On Behalf of Plaintiff Flores and the California Subclass)**

148. Plaintiff Flores (referred to as "Plaintiff" throughout this Count) realleges all previous paragraphs as if fully set forth below.

149. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

150. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

151. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.*), Cal. Civil Code § 1798.81.5, Cal. Civ. Code § 1798.80 *et seq.*, and Section 5 of the FTC Act. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, and want of ordinary care are ongoing and continue to this date.

152. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and

disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

153. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein and storing Plaintiff's and Class Members' PII in an unsecure, internet accessible, electronic environment. Specific failures to follow industry standards and exercise reasonable care include: failing to encrypt the PII accessed during the Data Breach; maintaining customer PII for longer than it has a legitimate use; failing to regularly update passwords; failure to implement two-factor authentication for access to accounts and systems containing PII; failing to adequately train employees to recognize phishing and other social engineering techniques; and failing to implement and use software that can adequately detect phishing emails. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

154. Defendant's above-described wrongful actions, inaction, want of ordinary care, and practices also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA,



CRA, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant’s wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant’s legitimate business interests other than engaging in the above-described wrongful conduct.

155. Defendant engaged in unfair business practices under the “balancing test.” The harm caused by Defendant’s failure to implement proper data security measures, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant’s failure to follow basic data security protocols cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged.

156. Defendant engaged in unfair business practices under the “tethering test.” Defendant’s failure to implement proper data security measures, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

157. Defendant engaged in unfair business practices under the “FTC test.” The harm caused by Defendant’s failure to implement proper data security measures, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. This harm continues given the fact that Plaintiff’s and California Subclass members’ PII remains in Defendant’s possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant’s actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining “unfair acts or practices” as those that “cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition”); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

158. As a direct and proximate result of Defendant’s unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members’ were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value and the right to control their personal information.

159. Defendant’s violations were, and are, willful, deceptive, unfair, and unconscionable.

160. Plaintiff and California Subclass Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

161. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and California Subclass Members.

162. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

163. Plaintiff and California Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

#### **COUNT SIX**

**Violations of the California Consumer Privacy Act  
Cal. Civ Code §§ 1798.100 *et seq.*, § 1798.150(a)  
(On Behalf of Plaintiff Flores and the California Subclass)**

164. Plaintiff Flores (referred to as "Plaintiff" throughout this Count) realleges all previous paragraphs as if fully set forth below.

165. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

- (A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.
- (B) Injunctive or declaratory relief.
- (C) Any other relief the court deems proper.

166. Defendant is a "business" under § 1798.140(b) because Defendant:
- a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";
  - b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";
  - c. does business in California; and
  - d. has annual gross revenues in excess of \$25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50

percent or more of its annual revenues from selling consumers' personal information.

167. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

168. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and California Subclass members' unencrypted first and last names and Social Security numbers among other information.

169. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, Defendant subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

170. Plaintiffs' and California Subclass members' unencrypted and unredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed,

and viewed by unauthorized third parties.

171. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and California Subclass members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiffs' and California Subclass members' PII as a result of this attack.

172. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

173. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

174. More than 30 days from the filing of this Consolidated Complaint, Plaintiff Flores provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant failed to respond and/or has not cured or is unable to cure the violations described therein. Plaintiffs seek all relief available under the CCPA

including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars (\$750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

**COUNT SEVEN**  
**Injunctive and Declaratory Relief**  
**(On Behalf of Plaintiffs and the Nationwide Class)**

175. Plaintiffs reallege all previous paragraphs as if fully set forth below.

176. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

177. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class Members that requires it to adequately secure their Private Information.

178. Defendant still possesses the Private Information of Plaintiffs and the Class Members.

179. Defendant has not satisfied its obligations and legal duties to Plaintiffs and the Class Members.

180. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

181. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its obligations and duties of care to provide adequate security,

and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;
- c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
- d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- e. Ordering that Defendant segments Plaintiffs' and the Class's Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
- f. Ordering that Defendant cease storing unencrypted Private Information on its systems;
- g. Ordering that Defendant conduct regular database scanning and securing checks;



- h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- i. Ordering Defendant to implement and enforce adequate retention policies for Private Information, including destroying, in a reasonably secure manner, Private Information once it is no longer necessary for it to be retained; and
- j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

**COUNT EIGHT**  
**Breach of Third-Party Beneficiary Contract**  
**(On Behalf of Plaintiffs and the Nationwide Class)**

182. Plaintiffs reallege all previous paragraphs as if fully set forth below.

183. Plaintiffs and Class Members are intended third-party beneficiaries of a contract entered into between BCLP and Mondelez (the “contracting parties”), including a contract entered into before the Data Breach to provide legal services and securely store Plaintiffs’ and the Class’s PII that BCLP obtained from Mondelez (the “Contract”).

184. On information and belief, that respective contract contained provisions requiring BCLP to protect the PII that Mondelez received and in turn, disclosed to BCLP, in order to provide services to Mondelez.

185. On information and belief those provisions requiring BCLP to protect the PII it received from Mondelez were intentionally included for the direct benefit of Plaintiffs and Class Members, such that Plaintiffs and Class Members are intended third-party beneficiaries of this contract and are therefore entitled to enforce them.

186. BCLP breached the contract by not safeguarding Plaintiffs' and Class Members' PII and not utilizing adequate data security, as described herein, resulting in the Data Breach.

187. Exposure, breach, and identity theft were the expected risks both contracting parties could foresee from the improper performance of the Contract.

188. The injuries suffered by Plaintiffs and Class Members were the kind that proper performance was intended to prevent.

189. As a direct and proximate result of BCLP's breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

190. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial.

## **COUNT NINE**

### **Bailment**

#### **(On Behalf of Plaintiffs and the Nationwide Class)**

191. Plaintiffs reallege all previous paragraphs as if fully set forth below.

192. Plaintiffs' and Class Members' PII was provided to BCLP through its business relationship with Mondelez in the ordinary course of business.

193. BCLP was under a duty to keep the PII it received, including that of Plaintiffs' and the Class's, private and confidential.

194. There was a shared understanding that Plaintiffs' and the Class's PII would remain confidential.

195. Plaintiffs' and Class Members' PII is personal property, and it was conveyed to BCLP for the certain purpose of keeping the information private and confidential.

196. Plaintiffs' and Class Members' PII has value, and it is highly prized by hackers and cybercriminals. BCLP was aware of the risks it took when accepting their PII for safeguarding, and it assumed the risk voluntarily.

197. Once BCLP accepted Plaintiffs' and Class Members' PII, it was in the exclusive possession of that PII, and neither Plaintiffs nor Class Members could control that information once it was within BCLP's possession, custody, and control.

198. BCLP did not safeguard Plaintiffs' or Class Members' PII when it failed to adopt and enforce adequate security safeguards to prevent a known risk of cyberattack.

199. BCLP's failure to safeguard Plaintiffs' and Class Members' PII resulted in their PII being accessed and obtained by third-party cybercriminals.

200. BCLP failed to return Plaintiffs' and the Class's PII after the Breach.

201. As a result of BCLP's failure to keep Plaintiffs' and Class Members' PII secure, Plaintiffs and Class Members suffered injury, for which compensation-including nominal damages and compensatory damages-are appropriate.

**VII. PRAYER FOR RELIEF**

Plaintiffs 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 Plaintiffs and the proposed Class, appointing Plaintiffs 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 Plaintiffs and the Class;
- c. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;
- d. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- e. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- f. Awarding restitution and damages to Plaintiffs 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 Plaintiffs 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.

### **VIII. JURY DEMAND**

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: November 10, 2023

Respectfully submitted,

/s/: William B. Federman

William B. Federman  
**FEDERMAN & SHERWOOD**  
10205 N. Pennsylvania Ave.  
Oklahoma City, OK 73120  
Telephone: (405) 235-1560  
Facsimile: (405) 239-2112  
wbf@federmanlaw.com  
*Interim Lead Class Counsel*

Thomas A. Zimmerman, Jr.  
(IL #6231944)  
tom@attorneyzim.com  
**ZIMMERMAN LAW**  
**OFFICES, P.C.**  
77 W. Washington Street  
Suite 1220  
Chicago, Illinois 60602  
(312) 440-0020 telephone  
(312) 440-4180 facsimile  
*Interim Liaison Class Counsel*

M. Anderson Berry  
**CLAYEO C. ARNOLD,**  
**A PROFESSIONAL LAW CORP.**  
865 Howe Avenue  
Sacramento, CA 95825  
Telephone: (916) 239-4778

Facsimile: (916) 924-1829

aberry@justice4you.com

***Additional Counsel for Plaintiffs and  
the Class***

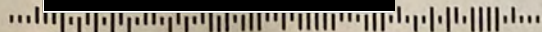
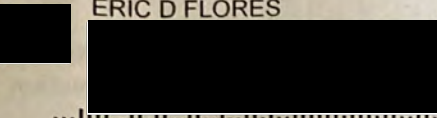
# Exhibit 1



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

June 15, 2023

J5767-L01-0038026 T00097 P004 \*\*\*\*\*ALL FOR AADC 920  
ERIC D FLORES



**Re: NOTICE OF DATA BREACH**

Dear Eric D Flores:

Mondelēz Global LLC (“Mondelēz,” “we,” “us,” “our”) is writing to inform you of an incident that involved some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you can take to protect your personal information. Mondelēz takes this incident and the security of your personal information very seriously, and we sincerely regret any concern or issue this incident may cause.

**WHAT HAPPENED?** Mondelēz retained the legal services of the law firm Bryan Cave Leighton Paisner LLP (“Bryan Cave”) to provide advice on customary legal matters of a company its size. To provide these services, Bryan Cave obtained some personal information of current and former Mondelēz employees.

Bryan Cave has stated that on February 27, 2023, it detected unauthorized access to its systems, including an area it used to store certain customer files. This access occurred from February 23, 2023 until March 1, 2023. Bryan Cave initiated a robust investigation with the assistance of an outside cybersecurity forensics firm and notified law enforcement. Bryan Cave informed us of unauthorized access on March 24, 2023, while continuing to investigate the incident, and later confirmed that an unauthorized third party acquired certain data, which was still being determined. On May 22, 2023, based upon additional information received from Bryan Cave, Mondelēz determined that it finally had enough information to determine who was impacted and that affected individuals should be notified. Mondelēz proceeded to conduct a thorough review of impacted information to identify all affected current and former employees, which was just completed, and is now providing notification. Please know that this incident did not occur on or affect Mondelēz systems or networks in any way.

**WHAT INFORMATION WAS INVOLVED?** The investigation determined that the personal information which was included in the impacted data may include your: social security number, first and last name, address, date of birth, marital status, gender, employee identification number, and Mondelēz retirement and/or thrift plan information. Financial information, such as account information or credit card numbers, were not involved in this incident.

**WHAT WE ARE DOING.** Please know that protecting your personal information is something that Mondelēz takes very seriously. Bryan Cave conducted an investigation with an outside cybersecurity forensic firm to confirm the nature and scope of the incident. Bryan Cave also notified law enforcement. Bryan Cave informed us that they have taken steps to address the incident and prevent a similar occurrence in the future. Mondelēz is providing notice and offering credit monitoring services to individuals based on the personal information that was potentially impacted.



**WHAT YOU CAN DO.** We encourage you 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. If you have questions, please contact us at the number described below.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> Credit Plus 1B for 24 months. This helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

To enroll in this credit monitoring service, please contact Experian by calling the phone number listed below. If you have internet access, you may also enroll by visiting the website listed below. You will need the Activation Code provided below to complete your enrollment.

**Enrollment URL:** <https://www.experianidworks.com/plus>

**Your Activation Code:** [REDACTED]

**Enrollment Deadline:** September 30, 2023 (Please be sure to enroll by this date; your code will not work after the deadline.)

If you have questions about the product or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-901-4621 by September 30, 2023. Be prepared to provide engagement number B096059 for Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

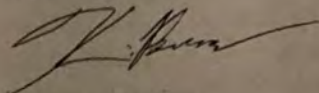
- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only. \*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Internet Surveillance: Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE<sup>TM</sup>: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$1 Million Identity Theft Insurance<sup>\*\*</sup>: Provides coverage for certain costs and unauthorized electronic fund transfers.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**FOR MORE INFORMATION.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-901-4621 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide engagement number B096059.

Sincerely,



Kevin Brennan  
Chief Counsel Litigation (US)

B096059

**Information About Identity Theft Protection****Monitor Your Accounts**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax®**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 9701  
Allen, TX 75013-9701  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion®**  
P.O. Box 1000  
Chester, PA 19016-1000  
1-800-888-4213  
[www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

**Credit Freeze**

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

**Fraud Alerts**

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016-2000  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Additional Information**

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

**The Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**District of Columbia Residents:** You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia  
400 6<sup>th</sup> Street, NW  
Washington, D.C. 20001  
(202) 727-3400  
Email: [oag@dc.gov](mailto:oag@dc.gov)  
<https://oag.dc.gov/Consumer>

**Maryland Residents:** You may obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office at:

Attorney General of Maryland  
200 St. Paul Place  
Baltimore, MD 21202  
Telephone: 1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include: the right to access information in your consumer file at a consumer reporting agency; to dispute incomplete or inaccurate information in your consumer file at a consumer reporting agency; to have consumer reporting agencies correct or delete inaccurate information in your consumer file; the right to block information in your consumer file that is the result of identity theft; and the right to have a fraud alert placed on your consumer file (as described above). For more information, please visit [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf).

**New York Residents:** You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General  
Consumer Frauds & Protection Bureau  
The Capitol  
Albany, NY 12224-0341  
(800) 771-7755  
<https://ag.ny.gov/consumer-frauds-bureau>

New York Department of State  
Division of Consumer Protection  
99 Washington Avenue, Suite 650  
Albany, NY 12231  
(800) 697-1220  
[www.dos.ny.gov](http://www.dos.ny.gov)

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina  
114 West Edenton Street  
Raleigh, NC 27699-9001  
Telephone: 1-919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

**Oregon Residents:** You may obtain information about reporting suspected identity theft from the following Oregon agencies:

Office of the Attorney General  
Oregon Department of Justice  
1162 Court St. NE  
Salem, OR 97301-4096  
Email: [AttorneyGeneral@doj.state.or.us](mailto:AttorneyGeneral@doj.state.or.us)

Office of Attorney General  
Consumer Protection  
Toll-Free: 1-877-877-9392  
<https://justice.oregon.gov/consumercomplaints/>