IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LILYBETH DURAN individually and on behalf of all others similarly situated, Plaintiff, v. **JP MORGAN CHASE & CO.** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Lilybeth Duran ("Duran") individually and on behalf of all others similarly situated, brings this action against JP Morgan Chase & Co. ("JP Morgan"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold the Defendant responsible for the injuries the Defendant inflicted on Plaintiff and tens of thousands of similarly situated persons ("Class Members") due to the Defendant's impermissibly inadequate and unlawful data security, which caused the personal information of Plaintiff and those similarly situated to be viewed by unauthorized personnel between August 26, 2021 and February 23, 2024 (the "Data Breach").

2. Defendant JP Morgan operates a multinational finance company. It provides global financial services, such as investment banking, treasury and securities services, asset management,

private banking, card member services, commercial banking, home finance and retail banking. JP Morgan serves business enterprises, institutions, and individuals.[1]

3. The Data Breach affected 451,809 individuals.[2] The data, which the Defendant permitted its unauthorized personnel to review, were highly sensitive. The breached data included personal identifying information ("PII") such as: first and last names, Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account).[3]

4. Upon information and belief, prior to and through the date of the Data Breach, the Defendant obtained Plaintiff's and Class Members' PII and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, the Defendant inadequately and unlawfully maintained its network, platform, software—rendering these easy prey for its own unauthorized employees, who may then resell such data to cybercriminals.

5. Upon information and belief, the risk of the Data Breach was known to the Defendant. Thus, the Defendant was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

6. Then, after the Data Breach, Defendant failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, Defendant deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Defendant impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

---

[1] Bloomberg. "JP Morgan Chase & Co", https://www.bloomberg.com/profile/company/JPM:US (last accessed May 6, 2024).
[2] Office of Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/8ef595ed-6e79-4c9e-b722-74c2efa04511.shtml (
[3] *Id.*

7. Even when Defendant finally notified Plaintiff and Class Members that their PII was accessed by unauthorized personnel, Defendant failed to adequately describe the Data Breach and its effects, as well as the measures it took to prevent data breaches from occurring in the future.

8. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of Defendant's negligence. Plaintiff and Class Members now suffer from a present and continuing risk of fraud and identity theft and must now constantly monitor their financial accounts.

9. Armed with the PII accessed in the Data Breach, criminals can commit a boundless litany of financial crimes. Specifically, and without limitation, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

12. Through this action, Plaintiff seeks to remedy these injuries on behalf of herself and all similarly situated individuals whose PII was compromised in the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and the appointment of an independent and qualified cyber auditor to monitor Defendant's cyber hygiene, all of which will be funded by Defendant.

PARTIES

14. Plaintiff Duran is a natural person and resident and citizen of Gwinnett County, Georgia. Duran was a member of an employee-sponsored retirement fund, for which Defendant served as a payment agent, between 2016 and 2024. On or about April 18, 2024, Duran received a letter informing her of the Data Breach ("Data Breach Notification"), as described more fully below.

15. Defendant JP Morgan is a Delaware corporation with its headquarters and principal place of business located in New York City, New York.[4]

JURISDICTION AND VENUE

16. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than that of Defendant JP Morgan.

[4] Florida Division of Corporations, https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResults?InquiryType=EntityName&InquiryDirectionType=PreviousRecord&SearchTerm=JP%20Morgan%20Chase&SearchNameOrder=JPMORGANCHASEBANKNA%20Q170000000400&ListNameOrder=JPMORGANCHASE%20F020000062890&Detail=FL.DOS.Corporations.Shared.Contracts.FilingRecord (last accessed on May 6, 2024).

17. This Court has personal jurisdiction over Defendant JP Morgan, because JP Morgan maintains its principal place of business in this district.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District and JP Morgan maintains its principal place of business in the jurisdiction.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the PII of Plaintiff and Class Members

19. Defendant provides banking services to individuals and corporations, in person and online, throughout the United States and abroad. Among other services, Defendant provides benefit payment services to group pension plan participants.

20. Upon information and belief, Defendant received and maintained PII of group pension plan participants, such as individuals' names, addresses, dates of birth, and Social Security numbers. These records are stored on Defendant's computer systems.

21. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

22. Defendant acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

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

24. On its website, Defendant states:[5]

> We work hard to protect your information.
> We take our responsibility to protect the privacy and confidentiality of your information, including personal information, very seriously. We maintain physical, electronic and procedural safeguards that comply with applicable legal standards to secure such information from unauthorized access and use, accidental or unlawful alteration and destruction, and other unlawful or unauthorized forms of Processing. **We hold our employees accountable for complying with relevant policies, procedures, rules and regulations concerning the privacy and confidentiality of information**. (Emphasis added.)

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

26. Upon information and belief, Plaintiff and 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.

27. Defendant could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, and regulating and logging access to client PII.

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

[5] JP Morgan, "Privacy Policy", https://www.jpmorgan.com/privacy (last accessed on May 6, 2024).

29. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

30. Defendant failed to properly select its information security partners.

31. Defendant failed to ensure the proper monitoring and logging of employee access to PII.

32. Defendant failed to ensure the proper monitoring and logging of file access and modifications.

33. Defendant failed to ensure the proper training its own and its technology partners' employees as to cybersecurity best practices.

34. Defendant failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

35. Defendant failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

36. Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

37. Defendant failed to provide adequate supervision and oversight of the PII 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 PII of Plaintiff and Class Members, misuse the PII and disclose it to others without consent.

38. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions, such as unauthorized access which occurred in this case.

39. Upon information and belief, Defendant failed to monitor user behavior and activity to identify possible threats.

The Data Breach

40. On or about April 18, 2024, Defendant mailed the Data Breach Notification letter to its former and current clients, containing, among other the following statements:[6]

> **Here's what happened and what information was involved**
> • On February 26, 2024, we learned of a software issue that caused certain reports run by three authorized system users to include plan participant information that they were not entitled to see, including yours.
> • The three users were employed by J.P. Morgan customers or their agents.
> • The system users ran a limited number of reports between August 26, 2021 and February 23, 2024.
> • The reports included your name, address, Social Security number, payment and deduction amounts, as well as bank routing and account number if you set up direct deposit.
>
> **What we are doing**
> • We promptly addressed the access issue and have applied a software update.

41. Defendant offered inadequate suggestions regarding remedies Class Members could utilize to prevent identity theft:

> **What you can do**
> • It is always a good practice to regularly review your accounts and monthly statements. If you identify any transactions you do not recognize, call the number on your statement or the back of your credit or debit card.
> • You may consider placing a security freeze on your credit report(s).
> • While we have no indication that your information has been misused, we suggest that you accept the attached offer of two years of free credit monitoring through Experian's® IdentityWorks®. This helps alert you to changes to your credit bureau information.
> • Please see the enclosed important information describing the benefits, how to enroll and the additional steps you can take to help protect yourself.

42. Defendant was untimely and unreasonably delayed in providing notice of the Data Breach to Plaintiff and Class Members.

[6] Maine Attorney General, "Data Breach Notifications", https://apps.web.maine.gov/online/aeviewer/ME/40/8ef595ed-6e79-4c9e-b722-74c2efa04511.shtml (last visited on May 6, 2024).

43. In the Data Breach Notification, Defendant offered "two years of free credit monitoring through Experian's® IdentityWorks®," for 12 months. This offer, made by Defendant, is woefully inadequate given that risks of identity theft do not expire within two years, and continue for a lifetime.

44. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

45. In sum, Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

46. Defendant did not provide any additional details about the attack.

47. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[7]

[7] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, *https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed May 7, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

48. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[8] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[9] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

49. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

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

51. Aside from the offer of two years of credit monitoring services, which is inadequate for reasons described above, Defendant has offered no measures to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for the rest of their lifetimes .

[8] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed May 7, 2024).
[9] *Id.*

52. Defendant had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

53. Plaintiff and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was exposed and reviewed by Defendant's unauthorized employees, beyond several categories listed in the letter as "included" in the Data Breach, and what steps are being taken, if any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

54. Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

Defendant Failed to Comply with FTC Guidelines

55. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[10] To that end, the FTC has issued numerous

[10] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed May 6, 2024).

guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against unauthorized access to customer PII.

56. 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.[11] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

57. 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.

58. The FTC 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.[12]

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

[11] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed May 6, 2024).

[12] *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 7, 2024).

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

Defendant Failed to Comply with The Gramm-Leach Bliley Act

61. Defendant is a financial institution, as that term is defined in s. 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §6809(3)(A).

62. Regulations, enacted pursuant to 15 U.S.C. §6801(b) and codified at 16 CFR §314.3 and §314.4, mandate that financial institutions develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the

financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.

63. Among other regulations, the Safeguards Rule mandates financial institutions to develop safeguards to control the risks [they] identity through risk assessment, including by:

> (1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:
>
> > (i) **Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information**; and
> >
> > (ii) **Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information**;
>
> (2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;
>
> (3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;
>
> (4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
>
> (5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;
>
> (6)
>
> > (i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be

> retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and
>
> (ii) Periodically review your data retention policy to minimize the unnecessary retention of data;
>
> (7) Adopt procedures for change management; and
>
> (8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users. (Emphasis added).

64. Defendant failed to comply with the Safeguard Rule, and in particular, failed to limit access to Plaintiff's and Class Members' PII only to authorized personnel that required such access as part of their job function, leading to the losses suffered by Plaintiff and the Class Members.

Defendant Failed to Follow Industry Standards

65. Despite its alleged commitments to securing sensitive data, Defendant does not follow industry standard practices in securing PII.

66. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to data breach, because of the value of the PII which they collect and maintain.

67. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendant, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and *most importantly in the present case*, limiting which employees can access sensitive data.

68. Other best cybersecurity practices that are standard in the financial service industry

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.

69. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. Such frameworks are the existing and applicable industry standards in the financial service industry. Defendant failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiff and Class Members

71. Plaintiff and Class Members are members of pension or benefit plans which plans retained Defendant as the benefit payments agent.

72. As a prerequisite of obtaining benefits payments from pension or retirement plans which retained the Defendant as a payment agent, Defendant required Plaintiff and Class Members to disclose their PII.

73. When Defendant finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's Data Breach Notice fails to explain how the breach occurred (what "software issue" was exploited by its unauthorized

employees), what exact data elements of each affected individual were compromised, and the extent to which those data elements were compromised.

74. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

75. All Class Members were injured when Defendant caused their PII was accessed by unauthorized employees.

76. Plaintiff and Class Members entrusted their PII to Defendant. Thus, Plaintiff had the reasonable expectation and understanding that Defendant would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. Plaintiff and Class Members would not have entrusted their PII to Defendant had they known that Defendant would not take reasonable steps to safeguard their information from unauthorized access by its employees.

77. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Data Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

78. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

79. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to Defendant.

80. The ramifications of Defendant's failure to keep Plaintiff's and the Class Members' PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

81. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[13]

82. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members 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;

[13]Anne Saita, "Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on May 7, 2024).

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 their PII; and

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

83. 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.[14]

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

85. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

[14] Brian Stack, "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/ (last visited on May 7, 2024).

86. One such example of criminals using PII for profit is the development of "Fullz" packages.[15]

87. 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.

88. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's 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 other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

[15] "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 can be made off 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/tag/fullz/ (last visited on May 7, 2024).

89. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

90. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

91. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

92. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

93. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

94. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated

that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[16]

95. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[17] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) **limiting administrative access to business systems**; (5) using industry-tested and accepted methods for securing data; (6) **monitoring activity on networks to uncover unapproved activity**; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[18]

96. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[19] The FTC treats 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(a) of the FTC Act (the "FTCA").

97. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services,*

---

[16] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on May 7, 2024).

[17] "Start With Security, A Guide for Business," FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 7, 2024).

[18] *Id.*

[19] "Taking Charge, What to Do If Your Identity is Stolen," U.S. DEPARTMENT OF JUSTICE, at 3 (January 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited on May 7, 2024).

Inc., No. C-4326, Complaint ¶ 7 (June 15, 2011) ("[Respondent] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Respondent] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Respondent] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

98. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

99. Charged with handling highly sensitive PII including, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that

would be imposed on Defendant's customers as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

100. Defendant's use of outdated and insecure computer systems and its failure to maintain adequate security measures and an up-to-date technology security strategy, which resulted in its employees gaining unauthorized access to Class Members' PII, demonstrates a willful and conscious disregard for privacy.

101. Defendant's failure to properly and promptly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed 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.

CLASS ACTION ALLEGATIONS

102. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

103. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons residing in the United States whose PII was impacted by the Data Breach at JP Morgan, between august 26, 2021 and February 23, 2024.

104. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

105. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling

interest, and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

106. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

107. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

108. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of hundreds of thousands of individuals who reside in the U.S. and were or are enrolled in retirement or benefit plans serviced by JP Morgan as a benefits payment agent for its corporate clients, and whose PII was compromised by the Data Breach.

109. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If 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;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII;

f. If Defendant breached its duty to Class Members to safeguard their PII;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant failed to provide notice of the Data Breach in a timely manner;

k. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

m. If Defendant's conduct was negligent;

n. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

o. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

p. If Defendant breached implied contracts with Plaintiff and Class Members;

q. If Defendant was unjustly enriched as a result of the Data Breach; and

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

110. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and all Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

111. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

112. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

113. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for

Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

114. 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.

115. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

116. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 109.

117. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

118. Plaintiff re-alleges and incorporates by reference paragraphs 1-117 of the Complaint as if fully set forth herein.

119. Defendant required its clients (i.e., pension or benefit plans) to submit Plaintiff's and Class Members' non-public PII to Defendant, to receive Defendant's services as a payment agent.

120. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from access by unauthorized personnel. Defendant's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

121. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable to Defendant. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals, including its own employees, would at some point try to access Defendant's databases of PII.

122. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

123. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its, or its service providers', systems and networks, and the personnel responsible for them, adequately protected the PII.

124. Defendant's duty of care to use reasonable security measures to restrict unauthorized user access arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common

law. Defendant was in a superior position to ensure that its own, and its service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

125. Defendant failed to take appropriate measures to protect the PII of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the financial services industry. Any purported safeguards that Defendant had in place were wholly inadequate.

126. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII.

127. Defendant was negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiff's and Class Members' PII.

128. Under the FTCA, Defendant had a duty to employ reasonable security measures. Specifically, this statute 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.[20]

129. Moreover, Plaintiff's and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, 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 very same injuries that Defendant inflicted upon Plaintiff and Class Members.

[20] 15 U.S.C. § 45.

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

131. As stated above, among other regulations, the Safeguards Rule promulgated under the GLBA, mandates financial institutions to develop safeguards to control the risks [they] identity through risk assessment of their computer networks.

132. Defendant's failure to comply with FTCA and GLBA statutory duties and standards of conduct constitutes negligence. Defendant's failure to comply with the requisite standard of care caused the Breach, exposing Plaintiff's and Class Members' PII to cybercriminals and causing Plaintiff and Class Members pecuniary and non-pecuniary harm detailed herein.

133. But for Defendant's wrongful and negligent breach of its duties to Plaintiff and the Class, Plaintiff's and Class Members' PII would not have been compromised, accessed, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

134. Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members 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 in an effort to mitigate the fallout of the Data Breach.

135. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or

should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the PII of Plaintiff and Class Members.

136. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA, GLBA and their respective regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

137. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. 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.

138. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew or should have known that its systems and technologies for processing and securing the PII of Plaintiff and the Class had security vulnerabilities.

139. As a result of Defendant's negligence, the PII and other sensitive information of Plaintiff and Class Members was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Class Members.

140. Simply put, Defendant's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

141. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

142. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of ten years.

SECOND CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of the Plaintiff and the Class)

143. Plaintiff re-alleges and incorporates by reference paragraphs 1-117 of the Complaint as if fully set forth herein.

144. Defendant entered into written contracts with its clients to provide payments agent services for their retirement or benefit plans.

145. These contracts included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' PII.

146. These contracts were made expressly for the benefit of Plaintiff and Class Members, as intended third party beneficiaries of the contracts entered between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, its clients' employees—Plaintiffs and Class Members—would be harmed.

147. Defendant's clients fully performed their obligations under their contracts with Defendant.

148. However, Defendant did not secure, safeguard, and/or keep private Plaintiff's and Class Members' PII. Defendant allowed unauthorized employees to access Plaintiff's and Class Members' PII without permission. Therefore, Defendant breached its contracts with Plaintiff and Class Members.

149. As a result of the breach of contracts between Defendant and its clients, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

150. Plaintiff and Class Members, as third party beneficiaries of the contracts between Defendant and its clients, are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

151. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of ten years.

THIRD CAUSE OF ACTION
Implied Contract
(On Behalf of the Plaintiff and the Class)

152. Plaintiff re-alleges and incorporates by reference paragraphs 1-117 of the Complaint as if fully set forth herein.

153. This claim is pleaded in the alternative to the Second Cause of Action, above.

154. Plaintiff and Class Members were required to deliver their PII to Defendant as part of the process of obtaining financial services from Defendant.

155. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

156. Defendant accepted possession of Plaintiff's and Class Members' PII, for the ostensible purpose of contracting with Plaintiff and Class Members.

157. Plaintiff and Class Members entrusted their PII to Defendant. 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 Class Members if their data had been breached and compromised or stolen.

158. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and

regulations (including FTC guidelines on data security and GLBA regulations) and were consistent with industry standards.

159. Implicit in the agreement between Plaintiff 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 access to, or disclosures of, the PII**, (d) provide Plaintiff 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 Plaintiff and Class Members from unauthorized disclosure or uses**, (f) retain the PII only under conditions that kept such information secure and confidential.

160. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

161. As discussed above, the Defendant's privacy policy promised Plaintiff and Class Members that it would safeguard their PII in a reasonably secure fashion.

162. Plaintiff and Class Members paid money to the Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

163. Plaintiff 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.

164. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

165. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant. Defendant, on the other hand, breached its obligations under the implied contracts with Plaintiff and Class Members by failing to safeguard their PII and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

166. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) theft of their PII; (ii) lost or diminished value of PII; (iii) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) 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 is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its 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 for a lifetime.

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

169. Plaintiff re-alleges and incorporates by reference paragraphs 1-117 of the Complaint as if fully set forth herein.

170. This Claim is pleaded in the alternative to Second and Third Causes of Action, above.

171. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members, through their pension or benefit funds.

172. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

173. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, through their contributions to pension or benefit plans, which plans in turn retained Defendant as a payment agent, Plaintiff and Class Members purchased goods and services from Defendant, and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

174. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

175. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII, including measures that would have monitored and restricted unauthorized employee access to such PII.

Instead of providing a reasonable level of security that would have prevented the hacking incident, 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 security.

176. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

177. Defendant failed to secure Plaintiff's and Class Members' PII, and prevent unauthorized employee access to it, and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

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

179. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

180. Plaintiff and Class Members have no adequate remedy at law.

181. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (g) 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.

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

183. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representatives, and the undersigned as Class Counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, 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 business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the 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;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. 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 PII, as well as protecting the PII of Plaintiff and Class Members;

vi. 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 systems for protecting PII;

vii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, including unauthorized employee access, and assess whether monitoring tools are

properly configured, tested, and updated; and

viii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of unauthorized employee access to their PII, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. A mandatory injunction requiring the Defendant to fund the appointment of an independent and qualified cyber auditor to monitor Defendant's cyber hygiene;

E. A mandatory injunction requiring Defendant to purchase credit monitoring and identity theft protection services for each Class Member for ten years;

F. An injunction enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the PII that was subject to unauthorized access;

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

H. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

I. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

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

K. For all other Orders, findings, and determinations identified and sought in this Complaint; and

L. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury for any and all issues in this action so triable as of right.

Dated: May 7, 2024

Respectfully Submitted,

/s/ Jonathan M. Sedgh

Jonathan M. Sedgh
New York Bar No. 4557260
JSedgh@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
350 Fifth Avenue, Suite 6705
New York, NY 10118
Telephone: (212) 738-6299

Ronald Podolny
NY Bar: 4772232
ronald.podolny@forthepeople.com
John A. Yanchunis*
JYanchunis@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

John G. Emerson*
jemerson@emersonfirm.com
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042-2754
Tel. 800.551.8649
Fx. 501.286.4659

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class