

Exhibit A

The ILND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (See instructions on next page of this form.)

I. (a) PLAINTIFFS

MICHAEL SHIELDS, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff (Except in U.S. plaintiff cases)

(c) Attorneys (firm name, address, and telephone number)

Gary M. Klinger, Milberg Coleman Bryson Phillips Grossman, PLLC 227 W. Monroe St., Ste. 2100, Chicago, IL 60606; (866) 252-0878

DEFENDANTS

MONDELEZ GLOBAL, LLC

County of Residence of First Listed Defendant (In U.S. plaintiff cases only)

Note: In land condemnation cases, use the location of the tract of land involved.

Attorneys (If Known)

Not Known

II. BASIS OF JURISDICTION (Check one box, only.)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question, 4 Diversity

III. CITIZENSHIP OF PRINCIPAL PARTIES (For Diversity Cases Only.)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

IV. NATURE OF SUIT (Check one box, only.)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, SOCIAL SECURITY, FEDERAL TAXES, OTHER STATUTES.

V. ORIGIN (Check one box, only.)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District, 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

VII. PREVIOUS BANKRUPTCY MATTERS (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

Check if this is a class action under Rule 23, F.R.C.V.P.

Demand \$ 500000

CHECK Yes only if demanded in complaint:

Jury Demand: Yes No

IX. RELATED CASE(S) IF ANY (See instructions):

Judge Case Number

X. Is this a previously dismissed or remanded case?

Yes No If yes, Case #

Name of Judge

Date: 6/23/2023

Signature of Attorney of Record /s/ Gary M. Klinger

Authority for Civil Cover Sheet

The ILND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use
(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the
(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box. Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

DANIEL BERNDT, on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Winnebago County, IL (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

David Lietz, Milberg Coleman, 5335 Wisconsin Ave. NW, Ste. 440, Washington, D.C., 20015, (866) 252-0878

DEFENDANTS

MONDELEZ GLOBAL LLC

County of Residence of First Listed Defendant Cook County, IL (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

Not Known

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

Large table with categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes sub-sections like PERSONAL INJURY, PERSONAL PROPERTY, HABES CORPUS, etc.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)(2); 28 U.S.C. § 1391(b)
Brief description of cause: Data breach

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ 5,000,000 CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER 1:23-cv-03399

DATE June 23, 2023 SIGNATURE OF ATTORNEY OF RECORD s/ David K. Lietz

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

DANIEL BERNDT, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

MONDELÉZ GLOBAL LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Daniel Berndt (“Plaintiff”), individually and on behalf of all other similarly situated individuals (the “Class Members,” as defined below), by and through counsel, file this Amended Class Action Complaint against Mondelēz Global LLC (“Mondelēz” or “Defendant”) and allege the following based on personal knowledge of facts pertaining to him and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Mondelēz is a food retailer and is part of one of the largest snack companies in the world. Mondelēz is a wholly owned subsidiary of Mondelēz International, Inc., which had global net revenues of approximately \$31.5 billion in 2022.¹

2. Plaintiff and the other Class Members are current and former employees of Mondelēz. As part of their employment, Plaintiff and the Class entrusted their sensitive information to Mondelēz with the reasonable expectation that Mondelēz would maintain that information safely and securely. Defendant betrayed the trust of Plaintiff and the other Class

¹ See <https://www.mondelezinternational.com/About-Us>.

Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

3. Plaintiff and the Class Members (as further defined below) have had their personal identifiable information exposed as a result of Mondelēz’s inadequately secured computer network.

4. This class action seeks to redress Mondelēz’s unlawful, willful and wanton failure to protect the personal identifiable information of approximately 51,110 individuals that was exposed in a major data breach of Defendant’s network (the “Data Breach” or “Breach”), in violation of its legal obligations.²

5. The Data Breach was discovered on February 27, 2023, when Mondelēz became aware of unauthorized activity on its systems, including in an area it used to store customer files.³ Mondelēz investigated the attack with the assistance of legal counsel and third-party computer specialists. The investigation confirmed that certain Mondelēz systems containing confidential and personal information had been accessed without authorization between at least February 23, 2023 until March 1, 2023.⁴ In addition, investigators determined unauthorized access on March 24, 2023, and “confirmed that an unauthorized third party acquired certain data.”⁵

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

³ See <https://www.doj.nh.gov/consumer/security-breaches/documents/mondelez-global-20230615.pdf>.

⁴ *Id.*

⁵ *Id.*

6. According to Mondelēz, the personal identifiable information exposed in the Breach included: 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 (the “Private Information”).⁶

7. Due to Defendant’s negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of hundreds of thousands of individuals.

8. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

9. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

⁶ See <https://apps.web.maine.gov/online/aevviewer/ME/40/ca25f29f-db60-4baf-ba53-8bae79da4d97.shtml>; see also Breach Notice Letter, attached hereto as Exhibit 1.

II. THE PARTIES

Plaintiff

10. Plaintiff Daniel Berndt is domiciled in and a citizen of Illinois.

11. Sometime shortly after June 15, 2023, Plaintiff received a breach notification letter from Mondelēz informing him that his personal information had been exposed to cybercriminals during the Data Breach. According to the notice letter, Plaintiff's 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 may have been accessed by unauthorized cybercriminals.

Defendants

12. Mondelēz is one of the largest snack companies in the world. In 2022, Mondelēz's parent company recognized global net revenues of approximately \$31.5 billion.

13. Mondelēz Global LLC is a limited liability company food retailer, incorporated under the state laws of Delaware with its principal place of business located at 905 West Fulton Market, Suite 200, Chicago, Illinois.

III. JURISDICTION AND VENUE

14. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

15. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant

employs a significant number of Class Members in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

16. The Data Breach was discovered on February 27, 2023, when Mondelēz became aware of unauthorized activity on its systems, including in an area it used to store customer files.⁷ Mondelēz investigated the attack with the assistance of legal counsel and third-party computer specialists. The investigation confirmed that certain Mondelēz systems containing confidential and personal information had been accessed without authorization between at least February 23, 2023 until March 1, 2023.⁸ In addition, investigators determined unauthorized access on March 24, 2023, and “confirmed that an unauthorized third party acquired certain data.”⁹

17. 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.

18. Despite having known about the Data Breach since February 27, 2023, notices were not sent to affected individuals until June 15, 2023.

19. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff’s and the other Class Members’ Private Information from unauthorized disclosure.

20. Defendant also failed to provide timely and sufficiently notice to Plaintiff and Class Members.

⁷ See <https://www.doj.nh.gov/consumer/security-breaches/documents/mondelez-global-20230615.pdf>.

⁸ *Id.*

⁹ *Id.*

21. Defendant's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

B. Plaintiff's Experience

22. Shortly after June 15, 2023, Plaintiff received a breach notification letter from Mondelēz informing him that his personal information, including his 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, had been potentially accessed and/or acquired by cybercriminals during the Data Breach.

23. Plaintiff and Class Members' Private Information was provided to Defendant as part of his employment with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Omitted from the Notice Letter were any explanations as to why it took Defendant approximately four months after detecting the Data Breach to inform Plaintiff and Class Members of its occurrence, the details of the root cause of the Data Breach, the vulnerabilities exploited, the precise information that was exposed to cybercriminals, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

25. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

26. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

27. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their Social Security numbers. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

28. Because of the Data Breach, Plaintiff's Private Information is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

29. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his personal information, reviewing his financial statements for accuracy, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Mondelēz specifically directed him to take these actions. Indeed, the letter stated: "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."¹⁰

¹⁰ See <https://www.doj.nh.gov/consumer/security-breaches/documents/mondelez-global-20230615.pdf>.

30. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

31. Plaintiff has been careful to protect and monitor his identity.

32. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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 Private Information; and (e) continued risk to Plaintiff's Private Information, 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 Private Information that was entrusted to Defendant.

C. Cyber Criminals Have Used and Will Continue to Use Plaintiff's Private Information to Defraud Them

33. Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

34. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.¹¹ For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.¹² These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

35. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.*¹³

[Emphasis added.]

¹¹ "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

¹² See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

¹³ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

36. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.¹⁴

37. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Mondelēz is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.¹⁵ “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”¹⁶

38. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to Private Information, they *will* use it.¹⁷

39. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information *may continue for years*. As a result, studies

¹⁴ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, <https://www.gao.gov/assets/270/262904.html>.

¹⁵ Michael Kan, *Here’s How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

¹⁶ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

¹⁷ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁸

40. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.¹⁹

41. The ramifications of Defendant's failure to keep its Class Members' Private Information secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

42. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

43. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.²⁰ This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.²¹

¹⁸ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, <https://www.gao.gov/assets/270/262904.html>.

¹⁹ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

²⁰ See Medical ID Theft Checklist, available at: <https://www.identityforce.com/blog/medical-id-theft-checklist-2>.

²¹ Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, available at:

44. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.²²

45. Defendant’s offer of limited identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the offered coverage has expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Mondelēz’s gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (i.e., fraudulent acquisition and use of another person’s Private Information)—it does not prevent identity theft.²³ Nor can an identity monitoring service remove personal information from the dark web.²⁴ “The people who trade in stolen personal information [on the dark web] won’t cooperate with an identity theft service or anyone else, so it’s impossible to get the information removed, stop its sale, or prevent someone who buys it from using it.”²⁵

<https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>.

²² “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4 (Sept. 2013), <http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>.

²³ See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

²⁴ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

²⁵ *Id.*

46. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

47. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

- a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;
- b. Trespass, damage to, and theft of their personal property including Private Information;
- c. Improper disclosure of their Private Information;
- d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;
- e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;
- f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
- h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal information for which there is a well-established and quantifiable national and international market;
- i. The loss of use of and access to their credit, accounts, and/or funds;
- j. Damage to their credit due to fraudulent use of their Private Information; and
- k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

48. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.²⁶ For example, Private Information can be sold at a price ranging from \$40 to \$200.²⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁸

49. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's Private Information.

²⁶ Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

²⁷ Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

²⁸ *In the Dark*, VPN Overview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

50. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Mondelēz is removed from Mondelēz’s unencrypted files.

51. Defendant acknowledged, in its letter to Plaintiff and other Class Members, that the Data Breach would cause inconvenience to effected individuals by providing numerous steps for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.²⁹

52. In particular, the letter acknowledged that financial harm would likely occur, advising Class Members to “to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity.”

53. At Mondelēz’s suggestion, Plaintiff is desperately trying to mitigate the damage that Mondelēz has caused her. Given the kind of Private Information Mondelēz made accessible to hackers, however, Plaintiff is very likely to incur additional damages. Because identity thieves have his Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.³⁰

54. None of this should have happened.

D. Defendant was Aware of the Risk of Cyber Attacks

55. Data security breaches have dominated the headlines for the last two decades. And it doesn’t take an IT industry expert to know it. The general public can tell you the names of some

²⁹ See <https://www.q-staffing.com/wp-content/uploads/2022/06/Qualified-Staffing-Website-Notice.pdf>; see also Exhibit 1, attached hereto.

³⁰ *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

of the biggest cybersecurity breaches: Target,³¹ Yahoo,³² Marriott International,³³ Chipotle, Chili's, Arby's,³⁴ and others.³⁵

56. Mondelēz should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

57. To be sure, Mondelēz has already been the victim of previous data breaches that similarly exposed individual's unencrypted personal information to the extent that it required Mondelēz to issue notices to affected individuals and various states' Attorneys' General.³⁶

58. Moreover, Mondelēz's website boasts, "[p]rotecting your personal information is important to us."³⁷ Mondelēz's privacy policy further ensures, "[w]e maintain administrative,

³¹ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.

³² Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

³³ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), <https://www.thessslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/>.

³⁴ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b>.

³⁵ See, e.g., Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

³⁶ See <https://www.doj.nh.gov/consumer/security-breaches/documents/mondelez-international-20180816.pdf>.

³⁷ See <https://www.mondelezinternational.com/Privacy-Policy#otnotice-section-0b809480-5293-4d75-ae1-8c4afd2a12ca>.

technical, and physical safeguards designed to help protect against unauthorized use, disclosure, alteration, or destruction of the personal information we collect....”³⁸

59. Mondelēz’s assurance makes it evident that Mondelēz recognized it had a duty to use reasonable measures to protect the Private Information that it collected and maintained. Yet, it appears that Mondelēz did not meaningfully or comprehensively use the reasonable measures, including the measures it claims to utilize.

60. Mondelēz was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. Mondelēz Could Have Prevented the Data Breach

61. Data breaches are preventable.³⁹ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”⁴⁰ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised”⁴¹

62. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information

³⁸ *Id.*

³⁹ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

⁴⁰ *Id.* at 17.

⁴¹ *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.⁴²

63. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.⁴³ The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

64. Upon information and belief, Mondelēz failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Mondelēz also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the

⁴²*Id.*

⁴³ FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

65. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁴⁴

66. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

⁴⁴ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁴⁵

67. Further, to prevent and detect cyberattacks, including the attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization’s helpdesk, search the internet for the sender organization’s website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....

⁴⁵ *Id.* at 3-4.

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website’s security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁴⁶

68. In addition, to prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
 - Prioritize and treat commodity malware infections as potential full compromise;

⁴⁶ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001>.

- **Include IT Pros in security discussions**
 - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
 - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**
 - Use Windows Defender Firewall
 - Enable tamper protection
 - Enable cloud-delivered protection
 - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁴⁷

69. Given that Defendant was storing the Confidential Information of more than 80,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect malicious cyberattacks.

70. Specifically, among other failures, Mondelēz had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.⁴⁸ Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal

⁴⁷ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

⁴⁸ See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

information, stating “[o]ur message to these organizations is simple: encryption is your best defense against these incidents.”⁴⁹

71. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

F. Defendant’s Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

72. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

73. Defendant stated that it discovered the Data Breach in October 2021. And yet, Mondelēz did not notify affected individuals until June 2022—*eight months after it learned of the Data Breach*. Even then, Mondelēz failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

74. During these intervals, the cybercriminals were exploiting the information while Mondelēz was secretly still investigating the Data Breach.

75. If Mondelēz had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

⁴⁹“Stolen Laptops Lead to Important HIPAA Settlements,” U.S. Dep’t of Health and Human Services (Apr. 22, 2014), available at <https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html>.

V. CLASS ACTION ALLEGATIONS

76. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

77. Plaintiff brings this action against Mondelēz on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the “Class”) defined as follows:

All persons Mondelēz identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

78. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

79. Members of the Class are referred to herein as “Class Members.”

80. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

81. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

82. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 51,110 individuals.

83. **Typicality:** Plaintiff’s claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Mondelēz’s uniform misconduct. The same event and conduct that gave rise to Plaintiff’s claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Mondelēz.

84. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

85. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Mondelēz's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

86. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

- c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;
- d. Whether Mondelēz breached its duties to Plaintiff and the Class as a result of the Data Breach;
- e. Whether Mondelēz failed to provide adequate cyber security;
- f. Whether Mondelēz knew or should have known that its computer and network security systems were vulnerable to cyber attacks;
- g. Whether Mondelēz's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;
- h. Whether Mondelēz was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within its network;
- i. Whether Mondelēz was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;
- j. Whether Mondelēz failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;
- k. Whether Mondelēz continues to breach duties to Plaintiff and the Class;
- l. Whether Plaintiff and the Class suffered injury as a proximate result of Mondelēz's negligent actions or failures to act;
- m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

- n. Whether Mondelēz's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

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

87. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

88. Defendant Mondelēz solicited, gathered, and stored the Private Information of Plaintiff and the Class.

89. Defendant had full knowledge of the sensitivity of the Private Information it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in Mondelēz's possession. As such, a special relationship existed between Mondelēz and Plaintiff and the Class.

90. Defendant was well aware of the fact that cyber criminals routinely target corporations, particularly those servicing the health industry, through cyberattacks in an attempt to steal the collected Private Information.

91. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard

such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

92. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

93. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks, including by encrypting documents containing Private Information, by not permitting documents containing unencrypted Private Information to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive Private Information. Additional duties that Mondelēz owed Plaintiff and the Class include:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
- b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. To adequately and properly audit and test its systems;
- d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
- e. To train its employees not to store Private Information for longer than absolutely necessary;
- f. To implement processes to quickly detect a data breach, security incident, or intrusion; and

- g. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

94. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information. Plaintiff and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with industry standards. Accordingly, Defendant has committed negligence *per se* by violating the FTC Act.

95. Various FTC publications and data security breach orders further form the basis of Defendant's duty.

96. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Mondelēz. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

97. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;
- b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

- c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;
- d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information, including maintaining it in an encrypted format;
- e. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;
- f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- g. Failing to abide by reasonable retention and destruction policies for Private Information it collects and stores; and
- h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

98. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

99. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

100. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

101. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

102. Plaintiff and the Class have suffered injury, including as described herein, and are entitled to actual and punitive damages in an amount to be proven at trial.

**SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of all Plaintiff and the Class)**

103. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

104. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant’s duty.

105. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

106. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

107. Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

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

109. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

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

111. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) lost or diminished value of their Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) damage to their credit scores; and (vi) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

112. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

113. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private

Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

114. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

115. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

116. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiff and the Class)**

117. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

118. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of their labor and by providing their valuable Private Information to Defendant.

119. Plaintiff and Class Members provided Defendant their labor and Private Information on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

120. Defendant benefited from receiving Plaintiff's and Class Members' labor and from receiving their Private Information through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

121. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

122. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

123. However, acceptance of the benefit under the facts and circumstances described herein 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 Plaintiff's and Class Members' Private Information. 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff 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.

124. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement the appropriate data management and security measures.

125. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

126. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to allow Defendant to have or maintain their Private Information.

127. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended on data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

128. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

129. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

**FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiff and the Class)**

130. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

131. Plaintiff and the Class entrusted their Private Information to Defendant in order to receive and maintain employment. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

132. In its Privacy Policy, Defendant represented that it values personal information and has implemented measures to help ensure an appropriate level of data security.

133. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

134. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

135. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

136. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

**FIFTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of all Plaintiff and the Class)**

137. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

138. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiff and the Class, including its duty to keep Plaintiff and Class Members' Private Information reasonably secure.

139. The fiduciary duty is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which required Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information it maintains and to keep it free from disclosure.

140. Defendant breached its fiduciary duty to Plaintiff by failing to implement sufficient safeguards and by disclosing Plaintiff's and other Class Members' Private Information to unauthorized third parties.

141. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential Private Information, Plaintiff and the Class Members have suffered damages.

142. As a direct result of Defendant's breach of its fiduciary duty and the disclosure of Plaintiff's and Class Members' Private Information, Plaintiffs and the Class have suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and humiliation.

143. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of the Private Information; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) loss of the benefit of the bargain; and (viii) emotional distress. At the very least, Plaintiff and the Class are entitled to nominal damages.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;
- b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

- e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
- f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated: June 23, 2023

Respectfully submitted,

/s/ David K. Lietz

David K. Lietz

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

5335 Wisconsin Avenue NW, Suite 440

Washington, D.C. 20015-2052

Telephone: (866) 252-0878

Facsimile: (202) 686-2877

dlietz@milberg.com

A. Brooke Murphy

(*pro hac vice* application forthcoming)

MURPHY LAW FIRM

4116 Will Rogers Pkwy, Suite 700

Oklahoma City, OK 73108

Telephone: (405) 389-4989

abm@murphylegalfirm.com

EXHIBIT 1

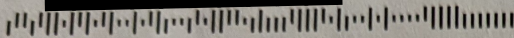


Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 15, 2023



J5767-L01-0028704 T00070 P003 *****SCH 5-DIGIT 61080
DANIEL BERNDT



Re: NOTICE OF DATA BREACH

Dear Daniel Berndt:

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.

B096059

0028704



J5767_L01

— EXHIBIT A —



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

June 15, 2023

J5767-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 GENERAL US ADULT 1B

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Re: NOTICE OF DATA BREACH

Dear Sample A. Sample:

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.

0000001



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 IdentityWorksSM 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.

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: ABCDEFGHI
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:

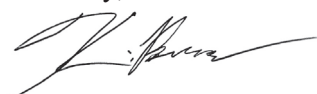
- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only. *
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Internet Surveillance: Technology searches the web, chat rooms and 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 ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$1 Million Identity Theft Insurance^{**}: 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)

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, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at 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

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
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

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
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

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
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

0000001



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

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 6th Street, NW
Washington, D.C. 20001
(202) 727-3400
Email: 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

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.

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

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

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

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

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

AUGUSTYN WIACEK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

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

Defendants.

Case No. 1:23-cv-04023

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

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

INTRODUCTION

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

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

affected over 51,000 individuals.²

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

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

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

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

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

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

² Mondelēz retirement data breached after hacker targets law firm Bryan Cave, Cybersecurity Dive, <https://www.cybersecuritydive.com/news/mondelez-retirement-hacker-targets-law-firm/653600/> (last visited June 23, 2023).

³ About us, Mondelez, <https://www.mondelezinternational.com/> (last visited June 23, 2023).

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

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

9. Defendants' failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

10. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

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

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

13. Plaintiff Augustyn Wiacek is a Data Breach victim.

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

Defendants' possession.

PARTIES

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

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

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

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

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

JURISDICTION & VENUE

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

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

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

BACKGROUND FACTS

BCLP

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

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

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

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

⁴ About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html> (last visited June 23, 2023).

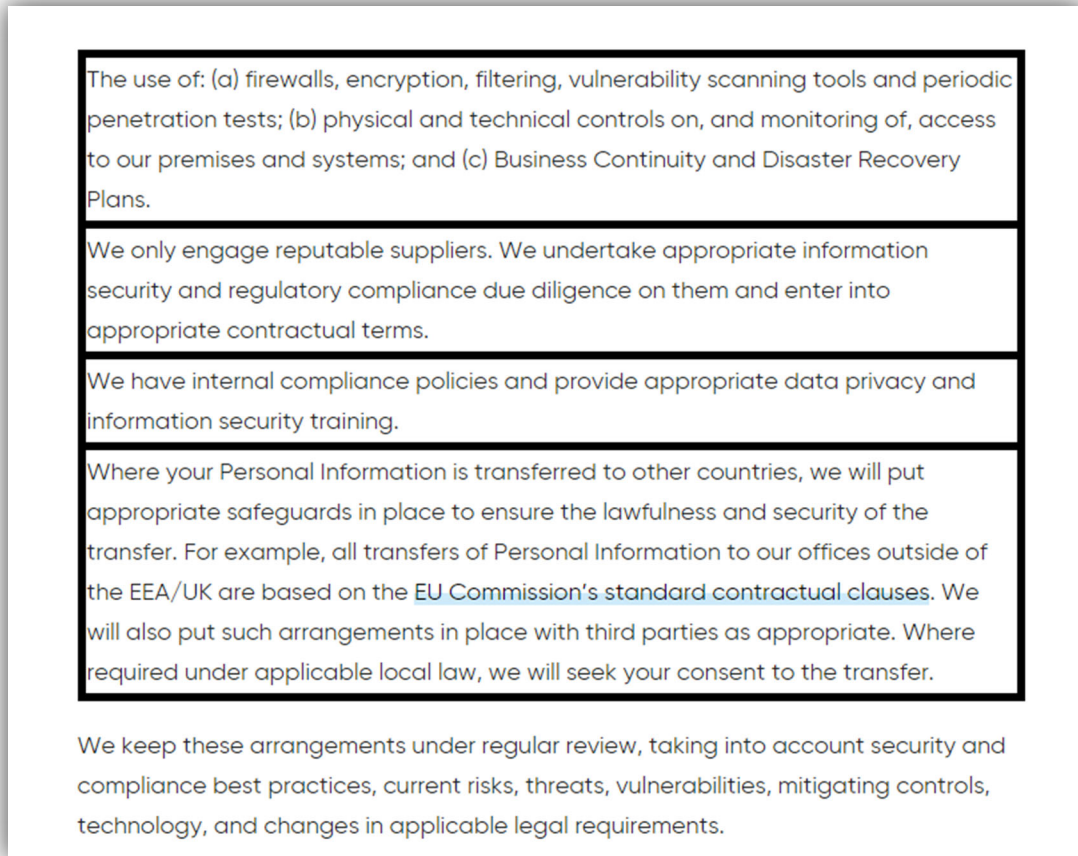
⁵ Data Privacy & Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html> (last visited March 16, 2023).

⁶ BCLP Revenue, Zippia, <https://www.zippia.com/bryan-cave-careers-17522/revenue/> (last visited June 23, 2023).

⁷ About us, BCLP, <https://www.bclplaw.com/en-US/about/about-bclp.html> (last visited June 23, 2023).

⁸ Data Privacy and Security, BCLP, <https://www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html#overview> (last visited June 23, 2023).

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



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

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

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

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

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 its client’s employee’s data and prioritize its data security. In fact, BCLP advertises that its “experience and practical approach to data breach response uniquely equip us to assist organizations by understanding both the law and the business implications of data breaches.”¹²

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

Mondelez

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

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

¹¹ *Id.*

¹² *Id.*

¹³ About us, Mondelez, <https://www.mondelezinternational.com/About-Us> (last visited June 23, 2023).

¹⁴ *Id.*

¹⁵ Investor Release Details, Mondelez, <https://ir.mondelezinternational.com/news-releases/news-release-details/mondelez-international-reports-q4-and-fy-2022-results> (last visited June 23, 2023).

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

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

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

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

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

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

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

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

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

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

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

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

51. On information and belief, Mondelez has offered only two years of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Further, the breach exposed employees' nonpublic, highly private information, a disturbing harm in and of itself.

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

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

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

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

55. In light of recent high profile data breaches at other law firm advising and food industry companies¹⁷, Defendants knew or should have known that their electronic records and employees' PII would be targeted by cybercriminals.

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

56. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁸ The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹⁹

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

58. Cyberattacks on the food industry and legal partner and advisers like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”²¹

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

Plaintiff Wiacek’s Experience

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

¹⁹ *Id.*

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

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

60. Plaintiff Wiacek is former Mondelez employee.

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

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

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

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

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

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

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

68. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

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

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

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

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

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

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;

- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

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

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

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

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

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

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

80. Defendants disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

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

Defendants failed to adhere to FTC guidelines.

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

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

- a. protect the sensitive consumer information that they keep;
- b. properly dispose of PII that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network’s vulnerabilities; and
- e. implement policies to correct security problems.

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

85. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

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

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

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

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

- i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;
- ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendants were negligent in maintaining, protecting, and securing PII;
- iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's PII;
- v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendants' Breach Notice was reasonable;
- vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

- viii. What the proper damages measure is; and
- ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

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

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

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

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

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

95. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

96. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's PII.

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

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

99. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and

members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

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

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

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

103. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's PII.

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

105. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

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

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

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

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

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

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

112. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

146. Defendants' reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

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

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

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

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

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

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

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

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

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

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

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

158. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting 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 Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

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

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

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

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

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

164. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

PRAYER FOR RELIEF

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

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: June 23, 2023

Respectfully submitted,

By: /s/ Raina C. Borrelli

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

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

DEIDRA CLAY, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Highland County, OH (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number) LAUKAITIS LAW LLC, 954 Avenida Ponce De Leon, Suite 205, #10518, San Juan, PR 00907 (215) 789-4462

DEFENDANTS

MONDELEZ GLOBAL LLC

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF, DEF, 1, 2, 3, 4, 5, 6, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

Table with columns: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes codes like 110 Insurance, 210 Land Condemnation, 310 Airplane, 365 Personal Injury, 625 Drug Related Seizure, 710 Fair Labor Standards, 820 Copyrights, 870 Taxes, 375 False Claims Act, etc.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U. S. C.1332 (d) Brief description of cause: Class action data breach

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ 5,000,001.00 CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE July 7, 2023 SIGNATURE OF ATTORNEY OF RECORD /s/ Kevin Laukaitis

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

DEIDRA CLAY, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

MONDELEZ GLOBAL LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiff Deidra Clay (“Plaintiff”) brings this class action against Defendant Mondelez Global LLC (“Defendant”) for its failure to properly secure and safeguard Plaintiff’s and Class Members’ protected health information and personally identifiable information stored within Defendant’s information network.

INTRODUCTION

1. Defendant is a multinational food, snack, beverage, and confectionery company.
2. Defendant acquired, collected, and stored Plaintiff’s and Class Members’ PHI/PII and/or financial information.
3. At all relevant times, Defendant knew or should have known, that Plaintiff and Class Members would use Defendant’s services to store and/or share sensitive data, including highly confidential PHI/PII.
4. On no later than February 23, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff’s and Class Members’ PHI/PII and

financial information as hosted with Defendant, with the intent of engaging in the misuse of the PII and financial information, including marketing and selling Plaintiff's and Class Members' PHI/PII.

5. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is at least 50,000.

6. Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"), which may include test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

7. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

8. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendant's information network, includes, without limitation, Social Security numbers, first and last names, addresses, dates of birth, marital status, gender, employee identification numbers, and Mondelez retirement and/or health plan information.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow

applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

10. As a result, the PHI/PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

13. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

14. Defendant is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

15. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part

of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant does business in this Judicial District.

THE PARTIES

Plaintiff Deidra Clay

16. Plaintiff Deidra Clay is an adult individual and, at all relevant times herein, a resident and citizen of Ohio, residing in Greenfield, Ohio. Plaintiff is a victim of the Data Breach.

17. Plaintiff was an employee of Defendant's, and their information was stored with Defendant as a result of their dealings with Defendant.

18. As required in order to obtain employment from Defendant, Plaintiff provided Defendant with highly sensitive personal, financial, health, and insurance information, who then possessed and controlled it.

19. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

20. At all times herein relevant, Plaintiff is and was a member of each of the Classes.

21. Plaintiff received a letter from Defendant, dated June 15, 2023, stating that their PHI/PII and/or financial information was involved in the Data Breach (the "Notice").

22. Plaintiff was unaware of the Data Breach—or even that Defendant had possession of their data until receiving that letter.

23. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring

and identity theft insurance options; time spent self-monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

24. Plaintiff was also injured by the material risk to future harm she suffers based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers and healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

25. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

26. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PHI/PII and/or financial information.

27. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII and financial information, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

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

Defendant Mondelez Global LLC

29. Defendant Mondelez Global LLC, is a limited liability corporation headquartered at 905 West Fulton Market, Ste 200, Chicago, IL 60607.

30. Defendant has only one member, who, upon information and belief, is a resident and citizen of Illinois.

31. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

32. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following classes/subclass(es) (collectively, the “Class”):

Nationwide Class:

All individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant on February 23, 2023.

Ohio Subclass:

All individuals within the State of Ohio whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach experienced by Defendant on February 23, 2023.

34. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely

election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

35. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

36. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

37. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Plaintiff Classes (which Plaintiff is informed and believes, and on that basis, alleges that the total number of persons is in the hundreds of thousands of individuals and can be determined analysis of Defendant's records) are so numerous that joinder of all members is impractical, if not impossible.

38. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

- a. Whether Defendant had a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PHI/PII;
- b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

- c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;
- e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;
- g. How and when Defendant actually learned of the Data Breach;
- h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Plaintiff and Class Members;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and
- l. Whether Plaintiff and Class Members are entitled to restitution as a

result of Defendant's wrongful conduct.

39. Typicality: Plaintiff's claims are typical of the claims of the Plaintiff Classes. Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

40. Adequacy of Representation: Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

41. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Plaintiff anticipates no management difficulties in this litigation.

42. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

43. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

44. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

45. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

46. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PHI/PII and/or financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

COMMON FACTUAL ALLEGATIONS

Defendant's Failed Response to the Breach

48. Not until after months it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII and/or financial information Defendant confirmed was potentially compromised as a result of the Data Breach.

49. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's

recommended next steps, and Defendant's claims that it had learned of the Data Breach on 05/22/2023, and completed a review thereafter.

50. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII and financial information with the intent of engaging in the misuse of the PHI/PII and financial information, including marketing and selling Plaintiff's and Class Members' PHI/PII.

51. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

52. Plaintiff and Class Members were required to provide their PHI/PII and financial information to Defendant in order to obtain employment, and a condition of employment, Defendant created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

53. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PHI/PII and financial information going forward.

54. Plaintiff and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

55. Unauthorized individuals can now easily access the PHI/PII and/or financial information of Plaintiff and Class Members.

Defendant Collected/Stored Class Members' PHI/PII and Financial Information

56. Defendant acquired, collected, and stored and assured reasonable security over Plaintiff's and Class Members' PHI/PII and financial information.

57. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PHI/PII and financial information.

58. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

59. By obtaining, collecting, and storing Plaintiff's and Class Members' PHI/PII and financial information, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PHI/PII and financial information from unauthorized disclosure.

60. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII and financial information.

61. Plaintiff and Class Members relied on Defendant to keep their PHI/PII and financial information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

62. Defendant could have prevented the Data Breach, which began no later than February 23, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PHI/PII and financial information.

63. Defendant's negligence in safeguarding Plaintiff's and Class Members' PHI/PII and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

64. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PHI/PII and financial information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

65. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties it owes Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Members' data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

66. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

67. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable

Health Information establishes national standards for protecting health information.

68. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

69. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

70. "Electronic protected health information" is "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

71. HIPAA's Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

72. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that

maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

73. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following the discovery of the breach.”

74. Defendant was also prohibited by the Federal Trade Commission Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.”¹

75. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII and financial information in Defendant’s possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

76. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII and financial information of Plaintiff and Class Members.

77. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PHI/PII and financial information was adequately secured and protected.

78. Defendant owed a duty to Plaintiff and Class Members to create and implement

¹ The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

reasonable data security practices and procedures to protect the PHI/PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

79. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

80. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

81. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendant.

82. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

83. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PHI/PII and financial information and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

84. PHI/PII and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

85. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from \$40 to \$200, and bank

details have a price range of \$50 to \$200²; Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web³; and other sources report that criminals can also purchase access to entire company data breaches from \$999 to \$4,995.⁴

86. Identity thieves can use PHI/PII and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with another’s picture, using the victim’s information to obtain government benefits, or filing a fraudulent tax return using the victim’s information to obtain a fraudulent refund.

87. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information is stolen and when it is used: according to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁵

² *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 7, 2023).

³ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed July 7, 2023).

⁴ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 7, 2023).

⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf> (last accessed July 7, 2023).

88. Here, Defendant knew of the importance of safeguarding PHI/PII and financial information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PHI/PII and financial information were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

89. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

90. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PHI/PII and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLAIMS FOR RELIEF

COUNT ONE

Negligence

(On behalf of the Nationwide Class and the Ohio Subclass)

91. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

92. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and financial information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PHI/PII and financial information of Plaintiff and Class Members in its computer systems and on its networks.

93. Among these duties, Defendant was expected:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII and financial information in its possession;
- b. to protect Plaintiff's and Class Members' PHI/PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;
- c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and
- d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII and financial information.

94. Defendant knew that the PHI/PII and financial information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

95. Defendant knew, or should have known, of the risks inherent in collecting and storing PHI/PII and financial information, the vulnerabilities of its data security systems, and

the importance of adequate security.

96. Defendant knew about numerous, well-publicized data breaches.

97. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI/PII and financial information.

98. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII and financial information that Plaintiff and Class Members had entrusted to it.

99. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI/PII and financial information.

100. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII and financial information contained therein.

101. Plaintiff's and Class Members' willingness to entrust Defendant with their PHI/PII and financial information was predicated on the understanding that Defendant would take adequate security precautions.

102. Moreover, only Defendant had the ability to protect its systems and the PHI/PII and financial information is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

103. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PHI/PII and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining

Class Members.

104. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII and financial information of Plaintiff and Class Members;
- b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI/PII and financial information had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard the PHI/PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII and financial information;
- d. by failing to provide adequate supervision and oversight of the PHI/PII and financial information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII and financial information of Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.
- e. by failing to adequately train its employees not to store PHI/PII and financial information longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI/PII and financial information;

- g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and
- h. by failing to encrypt Plaintiff's and Class Members' PHI/PII and financial information and monitor user behavior and activity in order to identify possible threats.

105. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

106. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

107. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII and financial information to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII and financial information.

108. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

109. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

110. Further, through its failure to provide timely and clear notification of the Data

Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and financial information, and to access their medical records and histories.

111. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI/PII and financial information of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

112. Plaintiff's and Class Members' PHI/PII and financial information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII and financial information by adopting, implementing, and maintaining appropriate security measures.

113. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

114. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

115. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII and financial information is used; (iii) the compromise, publication, and/or theft of their PHI/PII and financial information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII and financial information; (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 embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PHI/PII and financial information, which may 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 Plaintiff's and Class Members' PHI/PII and financial information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

116. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

117. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII and financial information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII and financial information in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Nationwide Class and the Ohio Subclass)

118. Plaintiff realleges and reincorporates every allegation set forth in the preceding

paragraphs as though fully set forth herein.

119. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII and financial information.

120. Defendant required Plaintiff and Class Members to provide and entrust their PHI/PII and financial information as a condition of obtaining Defendant's services.

121. Defendant solicited and invited Plaintiff and Class Members to provide their PHI/PII and financial information as part of Defendant's regular business practices.

122. Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII and financial information to Defendant.

123. As a condition of being direct patients of clients of Defendant, Plaintiff and Class Members provided and entrusted their PHI/PII and financial information to Defendant.

124. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

125. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI/PII and financial information to Defendant, in exchange for, amongst other things, the protection of their PHI/PII and financial information.

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

127. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to

provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

128. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class and the Ohio Subclass)

129. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

130. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

131. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

132. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew, or should have known, of the

security vulnerabilities of the systems that were exploited in the Data Breach.

133. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Nationwide Class and the Ohio Subclass)

134. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

135. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

136. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PHI/PII and financial information to Defendant for the purpose of obtaining health services, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PHI/PII and financial information secure.

137. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI/PII and financial information kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

138. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

139. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

140. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed purchasing and health care decision and took undue advantage of Plaintiff and Class Members.

141. Defendant was unjustly enriched at the expense of Plaintiff and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

142. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

143. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and each member of the proposed National Class and the Ohio Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel

as Class Counsel;

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

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

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

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- c. requiring Defendant to delete and purge the PHI/PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- d. requiring Defendant to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PHI/PII;

- e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;
- f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PHI/PII on a cloud-based database;
- g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiff and Class Members;
- j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and
 - l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.
- 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
 - 7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and
 - 8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: July 7, 2023

Respectfully submitted,

By: /s/ Kevin Laukaitis
Kevin Laukaitis
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Attorneys for Plaintiff(s) and the Plaintiff
Class(es)

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

IN RE: MONDELEZ DATA
BREACH LITIGATION

Master File No. 1:23-CV-03999

**CONSOLIDATED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

This Document Relates To: All Actions

Plaintiffs Michael Shields, Daniel Berndt, Augustyn Wiacek, Deidra Clay, and Julio Perez (“Plaintiffs”) bring this Consolidated Class Action Complaint (“Complaint”) against Mondelēz Global LLC (“Mondelēz” or “Defendant”), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels’ investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this Complaint against Mondelēz for its failure to properly secure and safeguard the personally identifiable information—that it collected, maintained, and disclosed to its outside counsel as part of its regular business practices—including, but not limited to: full names; dates of birth; Social Security numbers; addresses, marital status, gender, and employment information (collectively, “personally identifiable information” or “PII”).

2. Mondelēz is a food retailer that operates in “more than 150 countries[,]” and markets a variety of food products—including for Oreo, Honey Maid, Ritz, and many more brands.¹

¹ *Our Brands*, MONDELÉZ INTERNATIONAL, <https://www.mondelezinternational.com/Our-Brands> (last accessed Aug. 30, 2023).

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the data breach (“Data Breach”) experienced by Mondelēz’s outside counsel.

4. Mondelēz collected and maintained certain personally identifiable information of Plaintiffs and the putative Class Members (defined below), who are (or were) employees at Mondelēz. Pursuant to Mondelēz’s business, Mondelēz shared that PII with its outside counsel who, in turn, stored that information, unencrypted, on its inadequately secured system.

5. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves. Defendant betrayed its obligations to Plaintiffs and the other Class Members by failing to properly safeguard and protect their PII and thereby enabling cybercriminals to steal such valuable and sensitive information.

6. As a result of the Data Breach, Plaintiffs and tens of thousands of Class Members, suffered concrete injuries in fact including, but not limited to: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) damage to their credit scores; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant’s possession and/or control and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

7. The Data Breach was a direct result of Defendant's failure to ensure that adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' PII were in place to protect against a foreseeable and preventable cyber-attack.

8. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on computer networks in conditions vulnerable to cyberattacks. It was negligent of Defendant to provide Plaintiff's and Class Members' PII and to a third-party who lacked adequate security. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

9. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that data systems containing Plaintiffs' and Class Members' PII were protected against unauthorized intrusions; failing to disclose that they did not ensure that adequately robust computer systems and security practices were used to safeguard Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct. As a result of Defendant's negligence, the PII that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud (including the fraud suffered by Plaintiffs described below), and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class

Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

15. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

16. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to the relevant data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

17. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct.

PARTIES

Plaintiff Michael Shields

18. Plaintiff Michael Shields is and has been at all relevant times a resident and citizen of Warminster, Pennsylvania where he intends to remain. Mr. Shields received the Notice Letter, via U.S. mail, directly from Defendant, dated June 15, 2023.

Plaintiff Daniel Berndt

19. Plaintiff Daniel Berndt is and has been at all relevant times a resident and citizen of Illinois where he intends to remain. Mr. Berndt received the Notice Letter from Defendant, sometime shortly after June 15, 2023.

Plaintiff Augustyn Wiacek

20. Plaintiff Augustyn Wiacek is and has been at all relevant times a resident and citizen of New York where he intends to remain. Mr. Wiacek received the Notice Letter from Defendant, on June 21, 2023.

Plaintiff Deidra Clay

21. Plaintiff Deidra Clay is and has been at all relevant times a resident and citizen of Greenfield, Ohio where she intends to remain. Ms. Clay received the Notice Letter from Defendant, dated June 15, 2023.

Plaintiff Julio Perez

22. Plaintiff Julio Perez is and has been at all relevant times a resident and citizen of Texas where he intends to remain. Mr. Perez received the Notice Letter, via U.S. mail, directly from Defendant, on or about June 15, 2023.

Defendant Mondelēz

23. Defendant is a food retailer limited liability company incorporated under the state laws of Delaware with its principal place of business located at 905 West Fulton Market, Suite 200, Chicago, Illinois 60607.

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

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

JURISDICTION AND VENUE

26. 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 at least one member of the class, including several Plaintiffs, are citizens of a state different from Defendant.

27. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, regularly conducts business in Illinois, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

28. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

29. Mondelez is a food retailer that operates in “more than 150 countries[,]” and markets a variety of food products—including for Oreo, Honey Maid, Ritz, and many more brands.²

30. Upon information and belief, in the course of collecting PII from employees, including Plaintiffs, Defendant promised to ensure that confidentiality and adequate security would be provided for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

31. Indeed, Defendant’s Privacy Policy provides that: “[p]rotecting your personal information is important to us. We maintain 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.”³

32. Plaintiffs and the Class Members, as former and current employees of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII are involved. Among other things, Plaintiffs and Class Members reasonably expected that Defendant would not

² *Our Brands*, MONDELÉZ INTERNATIONAL, <https://www.mondelezinternational.com/Our-Brands> (last accessed Aug. 30, 2023).

³ *Privacy Policy*, MONDELÉZ INTERNATIONAL, as it appeared on February 22, 2023 <https://web.archive.org/web/20230222155233/https://www.mondelezinternational.com/Privacy-Policy#otnotice-section-0b809480-5293-4d75-ae1-8c4afd2a12ca> (last accessed Sept. 11, 2023).

provide their sensitive PII and to a third-party who lacked adequate data security measures and practices.

33. In the course of their employment relationship, employees, including Plaintiffs and Class Members, provided Defendant with at least the following PII:

- a. names;
- b. dates of birth;
- c. gender;
- d. Social Security numbers; and
- e. addresses.

34. Defendant had a duty to ensure that reasonable measures were taken to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

35. In the Notice of Data Breach letter (the "Notice Letter") sent to Plaintiffs and Class Members, Defendant asserts that "[o]n February 27, 2023, [Defendant's outside counsel] detected unauthorized access to its systems[.]"⁴ Defendant subsequently investigated the unauthorized access to the relevant systems, and as a result of that investigation, concluded that the unauthorized access "occurred from February 23, 2023 until March 1, 2023."⁵ The investigation further determined that, through this successful infiltration, unauthorized cybercriminals "acquired certain data," including the PII of 51,100 current and former employees of Defendant.⁶

36. Omitted from the Notice Letter were any explanation of why it took Defendant several days after detecting the Data Breach to stop the unauthorized access, the details of the root

⁴ *Data Breach Notifications*, MAINE ATTY GEN., <https://apps.web.maine.gov/online/aewiewer/ME/40/ca25f29f-db60-4baf-ba53-8bae79da4d97.shtml> (last accessed Aug. 30, 2023).

⁵ *Id.*

⁶ *Id.*

cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

37. Upon information and belief, the cyberattack was targeted at Defendant via its outside counsel, due to Defendant's status as an employer that collects, creates, and maintains PII on various computer networks and/or systems.

38. Upon information and belief, Plaintiffs' and Class Members' PII was, in fact, involved in the Data Breach.

39. The files, containing Plaintiffs' and Class Members' PII and stolen from Defendant via its outside counsel, included the following: names, addresses, dates of birth, Social Security numbers, marital status, gender, and employment information.⁷

40. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant via its outside counsel that included the PII of Plaintiffs and Class Members.

41. As evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls, the PII of Plaintiffs and Class Members was not encrypted while stored on the network, and Defendant stored PII on the network for longer than was necessary to effect the purpose of sharing the PII.

42. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' PII, did not have sufficiently effective endpoint detection.

⁷ *Id.*

43. Further, the fact that PII was acquired in the Data Breach demonstrates that the PII contained in the infiltrated network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

44. Plaintiffs' PII was accessed and stolen in the Data Breach and Plaintiffs now reasonably believe that their stolen PII is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

45. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiffs and Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant" and to review and monitor their financial accounts for many years to mitigate the risk of identity theft.⁸ The Notice Letter also encourages Plaintiffs and Class Members to change their passwords and to temporarily freeze their credit.⁹ The Notice Letter additionally warns Plaintiffs and Class Members to on guard for potential "schemes."¹⁰

46. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

47. That Defendant is encouraging its current and former employees to enroll in credit monitoring and identity theft restoration services and is warning Plaintiffs to be on guard for data

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

misuse, is an acknowledgment that the impacted individuals' PII *was* accessed, thereby subjecting Plaintiffs and Class Members to a substantial and imminent threat of fraud and identity theft.

48. Defendant had obligations created by contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

49. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

50. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

51. The unencrypted PII of Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

52. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of tens of thousands of current and former employees and employee applicants, including Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members

53. Defendant has historically acquired, collected, shared, and stored the PII of Plaintiffs and Class Members.

54. As a condition of employment, or as a condition of receiving certain benefits, Defendant requires that its employees, former employees, and other personnel entrust it with highly sensitive personal information.

55. By obtaining, collecting, using, and sharing with outside counsel Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

56. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

57. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk because Employers in Possession of PII are Particularly Susceptible to Cyber Attacks

58. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store other medical information, like Defendant, preceding the date of the breach.

59. Data breaches, including those perpetrated against employers that store PII in their systems, have become widespread.

60. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.

61. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("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, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”

62. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

63. Defendant knew and understood that unprotected or exposed PII in the custody and/or control of employers, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

64. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if the relevant data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

66. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

67. The ramifications of Defendant’s failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

68. As a business in custody of current and former employees’ PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if the relevant data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

69. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹¹ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹²

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹³ For example, Personal Information can be sold at a price ranging from \$40 to \$200,

¹¹ 17 C.F.R. § 248.201 (2013).

¹² *Id.*

¹³ *Your personal data is for sale on the dark web. Here’s how much it costs*, DIGITAL TRENDS, (Oct. 16, 2019) <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

and bank details have a price range of \$50 to \$200.¹⁴ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁵

71. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use It to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁶

72. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

¹⁴ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, (Dec. 6, 2017) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

¹⁵ *In the Dark*, VPNOVERVIEW, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Aug. 30, 2023).

¹⁶ *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Aug. 30, 2023).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁷

74. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is immutable, i.e., impossible to “close” and difficult, if not impossible, to change—Social Security number, name, and date of birth.

75. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁸

76. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

77. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

¹⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>.

¹⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁹

Defendant Failed to Comply with FTC Guidelines and Stored Plaintiffs' PII on a Network that Failed to Comply with FTC Guidelines

78. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

80. The FTC further recommends that companies not maintain PII 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.

¹⁹ Report to Congressional Requesters, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

81. The FTC has brought enforcement actions against employers for failing to protect employee data adequately and reasonably, 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.

82. These FTC enforcement actions include actions against employers over the compromised PII of its employees, like Defendant here.

83. Defendant failed to delete PII that was no longer necessary to maintain and failed to encrypt data that it shared and/or stored on third party networks.

84. Defendant failed to limit its sharing of PII on third party networks to only the time period necessary to effect the transaction.

85. Defendant failed to ensure that Plaintiffs’ and Class Members’ sensitive PII was stored in a network with basic data security practices.

86. Defendant’s failure to ensure that reasonable and appropriate measures were in place to protect against unauthorized access to employees’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

87. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiffs’ PII Was Stored on Network that Fails to Comply with Industry Standards

88. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

89. Several best practices have been identified that at minimum should be implemented by employers in possession and/or control of PII, like Defendant, including but not limited to ensuring that PII is stored on networks with: strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

90. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. The infiltrated network, that Defendant allowed to store Plaintiffs' PII, failed to implement these cybersecurity best practices, including failure to train staff.

91. The infiltrated network, that Defendant allowed to store Plaintiffs' PII, further failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to confirm that, or even inquire whether, the network storing its employees' sensitive complied with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES AND DAMAGES

93. As a result of Defendant's negligence and the inadequate data security practices that existed on the breached IT network, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession and/or control of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Plaintiffs' and Class Member's Risk of Identity Theft

94. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

95. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

96. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

98. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.²⁰

²⁰ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>.

99. With “Fullz” packages, 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.

100. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ 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 that was exfiltrated in the Data Breach, criminals may still 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.

101. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

102. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

103. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

104. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud.

Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

105. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant’s Notice Letter instructs them, “remain vigilant” and monitor their financial accounts for many years to mitigate the risk of identity theft and fraud.

106. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as signing up for credit monitoring and identity theft insurance, closing and opening new credit cards, and securing their financial accounts.

107. Plaintiffs’ mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²¹

108. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

109. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches

²¹ See United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>

(“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²²

Diminution of Value of PII

110. PII is a valuable property right.²³ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

111. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.²⁴

112. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.²⁵ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.²⁶ Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.²⁷

²² See United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf> (“GAO Report”).

²³ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

²⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

²⁵ David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019) <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

²⁶ *Home Page*, DATACOUPE, <https://datacoup.com/> (last accessed Aug. 30, 2023).

²⁷ *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last accessed Aug. 30, 2023).

113. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

114. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., Social Security numbers and names.

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

116. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if the relevant data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

118. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it allowed to be stored on a vulnerable network, amounting to potentially

tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

119. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to protect the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

120. Given the type of targeted attack in this case and sophisticated criminal activity, and the type of PII involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

121. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

122. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.²⁸ The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

²⁸ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

123. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

124. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss of Benefit of the Bargain

125. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When accepting employment from Defendant under certain terms, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Shield's Experiences

126. Plaintiff Shields was employed at Mondelēz from approximately 2009 to 2012. As a condition of his employment at Mondelēz, he was required to provide his PII to Defendant.

127. At the time of the Data Breach—from February 23, 2023, through March 1, 2023—Defendant retained Plaintiffs' PII in the systems that would be the subject of the Data Breach, despite the fact that Plaintiffs had not been employed with Defendant for over a decade.

128. Plaintiff Shields is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

129. Plaintiff Shields received the Notice Letter, by U.S. mail, directly from Defendant, dated June 15, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff's name, address, date of birth, Social Security number, gender, marital status, and employment information.

130. Because of the Data Breach, Plaintiff's PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

131. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his personal information, reviewing his financial statements for accuracy, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Mondelēz specifically directed him to take these actions. Indeed, the letter stated: "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."²⁹

²⁹ See *Notification of a Potential Data Security Incident*, DEP'T JUST. NEW HAMPSHIRE (June 15, 2023) <https://www.doj.nh.gov/consumer/security-breaches/documents/mondelez-global-20230615.pdf>.

132. 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 that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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; and (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.

Plaintiff Berndt's Experiences

133. Plaintiff Berndt is a former employee of Defendant Mondelēz. As a condition of his employment at Mondelēz, he was required to provide his PII to Defendant.

134. At the time of the Data Breach—from February 23, 2023, through March 1, 2023—Defendant retained Plaintiffs' PII in the systems that would be the subject of the Data Breach, despite the fact that Plaintiffs had not been employed with Defendant for some time.

135. Plaintiff Berndt is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

136. Plaintiff Berndt received the Notice Letter from Defendant, sometime shortly after June 15, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained

by unauthorized third parties. This sensitive information included Plaintiff's name, address, date of birth, Social Security number, gender, marital status, and employment information.

137. Because of the Data Breach, Plaintiff's PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

138. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his personal information, reviewing his financial statements for accuracy, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Mondelēz specifically directed him to take these actions. Indeed, the letter stated: "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."³⁰

139. 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 that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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

³⁰ *See id.*

and adequate data security and failing to protect Plaintiff's PII; and (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.

Plaintiff Wiacek's Experiences

140. Plaintiff Wiacek is a former employee of Defendant Mondelēz. As a condition of his employment at Mondelēz, he was required to provide his PII to Defendant.

141. At the time of the Data Breach—from February 23, 2023, through March 1, 2023—Defendant retained Plaintiffs' PII in the relevant systems, despite the fact that Plaintiffs had not been employed with Defendant for some time. Specifically, Plaintiff Wiacek worked for Mondelēz from July 1994 to July 2021.

142. Plaintiff Wiacek is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

143. Plaintiff Wiacek received the Notice Letter, by U.S. mail, directly from Defendant, on June 21, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff's name, address, date of birth, Social Security number, gender, marital status, and employment information.

144. Because of the Data Breach, Plaintiff's PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

145. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the breach online,

changing usernames and passwords for financial and other accounts (including those for his wife and kids), enrolling in credit monitoring, continuously monitoring his accounts, and receiving alerts from credit monitoring agencies in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Mondelēz specifically directed him to take these actions. Indeed, the letter stated: “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.”³¹

146. 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 that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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; and (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.

Plaintiff Clay’s Experiences

³¹ *See id.*

147. Plaintiff Clay was employed by Mondelēz in 2013. And as a condition of her employment, Mondelēz required that she disclose her PII.

148. At the time of the Data Breach—from February 23, 2023, through March 1, 2023—Defendant retained Plaintiff's PII in the relevant systems, despite the fact that Plaintiff had not been employed with Defendant for approximately a decade.

149. Plaintiff Clay is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

150. Plaintiff Clay received the Notice Letter from Defendant, dated June 15, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff's name, address, date of birth, Social Security number, gender, marital status, and employment information.

151. Because of the Data Breach, Plaintiff's PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

152. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, checking in once or twice monthly for any updates from Mondelēz or other available information, monitoring her personal information, reviewing her financial statements for accuracy, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. Plaintiff Clay has spent an average of 30–40 minutes a week since her receipt of the Data Breach notice ensuring that no fraudulent transactions have been made with her bank and no fraudulent credit applications have been made in her name.

153. The letter Plaintiff received from Mondelēz specifically directed her to take these actions. Indeed, the letter stated: “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.”³²

154. 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 that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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; and (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.

Plaintiff Perez’s Experiences

155. Plaintiff Perez was employed by Mondelēz from approximately 2008 to 2013. As a condition of his employment at Mondelēz, he was required to provide his PII to Defendant.

³² *See id.*

156. At the time of the Data Breach—from February 23, 2023, through March 1, 2023—Defendant retained Plaintiffs’ PII in the relevant systems, despite the fact that Plaintiffs had not been employed with Defendant for approximately a decade.

157. Plaintiff Perez is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

158. Plaintiff Perez received the Notice Letter, by U.S. mail, directly from Defendant, on or about June 15, 2023. According to the Notice Letter, Plaintiff’s PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff’s name, address, date of birth, Social Security number, gender, marital status, and employment information.

159. Because of the Data Breach, Plaintiff’s PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

160. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his personal information and credit score, reviewing his financial statements for accuracy, and monitoring his social security account for illicit activity, all in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Mondelēz specifically directed him to take these actions. Indeed, the letter stated: “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.”³³

161. 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 that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (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; and (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.

162. As a result of the Data Breach, and at the direction of Defendant’s Notice Letter, all Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: signing up for credit monitoring and identity theft insurance, closing and opening new credit cards, and securing their financial accounts. All Plaintiffs have spent significant time dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

³³ *See id.*

163. The Data Breach has caused all Plaintiffs to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

164. As a result of the Data Breach, all Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, all Plaintiffs are at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

165. All Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession and/or control, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

166. This action is properly maintainable as a class action. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated.

167. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant in June 2023 (the "Class").

168. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

169. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 51,000 individuals were notified by

Defendant of the Data Breach, according to the breach report submitted to Maine's Attorney General's Office.³⁴ The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

170. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

³⁴ *Data Breach Notifications*, MAINE ATTY GEN., <https://apps.web.maine.gov/online/aevviewer/ME/40/ca25f29f-db60-4baf-ba53-8bae79da4d97.shtml> (last accessed Aug. 30, 2023).

- h. 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;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and
- k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

171. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

172. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

173. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the

Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

174. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

175. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

176. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

177. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

178. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

179. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

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

181. Defendant required Plaintiffs and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

182. Plaintiffs and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

183. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable

means to secure and safeguard Class Members' PII—and the computer protected that held it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of the relevant security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

184. Defendant had a duty to ensure that the networks storing Plaintiffs' PII utilized reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

185. Section 5 of the FTC Act, as interpreted and enforced by the FTC, prohibits the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect 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 sensitive PII.

186. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

187. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against employers, which, as a result of failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm to its employees as that suffered by Plaintiffs and members of the Class.

188. Defendant's conduct constitutes negligence because the network that it allowed to store Plaintiffs' PII was in violation of Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards.

189. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

190. 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.

191. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of the relevant networks and systems;
- c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' PII; and,
- e. Failing to detect in a timely manner that Class Members' PII had been compromised.

192. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the food retailer industry.

193. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

194. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiffs and the Class.

195. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) damage to their credit scores; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and/or control and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

196. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

197. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) replace or strengthen the relevant data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

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

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

199. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

200. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by, inter alia, not ensuring that the network it allowed to stored Plaintiffs’ PII complied with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on the relevant systems.

201. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

202. Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

203. Moreover, the harm that has occurred is the type of harm that the FTC Act intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

204. But for Defendant’s wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

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

206. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) damage to their credit scores; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and/or control and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

207. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

209. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

210. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

211. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) replace or strengthen the relevant data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

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

213. Plaintiffs bring this claim for unjust enrichment in the alternative to Count IV (breach of implied contract).

214. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of their labor and by providing their valuable PII to Defendant.

215. Plaintiffs and Class Members provided Defendant their labor and PII on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such PII held by Defendant.

216. Defendant benefited from receiving Plaintiffs' and Class Members' labor and from receiving their PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

217. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

218. Because all PII provided by Plaintiffs and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it collected from its employees was inherent to the employment relationship.

219. Defendant also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

220. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiffs and Class Members.

221. Defendant enriched itself by saving the costs it reasonably should have expended to ensure that data security measures were in place on the networks that stored Plaintiffs' PII to secure Plaintiff' and Class Members' PII.

222. Plaintiffs and Class Members suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

223. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to protect Plaintiffs' PII and failed to ensure that Plaintiffs' PII was stored on systems that utilized basic security measures, including those mandated by industry standards.

224. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

225. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

226. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

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

228. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury as described herein.

229. Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

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

231. This count is pleaded in the alternative to Count III (Unjust Enrichment) above.

232. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant.

233. Plaintiffs and Class Members provided their labor and their PII to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure and to delete it once it was no longer necessary to maintain the PII for employment purposes.

234. Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

235. On information and belief, Defendant further promised to and represented it would comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

236. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

237. When Plaintiffs and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

238. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

239. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

240. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

241. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor the computer systems and networks that store Plaintiffs' PII to ensure that they adopted reasonable data security measures.

242. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

243. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

244. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

245. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

246. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

247. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) replace or strengthen the relevant data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

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

249. Plaintiffs 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.

250. Defendant owed a duty to Plaintiffs and Class Member to ensure that their PII was kept confidential. As such, Defendant cannot abandon its duty when it shares that PII to its outside counsel.

251. Defendant affirmatively and recklessly disclosed Plaintiffs' and Class Members' PII to unauthorized third parties via Defendant's failure to ensure proper data security.

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

253. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' 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.

254. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew the relevant information security practices were inadequate.

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

256. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that the relevant inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

257. As a proximate result of Defendant's acts and omissions, Plaintiffs' 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 Plaintiffs and the Class to suffer damages.

258. Defendant’s wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still within Defendant’s custody and/or control—but are subject to inadequate cybersecurity systems and policies.

259. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant’s continued possession and/or control of their sensitive and confidential records. A judgment for monetary damages will not end Defendant’s inability to safeguard Plaintiffs’ and the Class’s PII.

260. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs’ and Class Members’ PII.

261. Plaintiffs, on behalf of themselves and Class Members, seek 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 VII

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

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

263. 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).

264. Defendant engaged in “trade” or “commerce,” including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). And pursuant to Defendant’s “trade” or “commerce,” Defendant disclosed Plaintiffs and Class Members’ PII to its outside counsel.

Moreover, Defendant engages in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

265. 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 and/or ensure that adequate data security was used—including by Defendant’s outside counsel—as 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 to Plaintiffs and the Class regarding the 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 to Plaintiffs 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 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 personal information from further unauthorized disclosure, release, data breaches, and theft.

266. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about the 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.

267. Defendant intended that Plaintiffs 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.

268. 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.

269. 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 Personal Information Protection Act, 815 ILCS 530/1, *et seq.*

270. As a result of Defendant's wrongful conduct, Plaintiffs 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 and/or ensure sufficient security as to keep their PII from being hacked and taken and misused by others.

271. 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/or control 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/or control; 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.

272. 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying

- information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on the relevant systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring Defendant to audit, test, and train security personnel regarding any new or modified procedures;
 - ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of the relevant networks are compromised, hackers cannot gain access to other portions of the relevant systems;
 - x. requiring Defendant to conduct regular database scanning and securing checks;
 - xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with

- additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and the relevant systems for protecting personal identifying information;
 - xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor the relevant information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from the relevant servers; and
 - xvii. for a period of 10 years, appointing a qualified and independent third-party

assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Date: September 14, 2023

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Tel.: (866) 252-0878

Email: gklinger@milberg.com

A. Brooke Murphy*

MURPHY LAW FIRM

4116 Will Rogers Pkwy, Suite 700

Oklahoma City, Oklahoma 73108

(405) 389-4989

abm@murphylegalfirm.com

Raina C. Borrelli

Samuel J. Strauss

Brittany Resch

TURKE & STRAUSS LLP

613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com

Interim Co-Lead Class Counsel

LAUKAITIS LAW LLC

Kevin Laukaitis
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Daniel Srourian
(CA S.B. #285678)
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, CA 90010
Telephone: (213) 474-3800
Email: daniel@slfla.com

*Additional Counsel for Plaintiffs and the
Putative Class*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 14, 2023 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Gary M. Klinger

Gary M. Klinger