UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE FIDELITY INVESTMENTS DATA BREACH LITIGATION	Lead Case No: 1:24-CV-12601-LTS
This Document Relates To: All Cases	JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Richard Mason, Alexander Elterman, Ratiek Lowery, Robert Wilbert, and John Nixon (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class," as defined below), bring this Consolidated Class Action Complaint against defendant FMR LLC d/b/a Fidelity Investments, and defendant Fidelity Brokerage Services LLC d/b/a Fidelity Investments (collectively, "Fidelity" or "Defendant"), based on personal knowledge and the investigation of counsel, and allege as follows:

I. INTRODUCTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. Fidelity is a financial services company that offers a wide range of products and services. Fidelity is one of the world's largest asset managers. In 2023, Fidelity generated over $28.2 billion in revenue. As of January 2025, it had $15 trillion in assets under administration and $5.8 trillion in discretionary assets.

3. As part of its business, and in order to gain profits, Defendant obtained and stored the personal information of Plaintiffs and members of the Class ("Class Members").

4. From the outset of each Class Member's receipt of financial investment services

from Fidelity, it represents and assures them that "Fidelity recognizes the importance of maintaining personal information about you and when we use it, we do so with respect for your privacy."[1]

5. In a further effort to assure customers that Fidelity is doing all that is necessary and required to protect the confidentiality of their personal information, Defendant purportedly adopted protocols and practices that it represents to customers are followed with respect to their private personal information (the "Privacy Policy").[2]

6. Fidelity represents in its Privacy Policy that it obtains and uses personal information to: service, maintain and protect its customers' accounts; process transactions in those accounts; respond to inquiries from customers or their representatives; develop, offer and deliver products or services; operate and manage its business; and fulfill legal and regulatory requirements. "Fidelity collects public and non-public personal information from customers and visitors from various sources."[3]

7. Fidelity states that it protects its customers' information by "implement[ing] and maintain[ing] physical, administrative, technical, and organizational measures ***designed to protect personal information***, and we regularly adapt these controls to respond to changing requirements and advances in technology. At Fidelity, we restrict access to personal information to those who require it to develop, support, offer, and deliver products and services and to operate our business." It further represents in its Privacy Policy that "[w]hen [customers] interact with us by using websites, online services or applications (including mobile apps) that are owned and

[1] *Privacy Policy,* FIDELITY INVESTMENTS, https://www.fidelity.com/privacy/policy (last accessed Feb. 3, 2025).
[2] *Id.*
[3] *Id.*

controlled by Fidelity Investments ('our digital offerings'), or via electronic communications, Fidelity manages personal information in accordance with all of the practices and safeguards described in this policy."[4]

8. By taking possession and control of Plaintiffs' and Class Members' personal information, Defendant assumed a duty to securely store and protect it.

9. Defendant breached this duty and betrayed the trust of Plaintiffs and Class Members by failing to properly safeguard and protect their personal information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

10. Between August 17, 2024 and August 19, 2024, Fidelity detected suspicious activity on its computer network, indicating a data breach (the "Data Breach"). Based on a subsequent forensic investigation, Fidelity determined that cybercriminals launched a targeted cybersecurity attack, infiltrated Defendant's inadequately secured computer systems, and thereby gained access to Defendant's data files. The investigation further determined that, through this infiltration, cybercriminals accessed, acquired, and compromised data files containing the sensitive personal information of 77,099 individuals.

11. The personally identifiable information accessed by cybercriminals included particularly sensitive and high-risk information such as Social Security numbers, financial account information, and driver's license information, accompanied by victims' names (collectively, "PII" or "Personal Information").

12. Despite identifying the Data Breach internally as early as August 19, 2024, Defendant waited almost two months before it began notifying consumers, commencing on or

[4] *Id.*

about October 9, 2024, that the Data Breach had occurred.

13. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiffs' and Class Members' Personal Information; timely detect the Data Breach; take adequate steps to prevent and stop the Data Breach; disclose the material fact that it did not have adequate security practices in place to safeguard the Personal Information; and provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiffs and Class Members across the United States.

14. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals for decades to come.

15. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its failure to use statutorily required or reasonable industry cybersecurity measures to protect Class Members' Personal Information.

16. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiffs and Class Members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiffs and Class Members are now forced to deal with the danger of identity thieves possessing and using their Personal Information. Indeed, at least some information stolen in the Data Breach has already been misused, and Plaintiffs have already suffered actual fraud and/or identity theft.

17. As detailed herein, since the Data Breach, Plaintiff Wilbert has experienced fraud on two of his financial accounts, a third party attempted to unlawfully access Plaintiff Nixon's PayPal account requiring him to shut down that account, and Plaintiff Elterman has experienced

unrecognized credit inquiries, causing a decrease in his credit score. Moreover, after the Data Breach, Plaintiffs Mason, Lowery, and Elterman were notified that their PII has been posted on the dark web.

18. Additionally, Plaintiffs and Class Members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

19. Plaintiffs bring this action individually and on behalf of the Class and seek actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court deems necessary and proper.

II. THE PARTIES

20. Plaintiff Richard Mason ("Mason") is a citizen and resident of the State of California.

21. Plaintiff Alexander Elterman ("Elterman") is a citizen and resident of the State of California.

22. Plaintiff Ratiek Lowery ("Lowery") is a citizen and resident of the State of New York.

23. Plaintiff Robert Wilbert ("Wilbert") is a citizen and resident of the State of Florida.

24. Plaintiff John Nixon ("Nixon") is a citizen and resident of the Commonwealth of Massachusetts.

25. Defendant FMR LLC is a limited liability company organized under the laws of the State of Delaware with its principal place of business located in Boston, Massachusetts. Upon

information and belief, each member of FMR LLC is domiciled in Massachusetts.[5]

26. Defendant Fidelity Brokerage Services LLC is a limited liability company organized under the laws of the State of Delaware with its principal place of business located in Boston, Massachusetts. Fidelity Brokerage Services LLC is a single member limited liability company and is a wholly-owned subsidiary of Defendant FMR LLC.[6]

III. JURISDICTION AND VENUE

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

28. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts with this Commonwealth.

29. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

---

[5] *See* information regarding FMR LLC on the Massachusetts Secretary of State website, available at: https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=O8ZscbRYNYnYy358PzDSrHbsiK_ju583pN_m6wCTuSw-.

[6] *Fidelity Brokerage Services LLC Statement of Financial Condition 2023*, United States Security and Exchange Commission, https://www.sec.gov/Archives/edgar/data/278082/000027808224000003/FBS2023SoFC.pdf).

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Belated Notice

30. Fidelity detected suspicious activity on its computer network, indicating a data breach. Based on a subsequent forensic investigation, Fidelity determined that cybercriminals infiltrated its inadequately secured computer systems and thereby gained access to its data files between August 17, 2024 and August 19, 2024. The investigation further determined that, through this infiltration, cybercriminals accessed and acquired files containing the sensitive personal information of 77,099 individuals.[7]

31. Fidelity was a soft target for cyber thieves who recognized that as a financial investment company it collects, maintains, and even creates PII. The cyber-attack by a third-party "***retrieved*** certain documents related to Fidelity customers and other individuals by submitting fraudulent requests to an internal database containing images of those documents."[8] Those imaged documents included, *inter alia*, the Personal Information of customers including Plaintiffs and Class Members.

32. The Personal Information accessed by cybercriminals included names, Social Security numbers, financial account information, and driver's license information.[9]

33. Despite the sensitivity of the PII that was exposed, and the attendant consequences to affected individuals as a result of the exposure, Defendant failed to disclose the Data Breach for nearly two months after the Data Breach. This inexplicable delay further exacerbated the harms to

---

[7] *See Data Breach Notifications: Fidelity Investments,* OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a4103ed8-3176-4ca0-99e6-4a320f1c3b32.html (last accessed Feb. 3, 2025).

[8] *Fidelity breach exposed the personal data of 77,000 customers - what to do if you're affected,* ZDNET, https://www.zdnet.com/article/fidelity-breach-exposed-personal-data-of-77000-customers-what-to-do-if-youre-affected/ (emphasis added) (last accessed Feb. 3, 2025).

[9] https://securityaffairs.com/169717/data-breach/fidelity-investments-data-breach.html (last accessed Feb. 3, 2025).

Plaintiffs and Class Members.

34. Based on the notice letter received by Plaintiffs, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Personal Information was stolen in the Data Breach.

35. Upon information and belief, the unauthorized third-party cybercriminal(s) gained access to the Personal Information, exfiltrated the Personal Information from Defendant's network, and engaged (and will continue to engage) in misuse of the Personal Information, including marketing and selling Plaintiffs' and Class Members' Personal Information on the dark web.

36. Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Personal Information confidential and to protect such Personal Information from unauthorized access.

37. Nevertheless, Defendant failed to spend sufficient resources on encrypting sensitive personal data, preventing external access, detecting outside infiltration, and training its employees to identify hacking threats and defend against them.

38. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that sensitive information was part of the data that was compromised.

39. Given the type of targeted attack in this case, the type of Personal Information accessed, and the fact that such information was successfully exfiltrated by cybercriminals, there is a strong probability that the unencrypted Personal Information of Plaintiffs and Class Members has been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Personal Information for identity theft crimes. In fact, Plaintiffs' Personal Information has already been posted on the dark web since the Data Breach.

40. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Personal Information for Plaintiffs and Class Members.

41. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

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

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

44. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including their PII, which includes information (such as Social Security numbers) that are static, do not change, and can be used to commit a myriad of financial crimes.

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

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

47. Because Defendant had a duty to protect Plaintiffs' and Class Members' Personal Information that it collected, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

48. Defendant breached its obligations to Plaintiffs and Class Members and was otherwise negligent and/or reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to properly monitor its own data security systems for existing intrusions;

c. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

d. Failing to train its employees in the proper handling of emails containing Personal Information and maintain adequate email security practices;

e. Failing to ensure the confidentiality and integrity of electronic Personal Information it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Personal Information to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity

regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Personal Information;

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules;

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PII as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of Personal Information;

l. Failing to render the electronic Personal Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Personal Information;

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

n. Failing to adhere to industry standards for cybersecurity; and

o. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Personal Information.

49. Defendant negligently and/or recklessly failed to safeguard Plaintiffs' and Class Members' Personal Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Personal Information.

50. Accordingly, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

B. Plaintiffs' Experiences

Plaintiff Mason's Experience

51. Plaintiff Mason's Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

52. Plaintiff Mason received a notice letter from Defendant dated October 9, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

53. Plaintiff Mason is very careful about sharing his sensitive information.

54. Plaintiff Mason stores any documents containing his Personal Information in a safe and secure location. Plaintiff Mason has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

55. Because of the Data Breach, Plaintiff Mason's Personal Information is now in the hands of cybercriminals.

56. Plaintiff Mason has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

57. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Mason is now imminently at risk of crippling future identity theft and fraud.

58. Since the Data Breach, Plaintiff Mason has experienced data misuse. Specifically, in September 2024, Plaintiff Mason received notifications that his Personal Information—including his Social Security number—had been located on the dark web. Plaintiff Mason attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his Personal Information, and the fact that he has

not experienced anything like this prior to now.

59. As a result of the Data Breach, Plaintiff Mason has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Mason has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, monitoring his credit monitoring reports, placing a credit alert with Equifax, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

60. The letter Plaintiff Mason received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff Mason and all Class Members advised: ". . . it is always a good idea to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to your financial institution (if applicable), local law enforcement, or your appropriate state authority."[10] In addition, the breach notification letter listed several "Additional Steps To Protect Yourself" that victims of the Data Breach should take to help protect themselves, including enrolling in credit monitoring, monitoring accounts, reviewing credit reports, and placing fraud alerts with credit reporting bureaus.[11]

[10] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a4103ed8-3176-4ca0-99e6-4a320f1c3b32.html.
[11] *Id.*

61. As a result of the Data Breach, Plaintiff Mason has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. In particular, Plaintiff Mason is worried about his Personal Information being placed on the dark web and fears that criminals will use his information to commit identity theft that causes him financial harm.

62. Plaintiff Mason anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

63. Plaintiff Mason has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Mason's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Mason's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Mason's Personal Information; and (e) continued risk to Plaintiff Mason's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Elterman's Experience

64. Plaintiff Elterman's Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

65. Plaintiff Elterman received a notice letter from Defendant dated October 9, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

66. Plaintiff Elterman is very careful about sharing his sensitive information.

67. Plaintiff Elterman stores any documents containing his Personal Information in a safe and secure location. Plaintiff Elterman has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

68. Because of the Data Breach, Plaintiff Elterman's Personal Information is now in the hands of cybercriminals.

69. Plaintiff Elterman has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

70. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Elterman is now imminently at risk of crippling future identity theft and fraud.

71. Since the Data Breach, Plaintiff Elterman has experienced identity theft in the form of unrecognized credit inquiries. As a result, Plaintiff Elterman has further experienced a decrease in his credit score since the Data Breach. In addition, in the months since the Data Breach, Plaintiff Elterman has been notified that his Personal Information is available on the dark web. Plaintiff Elterman attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his PII, and the fact that he has not recently experienced anything like this prior to now.

72. As a result of the Data Breach, Plaintiff Elterman has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the

future consequences of the Breach. Among other things, Plaintiff Elterman has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, placing a credit freeze and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

73. The letter Plaintiff Elterman received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: ". . . it is always a good idea to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to your financial institution (if applicable), local law enforcement, or your appropriate state authority."[12] In addition, the breach notification letter listed several "Additional Steps To Protect Yourself" that victims of the Data Breach should take to help protect themselves, including enrolling in credit monitoring, monitoring accounts, reviewing credit reports, and placing fraud alerts with credit reporting bureaus.[13]

74. As a result of the Data Breach, Plaintiff Elterman has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. In particular, Plaintiff Elterman is worried about his Personal Information being placed on the dark web and fears that criminals will use his information to commit identity theft that causes him financial harm.

[12] *Id.*
[13] *Id.*

75. Plaintiff Elterman anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

76. Plaintiff Elterman has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Elterman's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Elterman's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Elterman's Personal Information; and (e) continued risk to Plaintiff Elterman's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Wilbert's Experience

77. Plaintiff Wilbert's Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

78. Plaintiff Wilbert received a notice letter from Defendant dated October 9, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

79. Plaintiff Wilbert is very careful about sharing his sensitive information.

80. Plaintiff Wilbert stores any documents containing his Personal Information in a safe

and secure location. Plaintiff Wilbert has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

81. Because of the Data Breach, Plaintiff Wilbert's Personal Information is now in the hands of cybercriminals.

82. Plaintiff Wilbert has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

83. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Wilbert is now imminently at risk of crippling future identity theft and fraud.

84. Since the Data Breach, Plaintiff Wilbert has experienced identity theft in the form of fraudulent charges on two separate financial accounts in October 2024. Plaintiff Wilbert attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his Personal Information, and the fact that he has not recently experienced anything like this prior to now.

85. As a result of the Data Breach, Plaintiff Wilbert has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Wilbert has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

86. The letter Plaintiff Wilbert received from Defendant specifically directed him to

take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: ". . . it is always a good idea to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to your financial institution (if applicable), local law enforcement, or your appropriate state authority."[14] In addition, the breach notification letter listed several "Additional Steps To Protect Yourself" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, and placing fraud alerts with credit reporting bureaus.[15]

87. As a result of the Data Breach, Plaintiff Wilbert has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. In particular, Plaintiff Wilbert is worried about his Personal Information being placed on the dark web and fears that criminals will use his information to commit identity theft that causes him financial harm.

88. Plaintiff Wilbert anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

89. Plaintiff Wilbert has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Wilbert's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Wilbert's Personal Information that was entrusted to Defendant;

[14] *Id.*
[15] *Id.*

(d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Wilbert's Personal Information; and (e) continued risk to Plaintiff Wilbert's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Nixon's Experience

90. Plaintiff Nixon's Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

91. Plaintiff Nixon received a notice letter from Defendant dated October 9, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

92. Plaintiff Nixon is very careful about sharing his sensitive information.

93. Plaintiff Nixon stores any documents containing his Personal Information in a safe and secure location. Plaintiff Nixon has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

94. Because of the Data Breach, Plaintiff Nixon's Personal Information is now in the hands of cybercriminals.

95. Plaintiff Nixon has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

96. As a result of the Data Breach, which exposed highly valuable information such as

his Social Security number, Plaintiff Nixon is now imminently at risk of crippling future identity theft and fraud.

97. Since the Data Breach, Plaintiff Nixon has experienced data misuse in the form of someone trying to access his Paypal account, causing him to shut down the account. Plaintiff Nixon attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his Personal Information, and the fact that he has not recently experienced anything like this prior to now.

98. As a result of the Data Breach, Plaintiff Nixon has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Nixon has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

99. The letter Plaintiff Nixon received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: ". . . it is always a good idea to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to your financial institution (if applicable), local law enforcement, or your appropriate state authority."[16] In addition, the breach notification letter listed several "Additional Steps To Protect Yourself" that

[16] *Id.*

victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, and placing fraud alerts with credit reporting bureaus.[17]

100. As a result of the Data Breach, Plaintiff Nixon has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. In particular, Plaintiff Nixon is worried about his Personal Information being placed on the dark web and fears that criminals will use his information to commit identity theft that causes him financial harm.

101. Plaintiff Nixon anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

102. Plaintiff Nixon has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Nixon's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Nixon's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Nixon's Personal Information; and (e) continued risk to Plaintiff Nixon's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

[17] *Id.*

Plaintiff Lowery's Experience

103. Plaintiff Lowery's Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

104. Plaintiff Lowery received a notice letter from Defendant dated October 9, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

105. Plaintiff Lowery is very careful about sharing his sensitive information.

106. Plaintiff Lowery stores any documents containing his Personal Information in a safe and secure location. Plaintiff Lowery has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

107. Because of the Data Breach, Plaintiff Lowery's Personal Information is now in the hands of cybercriminals.

108. Plaintiff Lowery has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

109. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Lowery is now imminently at risk of crippling future identity theft and fraud.

110. Since the Data Breach, Plaintiff Lowery has received texts and emails containing links to fraudulent requests to collect money. Moreover, in October 2024, Plaintiff Lowery received notification that his Personal Information was posted on the dark web. Plaintiff Lowery attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his Personal Information, and the fact that he has

not recently experienced anything like this prior to now.

111. As a result of the Data Breach, Plaintiff Lowery has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Lowery has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

112. The letter Plaintiff Lowery received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: ". . . it is always a good idea to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to your financial institution (if applicable), local law enforcement, or your appropriate state authority."[18] In addition, the breach notification letter listed several "Additional Steps To Protect Yourself" that victims of the Data Breach should take to help protect themselves, including enrolling in credit monitoring, monitoring accounts, reviewing credit reports, and placing fraud alerts with credit reporting bureaus.[19]

113. As a result of the Data Breach, Plaintiff Lowery has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. In particular, Plaintiff Lowery is worried about his

[18] *Id.*
[19] *Id.*

Personal Information being placed on the dark web and fears that criminals will use his information to commit identity theft that causes him financial harm.

114. Plaintiff Lowery anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

115. Plaintiff Lowery has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Lowery's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Lowery's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Lowery's Personal Information; and (e) continued risk to Plaintiff Lowery's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

C. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

116. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

117. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class Members' Personal Information.

118. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer and application systems to ensure the Personal Information in its possession was adequately secured and protected.

119. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

120. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach on its systems in a timely manner.

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

122. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information to Defendant.

123. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when data breaches occurred.

124. Defendant owed a duty of care to Plaintiffs and Class Members because it was a foreseeable victim of a data breach.

D. The Data Breach Was a Foreseeable Risk of which Defendant Was on Notice

125. Because Defendant had a duty to protect Plaintiffs' and Class Members' Personal Information, Defendant should have known through readily available and accessible information

about potential threats for the unauthorized exfiltration and misuse of such information.

126. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[20] Yahoo,[21] Marriott International,[22] Chipotle, Chili's, Arby's,[23] and others.[24]

127. 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.

128. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[25]

129. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[26]

---

[20] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last accessed Feb. 3, 2025).

[21] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last accessed Feb. 3, 2025).

[22] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last accessed Feb. 3, 2025).

[23] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last accessed Feb. 5, 2025).

[24] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last accessed Feb. 3, 2025).

[25] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified (last accessed Feb. 3, 2025).

[26] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (Jan. 25, 2023), available at:

130. 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."[27]

131. 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 as secondary forms of extortion."[28]

132. 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 companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

133. In fact, Fidelity was on specific and direct notice of the risk of data breaches

---

https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report (last accessed Feb. 3, 2025).

[27] 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 accessed Feb. 3, 2025).

[28] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last accessed Feb. 3, 2025).

because, approximately 10 months before the Data Breach at issue, Fidelity Investments Life Insurance Company, an affiliate of Fidelity, experienced a data breach through one of its vendors.[29] That data breach, in December 2023, exposed the sensitive personal information of approximately 1.3 million people.

134. Considering the information readily available (and specifically known to Fidelity, based on the data breach it had recently experienced) before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted Personal Information of Plaintiffs and Class Members in an internet-accessible environment, had reason to be on guard for the exfiltration of the Personal Information. Defendant's type of business also gave it cause to be particularly on guard against such an attack.

135. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Personal Information could be accessed, exfiltrated, and published as the result of a cyberattack.

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

137. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

E. The Data Breach Was Preventable

138. By obtaining, collecting, and storing the Personal Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known

[29] *See* https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/0c98c6d7-c7b3-4bbf-a7fa-8005c61168d6/67b5a0c4-e819-4aa7-b43b-f7e5f9d9fde6/Sample%20Notice.pdf (last accessed Feb. 3, 2025).

that it was responsible for protecting the Personal Information from disclosure.

139. 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."[30]

140. 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:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using

[30] *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 accessed Feb. 3, 2025).

Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[31]

141. 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 Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your Personal Information safe.** Check a website's security to ensure

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

the information you submit is encrypted before you provide it. . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[32]

142. 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 privilege credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full comprise

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

[32] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed Feb. 3, 2025).

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].[33]

143. Given that Defendant was storing the Personal Information of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

144. 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 Personal Information of Plaintiffs and Class Members.

145. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the Personal Information of Plaintiffs and Class Members. 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 need to do so.

146. Defendant's negligence in safeguarding the Personal Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data. Moreover, as alleged above, this was not Fidelity's first data breach. It

[33] *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 accessed Feb. 3, 2025).

should have taken stronger and better steps to protect the Personal Information at issue to prevent yet another breach.

147. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiffs and Class Members from being compromised.

148. Defendant disregarded the rights of Plaintiffs and Class Members by recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Personal Information of Plaintiffs and Class Members 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, Plaintiffs' and Class Members' Personal Information was compromised through disclosure to an unknown and unauthorized criminal third party.

149. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Personal Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

150. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiffs and Class Members are long-lasting and severe. Once Personal Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

F. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal Information to Defraud Them or to Sell on the Dark Web

151. Plaintiffs and Class Members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

152. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[34] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[35] These criminal activities have resulted and will result in devastating financial and personal losses to Plaintiffs and Class Members.

153. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market

[34] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed Feb. 3, 2025).

[35] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed Feb. 3, 2025).

for years.[36]

154. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiffs' and the Class Members' Personal Information on the dark web. The Personal Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

155. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[37]

156. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

157. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[39]

158. With this Data Breach, identity thieves have already started to prey on the victims, including Plaintiffs, and one can reasonably anticipate this will continue.

---

[36] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last accessed Feb. 3, 2025).

[37] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last accessed Feb. 3, 2025).

[38] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last accessed Feb. 3, 2025).

[39] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last accessed Feb. 3, 2025).

159. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[40] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[41] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[42]

160. Based on the foregoing, the Personal Information compromised in the Data Breach, which includes Social Security numbers, 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.

161. 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."[43]

162. 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.

---

[40] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Feb. 3, 2025).
[41] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Feb. 3, 2025).
[42] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).
[44] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last accessed Feb. 3, 2025).

163. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.

164. Cyber-criminals can cross-reference two sources of Personal Information 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.

165. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class' 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.

166. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

167. Victims of the Data Breach, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[44]

168. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of

[44] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last accessed Feb. 3, 2025).

suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other personal accounts for unauthorized activity for years to come.

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

a. Trespass, damage to, and theft of their personal property, including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' Personal

Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

170. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class Members' Personal Information.

171. Plaintiffs and Class Members are trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives.

172. None of this should have happened. The Data Breach was preventable.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal Information

173. Data breaches are preventable.[45] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

[45]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012) (last accessed Feb. 3, 2025).

security solutions."[46] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[47]

174. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[48]

Defendant Failed to Adhere to FTC Guidelines

175. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Personal Information.

176. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[49] 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."[50]

177. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide

[46] *Id.* at 17.
[47] *Id.* at 28.
[48] *Id.*
[49] 17 C.F.R. § 248.201 (2013).
[50] *Id.*

for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. Protect the sensitive consumer information that they keep;

b. Properly dispose of PII that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

178. 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.

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

180. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

181. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class's Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

182. As shown above, experts studying cybersecurity routinely identify entities that collect sensitive information as being particularly vulnerable to cyberattacks because of the value of the Personal Information which they collect and maintain.

183. Several best practices have been identified that at a minimum should be implemented by large financial entities 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 limiting which employees can access sensitive data.

184. Other best cybersecurity practices that are considered industry-standard 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.

185. Defendant failed to meet the minimum standards of any of the following frameworks: NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

186. These foregoing frameworks are existing and applicable industry standards, particularly for large financial entities. Defendant, however, failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

187. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Personal Information from those risks left that information in a dangerous condition.

188. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*: (i) recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

189. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. The nationwide class is defined as follows:

> All persons residing in the United States whose Personal Information was compromised as a result of the Data Breach, including all persons who received a breach notification letter from Defendant ("Nationwide Class").

190. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), and (c)(4), as appropriate, Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state data breach and/or consumer protection statutes, on behalf of subclasses for residents of California, Florida, Massachusetts, and New York (collectively, "State Subclasses") (for purposes of this Section, the Nationwide Class and State Subclasses are referred to herein collectively ("Class")).

191. Each State Subclass is defined as follows:

California Subclass

All residents of California whose Personal Information was compromised as a result of the Data Breach, including all California residents who received a breach notification letter from Defendant.

Florida Subclass

All residents of Florida whose Personal Information was compromised as a result of the Data Breach, including all Florida residents who received a breach notification letter from Defendant.

Massachusetts Subclass

All residents of Massachusetts whose Personal Information was compromised as a result of the Data Breach, including all Massachusetts residents who received a breach notification letter from Defendant.

New York Subclass

All residents of New York whose Personal Information was compromised as a result of the Data Breach, including all New York residents who received a breach notification letter from Defendant.

192. Plaintiffs reserve the right to amend the above definitions or to propose additional or revised subclasses in subsequent pleadings and motions for class certification.

193. Excluded from the Class are Defendant and its officers, directors and employees; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

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

195. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. At least, 77,099 received Notices of the Data Breach.

196. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event

and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

197. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class that Plaintiffs seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

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

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

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiffs' and Class Members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiffs and Class Members to use reasonable care in protecting their Personal Information;

h. 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 Plaintiffs and Class Members;

i. Whether Defendant continues to breach duties to Plaintiffs and Class Members;

j. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiffs and Class Members are entitled to recover damages, equitable relief, and other relief; and

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members and the general public.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of each Plaintiff and his/her Respective State Subclass)

200. Plaintiffs incorporate paragraphs 1-199 above as though fully set forth herein.

201. Defendant required Plaintiffs and Class Members to submit PII in order to obtain financial investment services.

202. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiffs and Class Members.

203. As described above, Fidelity owed duties of care to Plaintiffs and Class Members whose PII had been entrusted to Fidelity. Those duties of care included acting with reasonable care to secure and safeguard the PII of Plaintiffs and Class Members and using commercially reasonable methods to do so. Defendant assumed such duties upon accepting and storing the PII of Plaintiffs and Class Members in its systems.

204. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

205. Defendant acted with negligent disregard for the security of Plaintiffs' and Class Members' PII. Defendant knew or should have known that Fidelity had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or reasonably should have known that hackers were attempting to access the PII in financial service companies' databases, such as Fidelity's.

206. A "special relationship" exists between Defendant and Plaintiffs and Class Members. Fidelity entered into a "special relationship" with Plaintiffs and Class Members because Fidelity collected the PII of Plaintiffs and the Class Members and stored it in Fidelity's database – information that Plaintiffs and the Class Members had been required to provide to Fidelity.

207. Only Defendant was in the position to ensure its computer systems and data security practices were sufficient to protect the PII of Plaintiffs and Class Members.

208. Defendant also had an affirmative duty to timely disclose the Data Breach to Plaintiffs and the Class Members so they could take appropriate action to mitigate damages and protect themselves against further damage. Defendant failed to timely notify Plaintiffs and the Class Members by waiting months to inform them of the Data Breach and continuing to date to fail to provide them with sufficient information regarding the extent and full details regarding the Data Breach.

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

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

211. As a direct and proximate result of Defendant' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

212. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) 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 the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services Plaintiffs received.

213. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, and loss of privacy.

214. As a direct and proximate result of Defendant's continuing negligent conduct, Plaintiffs and Class Members are continuing to suffer the risks of exposure of their PII, which remains in Defendant's possession, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members in its possession.

COUNT II – BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of each Plaintiff and his/her Respective State Subclass)

215. Plaintiffs incorporate paragraphs 1-199 above as though fully set forth herein.

216. Plaintiffs and Class Members entered into implied contracts with Fidelity when they obtained financial investment services from Fidelity, for which they were required to provide their PII. The PII provided by Plaintiffs and Class Members to Fidelity was governed by and subject to Fidelity's privacy duties and policies.

217. Fidelity agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or otherwise compromised.

218. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed Fidelity would use part of the monies paid to Fidelity under the implied contracts to fund adequate and reasonable data security practices.

219. Based on Defendant's conduct, representations (including those in its Privacy Policy), legal obligations, and acceptance of Plaintiffs' and Class Members' Personal Information, Defendant had an implied duty to safeguard their Personal Information through the use of reasonable industry standards.

220. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Personal Information to Defendant, in exchange for, amongst other things, the protection of their PII.

221. Plaintiffs and Class Members would not have obtained financial investment services from Fidelity or provided and entrusted their PII to Defendant in the absence of the implied contract or implied terms between them and Fidelity. The safeguarding of the PII of Plaintiffs and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

222. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Fidelity.

223. Defendant breached its implied contracts with Plaintiffs and Class Members to protect their PII when it: (1) failed to have security protocols and measures in place to protect that

information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

224. As a direct and proximate result of Fidelity's breaches of implied contract, Plaintiffs and Class Members sustained actual losses and damages described above and are also entitled to recover nominal damages.

225. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) 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 the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services Plaintiffs received.

226. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class Members are continuing to suffer the risks of exposure of their PII, which remains in Defendant's possession, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members in its possession.

COUNT III – BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of each Plaintiff and his/her Respective State Subclass)

227. Plaintiffs incorporate paragraphs 1-199 above, as well as the allegations in Count II above, as though fully set forth herein.

228. Plaintiffs and Class Members entered into valid, binding, and enforceable implied contracts with Defendant, as alleged above.

229. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiffs' and Class Members' PII and to comply with industry standards and federal and state laws and regulations.

230. A "special relationship" exists between Defendant and Plaintiffs and Class Members. Fidelity entered into a "special relationship" with Plaintiffs and Class Members who sought investment services from Fidelity and, in doing so, entrusted Fidelity, pursuant to its requirements, with their PII.

231. Despite this special relationship with Plaintiffs and Class Members, Fidelity did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII.

232. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Fidelity.

233. Fidelity's failure to act in good faith in implementing the security measures required by the implied contracts denied Plaintiffs and Class Members the full benefit of their

bargain, and instead they received financial investment and finance-related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to this overpayment.

234. Fidelity's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Class Members to suffer actual damages resulting from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

235. Accordingly, Plaintiffs and Class Members have been injured as a result of Fidelity's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

236. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) 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 the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of

Defendant's services Plaintiffs received.

237. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class Members are continuing to suffer the risks of exposure of their PII, which remains in Defendant's possession, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members in its possession.

COUNT IV – BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of each Plaintiff and his/her Respective State Subclass)

238. Plaintiffs incorporate paragraphs 1-199 above as though fully set forth herein.

239. A "special relationship" exists between Defendant and Plaintiffs and Class Members. Fidelity entered into a "special relationship" with Plaintiffs and Class Members who sought investment services from Fidelity and, in doing so, entrusted Fidelity, pursuant to its requirements, with their PII.

240. Defendant accepted the special confidence placed in it by Plaintiffs and Class Members, even asserting that it "recognize[s] the importance of maintaining the privacy of personal information."[51]

241. In taking possession of the PII of Plaintiffs and Class Members, as required by Defendant, there was an understanding between the parties that Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the PII.

242. Defendant became the guardian of Plaintiffs' and Class Members' PII and accepted a fiduciary duty to act primarily for the benefit of its customers, including Plaintiffs and Class Members, including safeguarding Plaintiffs' and Class Members' PII.

243. Defendant's fiduciary duty to act for the benefit of Plaintiffs and Class Members

[51] *Privacy Policy,* FIDELITY INVESTMENTS, https://www.fidelity.com/privacy/policy (last accessed Feb. 3, 2025).

pertains as well to matters within the scope of its relationship with its clients, in particular, to keep secure the Personal Information of those clients.

244. Defendant owed a duty to Plaintiffs 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 by, misused by, or disclosed to unauthorized persons.

245. Plaintiffs and Class Members have a privacy interest in their PII and Defendant had a duty not to disclose or allow unauthorized access to that confidential information.

246. Plaintiffs and Class Members did not consent to or authorize Defendant to release or disclose their PII to unknown criminal actors.

247. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to: (a) encrypt and otherwise protect the integrity of its computer systems containing Plaintiffs' and the Class Members' PII; (b) diligently discover or investigate the Data Breach in a reasonable and practicable period of time; and (c) timely notify and/or warn them of the Data Breach.

248. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) 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 the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services Plaintiffs received.

249. As a direct and proximate result of Defendant's breach of fiduciary duties, Plaintiffs and Class Members have suffered other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, and loss of privacy.

250. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm in an amount to be proven at trial.

251. As a direct and proximate result of Defendant's breaches of fiduciary duties, Plaintiffs and Class Members are continuing to suffer the risks of exposure of their PII, which remains in Defendant's possession, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members in its possession.

COUNT V – UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of each Plaintiff and his/her Respective State Subclass)

252. Plaintiffs incorporate paragraphs 1-199 above as though fully set forth herein.

253. This claim is brought in the alternative to the other claims.

254. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of payments made for the purchase of financial investment services.

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

256. The payments for financial investment services that Plaintiffs and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for

the administrative costs of reasonable data privacy and security practices and procedures.

257. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the financial investment services with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate financial investment services without reasonable data privacy and security practices and procedures that they received.

258. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state and local laws, and industry standards.

259. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by Defendant.

260. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiffs and Class Members.

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

COUNT VI – MASSACHUSETTS CONSUMER PROTECTION ACT
CH. 93A, §§ 1 *et seq.*
(On behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of Plaintiff Nixon and the Massachusetts Subclass)

262. Plaintiffs incorporate paragraphs 1-199 above as though fully set forth herein.

263. Defendant, Plaintiff and the Class Members are each a "person" as defined by the Massachusetts Consumer Protection Act ("MCPA"), MASS. GEN. LAWS Ch. 93A, §1(a).

264. By offering financial investment and other services, Defendant is engaged in "trade" or "commerce" defined as "the advertising, the offering for sale, rent or lease, the sale,

rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security . . . and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of this commonwealth." MASS. GEN. LAWS Ch. 93A, §1(b).

265. Defendant obtained Plaintiffs' and Class Members' PII through advertising, offering, and/or distributing goods and services to Plaintiffs and Class Members and the Data Breach occurred at least in part through the use of the internet, an instrumentality of interstate commerce.

266. Defendant is engaged in trade or commerce that directly or indirectly affects the people of the Commonwealth of Massachusetts.

267. Under MASS. GEN. LAWS Ch. 93A, §2(a), "unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

268. Defendant violated MASS. GEN. LAWS Ch. 93A, §2(a) in that it has engaged in "unfair or deceptive acts or practices in the conduct of any trade or commerce."

269. Defendant had a duty to keep the Personal Information of Plaintiffs and the Class Members safe and secure under the various laws and regulations discussed hereinabove.

270. Defendant failed to adequately protect and secure the Personal Information of Plaintiffs and the Class Members and failed to comply with its obligations to protect and secure the Personal Information.

271. Defendant failed to comply with industry standards for the protection and security of the Personal Information.

272. Defendant failed to comply with its own privacy practice relating to the protection

and security of the Personal Information.

273. Defendant failed to disclose that it did not have adequate security practices in place to safeguard the Personal Information.

274. Criminals were able to access the Personal Information through the Data Breach.

275. Defendant had a duty to timely notify its clients, including Plaintiffs and the Class Members, of the Data Breach, including under MASS. GEN. LAWS Ch. 93H, §3, the Massachusetts Security Breach statute.

276. Defendant failed to timely notify its customers, including Plaintiffs and Class Members, of the Data Breach.

277. The aforementioned actions and omissions constitute unfair or deceptive acts or practices under MASS. GEN. LAWS Ch. 93A, §2(a).

278. Such acts by Defendant were likely to mislead a reasonable person purchasing and/or using Defendant's services.

279. Said acts are material in that a reasonable person would consider them important in deciding whether to purchase and/or use Defendant's services. If Plaintiffs the Class Members had known that Defendant had inadequate computer systems and data security practices to properly safeguard their PII, they would not have paid for Defendant's services or would have paid less than they did.

280. Defendant acted with disregard for the security of Plaintiffs' and Class Members' PII. Defendant knew or should have known that Fidelity had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII in financial service companies' databases, such as Fidelity's.

281. As a result of the aforementioned actions and omissions, Plaintiffs and Class Members have suffered, and will continue to suffer, injury in an amount to be determined at trial, including, but not limited to: the loss of the benefit of their bargain with Defendant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses incurred protecting themselves from fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

282. As a result of the aforementioned actions and omissions, Plaintiffs and Class Members seek their actual damages, statutory damages, double or treble damages, their costs and reasonable attorneys' fees, and any injunctive or equitable relief needed to secure Personal Information in the possession, custody, and control of Defendant and its agents. *See* MASS. GEN. LAWS Ch. 93A, § 9.

283. Further, as a direct result of Defendant's violations of the MCPA, Plaintiffs and Class Members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties,

as well as the steps Defendant's current and former customers must take to protect themselves.

284. A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice and the injury suffered was mailed or delivered to Defendant at least 30 days prior to the filing of a pleading alleging this claim for relief. *See* MASS. GEN. LAWS Ch. 93A, § 9(3). By letter dated January 7, 2025, Plaintiffs, on behalf of themselves and Class Members, sent Defendant notice under this provision.[52] By letter dated January 22, 2025, Defendant denied all allegations.

COUNT VII – CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100, *et seq.*
(On behalf of Plaintiffs Mason and Elterman and the California Subclass)

285. Plaintiffs Mason and Elterman incorporate paragraphs 1-199 above as though fully set forth herein.

286. Defendant violated the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiffs Mason and Elterman's and the California Subclass Members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure because of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs Mason and Elterman and the California Subclass Members. *See* Cal. Civ. Code § 1798.150.

287. As a direct and proximate result of Defendant's acts, Plaintiffs Mason and Elterman's and the California Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems and/or from the dark web, where hackers further disclosed its customers' PII, including that of Plaintiffs Mason and Elterman

[52] *See* Notice, attached hereto as Exh. 1.

and the California Subclass Members.

288. As a direct and proximate result of Defendant's acts, Plaintiffs Mason and Elterman and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of their legal protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

289. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs Mason and Elterman's and the California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs Mason and Elterman and the California Subclass Members.

290. Defendant is one of the largest investment firms in the United States and as of January 2025 it had $15 trillion in assets under administration and $5.8 trillion in discretionary assets.[53] Fidelity employs more than 75,000 people across 216 Investor Centers in the United States.[54] In 2023, Fidelity generated over $28.2 billion in revenue.[55] Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

291. Plaintiffs Mason and Elterman and the California Subclass Members are each a "[c]onsumer" as defined by Cal. Civ. Code § 1798.140(i) because they are "a natural person who

[53] *Our Company,* Fidelity, https://www.fidelity.com/about-fidelity/our-company (last accessed Feb. 3, 2025).
[54] *Id.*
[55] *Fidelity Annual Report 2023,* Fidelity (2023), https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/about-fidelity/2023-Fidelity-Investments-Annual-Report.pdf (last accessed Feb. 3, 2025); *see also* https://www.fidelity.com/about-fidelity/our-company (last accessed Feb. 3, 2025).

is a California resident, as defined in Section 17104 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017…."

292. Fidelity is a "[b]usiness" as that term is defined in Cal. Civ. Code § 1798.140(d). Defendant FMR LLC and Defendant Fidelity Brokerage Services LLC are each a limited liability company organized or operated for the profit or financial benefit of its shareholders or other owners. Defendant collects consumers' personal information (including that of Plaintiffs Mason and Elterman and the California Subclass Members) or such information is collected on Defendant's behalf, and Defendant determines the purposes and means of processing of consumers' personal information. Defendant does business in California and has annual revenues in excess of $25 million.

293. The information accessed during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(v)(1). At minimum, that information included customers' names; Social Security numbers; financial account data; and driver's license information, all of which is "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

294. Under the CCPA, Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information that it stored. *See* Cal. Civ. Code § 1798.150(a)(1).

295. Defendant's failure to prevent the Data Breach by implementing and maintaining reasonable security procedures and practices constitutes a breach of its duties under the CCPA.

296. By letter received by Defendant on or about November 6, 2024, Plaintiff Mason provided written notice to Defendant identifying the specific provisions of this Act he alleges it

violated.[56] By letter dated December 4, 2024, Defendant denied all allegations. *See* Cal. Civ. Code § 1798.150(b).

297. By letter dated December 23, 2024, Plaintiff Elterman provided written notice to Defendant identifying the specific provisions of this Act he alleges it violated.[57] By letter dated January 22, 2025, Defendant denied all allegations. *See* Cal. Civ. Code § 1798.150(b).

298. Plaintiffs Mason and Elterman, on behalf of themselves and the California Subclass Members, seek damages under the CCPA to the fullest extent possible. *See* Cal. Civ. Code § 1798.150.

COUNT VIII – CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code § 1798.82
(On behalf of Plaintiffs Mason and Elterman and the California Subclass)

299. Plaintiffs Mason and Elterman incorporate paragraphs 1-199 above as though fully set forth herein.

300. Under the California Customer Records Act ("CCRA"), Defendant FMR LLC and Defendant Fidelity Brokerage Services LLC are each a "business" under Cal. Civ. Code § 1798.80(a) in that, as limited liability companies, each is a "sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of [California], any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution."

301. Defendant "maintains computerized data that includes personal information that the … business does not own" and is required to "notify the owner … of the information" in event of

[56] *See* CCPA Notice, attached hereto as Exh. 2. This letter had a clerical error showing the date as June 25, 2024; however, Defendant responded that it received the letter on or about November 6, 2024.
[57] *See* CCPA Notice, attached hereto as Exh. 3.

a breach. Cal. Civ. Code § 1798.82(b).

302. The Data Breach was a "[b]reach of the security of the system" under Cal. Civ. Code § 1798.82(g) as it was an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, or integrity of personal information maintained by the person …."

303. The PII in the Data Breach was "personal information" under Cal. Civ. Code § 1798.82(h) because it was "an individual's first name or first initial and last name in combination with" at least one "of the following data elements, when either the name or the data elements [we]re not encrypted:" social security numbers and driver's license information. It was also "[p]ersonal information" under Cal. Civ. Code § 1798.80(e) because it was "(e) "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

304. The PII was "[r]ecords" under Cal. Civ. Code § 1798.80(b) because it is "any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted."

305. The PII in the Data Breach was not "encrypted" under Cal. Civ. Code § 1798.82(4) because it was not "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

306. Plaintiffs Mason and Elterman and the California Subclass Members are each an "[i]ndividual" under Cal. Civ. Code § 1798.80(d) as each is "a natural person," and each is a "[c]ustomer" under Cal. Civ. Code § 1798.80(c) as each is an "individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business."

307. Defendant's failure to timely disclose the Data Breach to Plaintiffs Mason and Elterman and the California Subclass Members violated the CCRA in that it failed to "notify the owner … of the information of the breach of the security of the data immediately following discovery, [where] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

308. As a direct result of the actions of Defendant that violated the CCRA, Plaintiffs Mason and Elterman and the California Subclass Members have been harmed.

309. Pursuant to Cal. Civ. Code § 1798.84(b), Plaintiffs Mason and Elterman and the California Subclass Members seek damages for Defendant's violations. Plaintiffs Mason and Elterman and the California Subclass Members also seek injunctive relief under Cal. Civ. Code § 1798.84(e).

310. The injunctive relief sought includes, but is not limited to:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

COUNT IX – CALIFORNIA UNFAIR COMPETITION LAW
California Business & Professions Code § 17200, *et seq.*
(On behalf of Plaintiffs Mason and Elterman and the California Subclass)

311. Plaintiffs Mason and Elterman incorporate paragraphs 1-199, as well as the allegations in Count VII and VIII above, as though fully set forth herein.

312. The California Unfair Competition Law ("UCL"), as defined in Cal. Bus. & Prof. Code § 17200 *et seq.*, prohibits "any unlawful, unfair or fraudulent business act or practice ."

313. Defendant, Plaintiffs Mason and Elterman and the California Subclass Members are each a "person" under the UCL, which includes "natural persons, corporations, firms, partnerships, joint stock companies, associations and other organizations of persons." *See* Cal. Bus. & Prof. Code § 17201.

314. Defendant's conduct violated § 17200 through its (1) unlawful and (2) unfair business acts or practices.

Unlawful

315. Defendant's business acts or practices were unlawful in that they violated at least the CCPA, as alleged hereinabove at Count VII, and CCRA, alleged hereinabove at Count VIII.

316. Defendant had a duty to keep the Personal Information of Plaintiffs Mason and Elterman and the California Subclass safe and secure under the various laws and regulations discussed hereinabove.

317. Defendant failed to adequately protect and secure the Personal Information and failed to comply with its obligations to protect and secure the Personal Information.

318. Defendant failed to comply with industry standards for the protection and security of the Personal Information.

319. Defendant failed to comply with its own Privacy Policy and practices relating to the protection and security of the Personal Information.

320. Defendant failed to disclose that it did not have adequate security practices in place to safeguard the Personal Information.

321. Criminals were able to access the Personal Information through the Data Breach.

322. Defendant had a duty to timely notify its clients, including Plaintiffs Mason and Elterman and the California Subclass Members, including under Cal. Civ. Code § 1798.82(b), a California Security Breach statute.

323. Defendant failed to timely notify its customers, including Plaintiffs Mason and Elterman and the California Subclass Members, of the Data Breach.

324. The aforementioned actions constitute unfair business acts or practices under § 17200.

325. If Plaintiffs Mason and Elterman and the California Subclass Members had known that Defendant had inadequate computer systems and data security practices to properly safeguard their PII, they would not have paid for Defendant's services or would have paid less than they did.

Unfair

326. Defendant failed to act with reasonable care to secure and safeguard the PII of Plaintiffs Mason and Elterman and the California Subclass Members. Defendant's conduct was thus immoral, unethical, unscrupulous, or substantially injurious to consumers and the utility of its

conduct, if any, does not outweigh the gravity of the harm to its victims.

327. Defendant's conduct was also unfair because it violates public policy as declared by specific constitutional, statutory, or regulatory provisions, including, but not limited to, the CCPA and CCRA.

328. Defendant's conduct was also unfair because the consumer injury is substantial, not outweighed by benefits to consumers or competition, and not one consumers, themselves, can reasonably avoid.

329. Pursuant to Cal. Bus. & Prof. Code § 17203, as a direct result of the aforementioned actions by Defendant, Plaintiffs Mason and Elterman and the California Subclass seek an order for the restitution of all monies which were unjustly acquired by Defendant through unlawful and unfair business acts or practices to the fullest extent available under law. These amounts are to be determined at trial. Plaintiffs Mason and Elterman and the California Subclass Members also seek reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5.

330. Pursuant to Cal. Bus. & Prof. Code § 17203, as a direct result of the aforementioned actions by Defendant, Plaintiffs Mason and Elterman and the California Subclass Members also seek an order enjoining Defendants from continuing to conduct business through unfair competition, including:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

COUNT X – NEW YORK GEN. BUS. LAW § 349
(On behalf of Plaintiff Lowery and the New York Subclass)

331. Plaintiff Lowery incorporates paragraphs 1-199 above as though fully set forth herein.

332. New York General Business Law § 349 ("GBL § 349") declares as unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or the furnishing of any service in" New York. GBL § 349(a).

333. Plaintiff Lowery and the New York Subclass Members are each a "person" under GBL § 349(h).

334. By offering financial investment and other services, Defendant is engaged in "the conduct of any business, trade or commerce or the furnishing of any service in" New York.

335. Defendant violated GBL § 349(a) in that it has engaged in "[d]eceptive acts or practices in the conduct of any business, trade or commerce or the furnishing of any service in" New York.

336. Defendant had a duty to keep the Personal Information of Plaintiff Lowery and the New York Subclass safe and secure under the various laws and regulations discussed hereinabove.

337. Defendant failed to adequately protect and secure the Personal Information and failed to comply with its obligations to protect and secure the Personal Information.

338. Defendant failed to comply with industry standards for the protection and security of the Personal Information.

339. Defendant failed to comply with its own privacy practice relating to the protection and security of the Personal Information.

340. Defendant failed to disclose that it did not have adequate security practices in place to safeguard the Personal Information.

341. Criminals were able to access the Personal Information through the Data Breach.

342. Defendant had a duty to timely notify its clients, including Plaintiff Lowery and the New York Subclass Members, of the Data Breach, including under N.Y. Gen. Bus. § 899-aa(3), the New York Security Breach statute.

343. Defendant failed to timely notify its customers, including Plaintiff Lowery and the New York Subclass Members, of the Data Breach.

344. The aforementioned actions and omissions constitute unfair or deceptive acts or practices under GBL § 349(a).

345. Defendant's acts were consumer oriented.

346. Defendant acted with disregard for the security of Plaintiff Lowery's and the New York Subclass Members' PII. Defendant knew or should have known that Defendant had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII in financial service companies' databases, such as Defendant's.

347. Such acts by Defendant were likely to mislead a reasonable person purchasing and/or using Defendant's services.

348. Said acts are material in that a reasonable person would consider them important in

deciding whether to purchase and/or use Defendant's services. If Plaintiff Lowery and the New York Subclass Members had known that Defendant had inadequate computer systems and data security practices to properly safeguard their PII, they would not have paid for Defendant's services or would have paid less than they did.

349. As a result of the aforementioned actions and omissions, Plaintiff Lowery and the New York Subclass Members have suffered, and will continue to suffer, ascertainable loss of money or property, in an amount to be determined at trial, including, but not limited to: the loss of the benefit of their bargain with Defendant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses incurred protecting themselves from fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

350. As a result of the aforementioned actions and omissions, Plaintiff Lowery and the New York Subclass Members seek their actual damages or fifty dollars, whichever is greater; three times their actual damages up to one thousand dollars to the extent Defendant is found to have acted willfully or knowingly in violating this statute; punitive damages; costs and reasonable attorneys' fees, and any injunctive or equitable relief needed to secure Personal Information in the possession, custody, and control of Defendant and its agents. *See* GBL § 349(h).

351. Also as a direct result of Defendant's violations of GBL § 349, Plaintiff Lowery and New York Subclass Members are entitled to injunctive relief, including, but not limited to, under GBL § 349(h):

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class Members, seek the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are the proper representatives of the Class requested herein;

B. Awarding declaratory, injunctive, and other equitable relief as is necessary to protect the interests of the Class Members; and

C. Awarding Plaintiffs and the Class actual damages, double or treble damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement of profits, attorney's fees, statutory costs, and such other and further relief as is just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: February 10, 2025

/s/ *Christina Xenides*
Christina Xenides (Bar No. 677603)
SIRI & GLIMSTAD LLP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
Telephone: (512) 265-5622
cxenides@sirillp.com

Liaison Counsel

Lori G. Feldman (admitted *pro hac vice*)
GEORGE FELDMAN McDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
Fax: (888) 421-4173
lfeldman@4-justice.com
eservice@4-justice.com

A. Brooke Murphy (admitted *pro hac vice*)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Interim Lead Counsel

Daniel Srourian*
SROURIAN LAW FIRM, P.C.
468 N. Camden Drive, Suite 200
Beverly Hills, California 90210
Telephone: (213) 474-3800
Fax: (213) 471-4160
daniel@slfla.com

Elizabeth Apostola*
ZEMEL LAW LLC
400 Sylavn Ave, Suite 200
Englewood Cliffs, NJ 07632
Telephone: (862) 227-3106
ea@zemellawllc.com

Interim Executive Committee Members

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS

GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Fax: (202) 686-2877
dlietz@milberg.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

Janine L. Pollack*
GEORGE FELDMAN MCDONALD, PLLC
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: (917) 983-2707
Fax: (888) 421-4173
jpollack@4-justice.com
Eservice@4-justice.com

Additional Counsel for Plaintiffs

* *pro hac vice* forthcoming

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on February 10, 2025, the foregoing was filed electronically with the Clerk of Court using the CM/ECF System and was thereby served on all counsel of record.

/s/ *Christina Xenides*
Christina Xenides

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.mad.276267/gov
on 2026-10-19 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/fidelity-investments

Court: U.S. District Court, District of Massachusetts
Case number: 1:24-CV-12601-LTS
Filed: 2025-02-10

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.