THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

CONCETTA C. VERDERAME on behalf of herself and all others similarly situated **Plaintiff,** **v.** **FUTURITY FIRST INSURANCE GROUP, LLC,** **Defendant.**	**Case No.:** **COMPLAINT-CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff Concetta C. Verderame ("Plaintiff") brings this Class Action Complaint against Futurity First Insurance Group, LLC ("Futurity" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of potentially several thousand individuals and businesses, including, but not limited to, name, address, date of birth, gender, signature, social security number, federal/state identification numbers, financial account information, telephone and/or fax number, and driver's license or state identification number.

2. Founded in 2008, Futurity represents itself as a nationwide network of insurance agents and advisors offering a range of financial products, including life insurance and annuities,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

as well as healthcare planning and retirement planning services, based in Middletown, Connecticut.

3. Prior to and through November 24, 2023, Defendant stored the PII of Plaintiff and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

4. On or before May 23, 2024, Defendant learned of a data breach on its network that occurred on or around November 24, 2023 (the "Data Breach").

5. Defendant determined that, during the Data Breach, an unauthorized third party gained access to several employee and independent agent email accounts and subsequently accessed and/or acquired the PII of Plaintiff and Class Members.

6. On or around July 24, 2024, Defendant began notifying Plaintiff and Class Members of the Data Breach.

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that was accessed and/or acquired by an unauthorized actor included name, date of birth, driver's license number, federal/state identification card number, tax identification number, social security number and/or financial account information, and other information such as phone number, address, and email address.

8. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the un-encrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

9. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class Members' PII. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

10. Prior to receiving notification, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

11. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect Plaintiff's and Class Members' PII; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) 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) may remain 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.

13. 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' PII was safeguarded, failing to take available steps to prevent an 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. As a result, Plaintiff's and Class Members' PII were compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. On behalf of herself and the Class as defined herein, Plaintiff brings claims for negligence, breach of fiduciary duty, breach of confidence, breach of express contract, breach of implied contract, and, in the alternative to their contract-based claims, unjust enrichment. The remedies Plaintiff seeks include actual, nominal, and putative damages; appropriate injunctive and declaratory relief; and attorneys' fees, costs, and expenses.

II. JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of 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 to establish minimal diversity.

16. Defendant is a citizen of Connecticut with its principal place of business in Middletown, Connecticut.

17. The District of Connecticut has personal jurisdiction over Defendant because it conducts substantial business in Connecticut and this District and collected and/or stored the PII of Plaintiff and Class Members in this District.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiff and Class Members.

III. PARTIES

19. Plaintiff Concetta C. Verderame is now and has at all relevant times been a citizen of New Jersey, currently residing in Cinnaminson, New Jersey. Plaintiff Verderame received the letter notifying her of the breach, via email, directly from Defendant dated July 26, 2024.

20. Defendant Futurity First Insurance Group, LLC is a Delaware limited liability company, registered to conduct business in Connecticut, with a principal place of business at 101 Centerpoint Drive, Suite 208, Middletown, Connecticut, 06457-7568. Defendant provides financial security and income planning products for seniors, pre-retirees, families and businesses nationwide through a nationwide network of wealth advisors, investment specialists, and financial representatives.

21. 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 Plaintiff. Plaintiff 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.

22. All of Plaintiff's claims stated herein are asserted against Defendant and any of

its owners, predecessors, successors, subsidiaries, agents and/or assigns.

IV. FACTUAL ALLEGATIONS

Background

23. Defendant collected the PII of Plaintiff and Class Members and stored it, unencrypted, on Defendant's internet-accessible network.

24. Plaintiff and Class Members relied on this sophisticated 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. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

26. On or about July 24, 2024, Defendant sent Plaintiff and Class Members an emailed *Notice of Data Breach* [2] informing Plaintiff and other Class Members that:

> FFIG[3] recently completed an investigation of suspicious activity associated with three employee and six independent agent email accounts.1 The investigation determined that there was unauthorized access to the email accounts, but the investigation could not determine whether any emails or attachments in the accounts may have been accessed or acquired. Therefore, FFIG searched the contents of the email accounts, which took a substantial amount of time and effort, and, on May 23, 2024, FFIG determined that one or more emails or attachments contained the name and one or more of the following of three Maine residents: Social Security number, and/or driver's license number.
>
> On July 24, 2024, FFIG sent notifications via U.S. First-Class mail to the three Maine residents in accordance with Me. Rev. Stat. Tit. 10, §1348.2 A copy of the notification is enclosed. FFIG is offering one year of complimentary credit monitoring, fraud consultation, and identity theft restoration services through

[2] Exhibit 1 (Notice of Data Breach posted at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/963349ac-7a51-49dd-9536-c4545d308125.html).
[3] Futurity First Insurance Group

> Experian to these individuals, whose Social Security number or driver's license may have been involved.
>
> To reduce the risk of a similar incident from occurring in the future, FFIG has taken and will continue to take steps to enhance the security of its email environment.

27. Defendant admitted in the *Notice of Data Breach* that an unauthorized actor accessed sensitive information about Plaintiff and Class Members, including their names and social security numbers.

28. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

29. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

31. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

32. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

33. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[4]

34. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[5]

35. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

36. Private Information is a valuable property right.[6] The value of Private Information as a commodity is measurable.[7] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies are estimated to

---

[4] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Feb. 24, 2023).

[5] Facts + Statistics: Identity Theft and Cybercrime, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 27, 2023).

[6] See Marc Van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[7] Robert Lowes, Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[8] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring

have spent over $19 billion on acquiring personal data of consumers in 2018.[9] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for years afterwards.

37. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

38. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[10]

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

---

Monetary Value, OECD (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-andtechnology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[9] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[10] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware- mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Feb. 24, 2023).

as secondary forms of extortion."[11]

40. 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 has been sold or posted on the [Dark] 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."

41. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

42. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to

[11] U.S. CISA, Ransomware Guide–September 2020, available at https://www.cisa.gov/stopransomware/ransomware-guide (last visited April 21, 2023).

exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

43. The FTC recommends that identity theft 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 (and 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 freezes on their credit, and correcting their credit reports.

44. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

45. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

46. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a

substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

47. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[12]

48. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

49. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

50. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and

[12] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.guanotronic.com/~serge/papers/isr10.pdf.

published as the result of a cyberattack.

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

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

52. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

53. By obtaining, collecting, and storing Plaintiff's and Class Members' PII of, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

54. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and 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.

55. 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."[13]

56. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how

[13] 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 (last visited Feb. 24, 2023).

it is delivered.

b. 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.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. 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.

h. 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.

i. 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.

j. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

k. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

l. Execute operating system environments or specific programs in a virtualized environment.

m. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[14]

57. To prevent and detect ransomware attacks, including the ransomware attack 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;

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

[14] *Id*. at 3-4.

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].[15]

58. Given that Defendant was storing the PII of thousands of individuals, Defendant could and should have implemented all the above measures to prevent and detect ransomware attacks.

59. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of individuals, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

60. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing Plaintiff's and Class Members' PII. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable

[15] *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/ (last visited Feb. 24, 2023).

need to do so.

61. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

62. 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' PII from being compromised.

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] 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."[17]

64. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII 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.

Value of Personal Identifiable Information

65. 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. For example, personal information can be sold at a price ranging from $40 to

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id*.

$200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

66. 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.

67. 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."[21]

68. 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.

69. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[18] *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 Feb. 24, 2023).

[19] *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 Feb. 24, 2023).

[20] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 24, 2023.

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit CardNumbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 24, 2023).

70. 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 continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class Members' PII, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

72. Plaintiff 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.

73. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, 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.

74. To date, Defendant has offered Plaintiff and Class Members 12 months of complimentary credit monitoring and identify protection services through Experian IdentityWorks. The offered service is inadequate to protect Plaintiff and Class Members from the

[22] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 24, 2023).

threats they face for years to come, particularly in light of the PII at issue here.

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

Plaintiff's Experience

76. Plaintiff Verderame retained the services of a financial advisor in New Jersey who was part of Defendant's nationwide network of wealth advisors, investment specialists, and financial representatives. She provided her PII in connection with the financial advisor in order to establish an account and enable her financial advisor to provide investment advice and other services. She received Defendant's Notice of Data Breach, dated July 24, 2024, on or about that date.

77. As a result of the Data Breach, Plaintiff's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

78. 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* and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

79. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

80. Plaintiff stores any documents containing her sensitive PII in a safe and secure

location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

81. Despite her best efforts, Plaintiff has suffered numerous occurrences of fraudulent activity including fraudulent bank charges using her personal information that was taken from Defendant.

82. Defendant's data security shortcomings resulted in the Data Breach and caused Plaintiff significant injuries and harm in several ways. For example, Plaintiff has devoted and will continue to devote significant time, energy, and money to: closely monitoring her bills, records, and credit and financial accounts; changing login and password information on any sensitive account; carefully screening and scrutinizing phone calls, emails, and other communications to ensure that she is not being targeted by identity theft scams, medical identity theft scams, or other attempts at fraud; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect herself; and placing fraud alerts and/or credit freezes on their credit file. Plaintiff has taken or will be forced to take these measures to mitigate her potential damages because of the Data Breach.

83. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

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

V. CLASS ACTION ALLEGATIONS

85. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure and Local Rule 23.1.

86. The Class that Plaintiff seeks to represent is defined as follows:

> All persons in the United States and its territories whose PII was compromised in the Data Breach, including all individuals who received a data breach notification letter from Defendant. (the "Nationwide Class").

87. 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; any and all federal, state or local governments, including but not limited to their 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 their immediate family members.

88. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

89. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant reported that customer account information and transactions[23] was impacted in the Data Breach, and the Class is apparently identifiable within Defendant's records.

90. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class

[23] *See* https://www.securityweek.com/evolve-bank-data-leaked-after-lockbits-federal-reserve-hack/ (last visited June 28, 2024).

Members. These include *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' Private Information from unauthorized access and disclosure;

b. Whether Defendant's actions and its allegedly lax data security practices used to protect Plaintiff's and class members' PII violated the FTC Act and/or other state laws and/or Defendant's other duties alleged herein;

c. Whether Defendant 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 class members;

d. Whether Plaintiff and class members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

e. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and class members' PII;

f. Whether an implied contract existed between class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure class members' PII from unauthorized access and disclosure;

g. Whether an express contract existed between class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure class members' PII from unauthorized access and disclosure;

h. Whether Plaintiff and class members are intended third party beneficiaries of contracts between Defendant and third parties, and if so whether Defendant breached those contracts;

i. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and class members;

j. Whether Defendant's actions and inactions alleged herein constitute gross negligence;

k. Whether Defendant breached its duties to protect Plaintiff and class members' Private Information; and

l. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

91. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

92. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

93. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has 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 Class Members and making final injunctive relief appropriate with

respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff 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 Plaintiff.

94. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff received the notification of the data breach and has experienced actual damages as a result of the breach. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

95. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

96. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate

procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it 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 Plaintiff was 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.

97. 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.

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

99. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to class members' names and addresses affected by the Data Breach. Indeed, class members have already been preliminarily identified and sent notice of the Data Breach.

100. 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.

101. 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

Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

102. 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, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. 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;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or

nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

103. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

104. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

105. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

106. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

107. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

108. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

109. Defendant's duty to use reasonable security measures arose as a result of the

special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiff and the Nationwide Class's confidential PII in the course of its business practices.

110. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

111. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

112. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

113. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

114. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

115. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

116. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

117. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

118. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

119. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

120. Defendant improperly and inadequately safeguarded the PII of Plaintiff sand the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

121. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

122. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

123. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

124. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

125. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

126. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide 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.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of 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, tax fraud, 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; 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 PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

128. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide 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.

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

130. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

131. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

132. As part of its financial, investment, insurance and retirement services, Plaintiff and the Class provided and entrusted their PII to Defendant.

133. Defendant required Plaintiff and the Class to provide and entrust their PII as a condition of obtaining services from Defendant.

134. As a condition of receiving services from Defendant, Plaintiff and the Class provided and entrusted their PII. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and the Class if their PII had been compromised or stolen.

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

136. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

137. 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) the threat of the sharing and detrimental use of their confidential information; 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.

138. 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.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Class)

139. Plaintiff and the Nationwide Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

140. Plaintiff brings this claim individually and on behalf of the Class.

141. Plaintiff and class members have an interest, both equitable and legal, in their PII that was conveyed to, collected by, and maintained by Defendant and that was accessed or compromised in the Data Breach.

142. As a recipient of customers' PII, Defendant has a fiduciary relationship to its customers, including Plaintiff and the class members.

143. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class. Plaintiff and class members were entitled to expect their information would remain confidential while in Defendant's possession.

144. Defendant owed a fiduciary duty under common law to Plaintiff and class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

145. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and class members' financial records.

146. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiffs and class members, information not generally known.

147. Plaintiff and class members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

148. Defendant breached its fiduciary duties owed to Plaintiff and class members by, among other things:

a. mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its

patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

149. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and class members, their PII would not have been compromised.

150. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and class members have suffered injuries, including:

a. Theft of their PII; Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services; Lowered credit scores resulting from credit inquiries following fraudulent activities;

c. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

d. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard

Plaintiff's and class members' data against theft and not allow access and misuse of their data by others;

f. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and class members' data;

g. and Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and class members.

151. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Class)

152. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

153. Plaintiff brings this claim individually and on behalf of the Class.

154. Plaintiffs and class members have an interest, both equitable and legal, in their PII that was conveyed to, collected by, and maintained by Defendant and that was accessed or compromised in the Data Breach.

155. Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

156. Plaintiff and the Class provided Defendant with their personal and confidential PII under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PII.

157. Defendant owed a duty to Plaintiff and class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

158. Defendant had an obligation to maintain the confidentiality of Plaintiff's and class members' PII.

159. Plaintiff and class members have a privacy interest in their personal financial matters, and Defendant had a duty not to disclose confidential medical information and records concerning its customers.

160. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII and confidential financial records of Plaintiff and class members.

161. Plaintiff's and class members' PII is not generally known to the public and is confidential by nature.

162. Plaintiff and class members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

163. Defendant breached the duties of confidence it owed to Plaintiff and class members when Plaintiff's and Class Members' PII was disclosed to unknown criminal hackers.

164. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and class members' PII, including by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable

internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its on privacy policies and practices published to its customers;

h. storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and

i. making an unauthorized and unjustified disclosure and release of Plaintiffs and the class members' PII to a criminal third party.

165. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff and class members, their privacy, confidences, and PII would not have been compromised.

166. As a direct and proximate result of Defendant's breach of Plaintiff's and class members' confidences, Plaintiff and class members have suffered injuries, including:

a. Loss of their privacy and confidentiality in their PII;

b. Theft of their private information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their private information;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Futurity First Insurance Group, LLC Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their private information being placed in the hands of criminals;

h. Damages to and diminution in value of their private information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and class members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and class

members' data; and

j. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

167. Additionally, Defendant received payments from Plaintiff and class members for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiff's and class members' PII.

168. Defendant breached the confidence of Plaintiff and class members when it made an unauthorized release and disclosure of their confidential information and PII and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff's and class members' expense.

169. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiff and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

170. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

171. Plaintiff brings this claim individually and on behalf of the Class.

172. Plaintiff and class members had a reasonable expectation of privacy in the PII Defendant mishandled.

173. Defendant's conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

174. By intentionally failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members, which is highly offensive and objectionable to an ordinary person; and,

c. Intentionally causing anguish or suffering to Plaintiff and class members.

175. Defendant knew that an ordinary person in Plaintiff's or class members' position would consider Defendant's intentional actions highly offensive and objectionable.

176. Defendant invaded Plaintiff's and class members' right to privacy and intruded into Plaintiff's and class members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

177. Defendant intentionally concealed from and delayed reporting to Plaintiff and class members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

178. The conduct described above was at or directed at Plaintiff and class members.

179. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and

objectionable.

180. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

181. As a direct and proximate result of Defendant's conduct, Plaintiff and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VI
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiff and the Class)

182. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and all the other claims herein.

183. Plaintiff brings this claim individually and on behalf of the Class.

184. Defendant's privacy policy created an express contractual obligation to safeguard and protect the sensitive information of Plaintiff and class members.

185. Defendant breached this contractual duty by failing to adequately safeguard Plaintiff's and class members' PII, and by allowing it to be disseminated to unauthorized third parties.

186. Plaintiff and class members substantially performed their part of the bargain.

187. Defendant's breach of this contractual obligation in the privacy policy and elsewhere caused damages to Plaintiff and class members, as set forth herein.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

188. Plaintiff and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

189. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's contractual based claims pursuant to Fed. R. Civ. P. 8.

190. Upon information and belief, Defendant funds its data security measures utilizing payments made by or on behalf of Plaintiff and the class members.

191. 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.

192. Plaintiff and class members conferred a monetary benefit on Defendant. Specifically, they purchased financial services from Futurity and/or its agents 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 had their PII protected with adequate data security.

193. 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.

194. 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. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead elected 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.

195. 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 its common law and statutory duties.

196. Defendant failed to secure Plaintiff and class members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and class members provided.

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

198. 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.

199. Plaintiff and class members have no adequate remedy at law.

200. 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.

201. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and class members, proceeds that it 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.

COUNT VIII
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

202. Plaintiff and the Class reallege and incorporate by reference herein all the

preceding allegations above as if fully alleged herein.

203. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

204. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

205. Plaintiff and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff's and the Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet- accessible environment, including the Social Security number of Plaintiff.

206. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiff and the Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff's harm.

207. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any newor modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

208. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

209. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant

has a pre-existing legal obligation to employ such measures.

210. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent such 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 Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. 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:

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 its 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 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 the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff 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 Defendant's 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 its 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 Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's 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 Plaintiff 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 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;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's 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 personal identifying information 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 Defendant's servers; and 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, consequential, and nominal 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

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

Dated: July 29, 2024

Respectfully submitted,

Seth R. Lesser (Bar No.: CT 27068)
Klafter Lesser LLP
Two International Drive, Suite 350
Rye Brook, NY 10573
Telephone: 914 934 9200
Facsimile: 914 934 9220
Email: seth@klafterlesser.com

Marc H. Edelson
(*Pro Hac Vice* anticipated)
EDELSON LECHTZIN LLP

411 S. State Street, Suite N-300
Newtown, PA 18940
Telephone: (215) 867-2399
Facsimile: 267-685-0676
Email: medelson@edelson-law.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org
