**UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**
**EASTERN DIVISION**

| | |
|---|---|
| IN RE GREYLOCK MCKINNON ASSOCIATES DATA SECURITY INCIDENT LITIGATION | Case No. 1:24-cv-10797<br><br>**CONSOLIDATED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Tim Isaac, Mary Isaac, Theresa McFadden, Valerie Gunther, Leland Wooten Jr., Paulette Zalewski, Dale Robertson, Daniel Jasperson, Albert Waddington, Dina Crocetto-Waddington, John McLaughlin, Charles McCurdy, Lynn Kohler, and Richard Lilly (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members," as defined *infra*), allege the following against Defendant Greylock McKinnon Associates, Inc., ("Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

## INTRODUCTION

1. Defendant is a consulting firm based in Boston, Massachusetts that provides expert economic analysis and litigation support.

2. As a part of providing those services, Defendant acquired and maintained the personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of consumers, including Medicare beneficiaries.

3. On February 5, 2024, Defendant discovered it had lost control over its computer

network and the highly sensitive personal information stored on its computer network in a data breach perpetrated by cybercriminals ("Data Breach"). Upon information and belief, the Data Breach's impact has been substantial, affecting over 300,000 individuals.

4. On information and belief, the Data Breach began on or around May 30, 2023. Following an internal investigation that concluded on February 5, 2024, Defendant learned cybercriminals had gained unauthorized access to consumer's Private Information, including but not limited to name, date of birth, address, Medicare Health Insurance Claim Number (which contains a Social Security number associated with a member) and medical information and/or health insurance information.[1]

5. On or about February 23, 2024—an appalling nine months after the Data Breach occurred—Defendant finally began notifying Class Members about the Data Breach ("Notice Letter") (*see* Plaintiffs' breach notices, attached as **Exhibit B**).

6. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the Private Information of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect Plaintiffs' and the Class Member's Private Information—rendering them easy targets for cybercriminals.

7. Defendant's Notice Letter obfuscated the nature of the breach and the threat it posted—refusing to tell victims how many people were impacted, how the breach happened, when it discovered the breach, or why it took Defendant nine months to finally begin notifying victims

[1] *See* State of California Department of Justice, Submitted Breach Notification Sample, https://oag.ca.gov/ecrime/databreach/reports/sb24-583540 (last accessed on June 5, 2024), attached hereto as ***Exhibit A***.

that cybercriminals had gained access to their highly private information.

8. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

10. Plaintiffs and Class Members are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and Class Members trusted Defendant with their Private Information. However, Defendant betrayed that trust by failing to properly use up-to-date security practices to prevent the Data Breach.

11. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

12. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the Private Information of Plaintiffs and Class Members was exactly that—private. No longer. Now, their Private Information is permanently exposed and unsecure, leaving them at a heightened and imminent risk of fraud and identity theft.

## PARTIES

13. Plaintiff Tim Isaac is a natural person and citizen of Kentucky, residing in Nicholasville, Kentucky.

14. Plaintiff Mary Isaac is a natural person and citizen of Florida, residing in Orange Park, Florida.

15. Plaintiff McFadden is a natural person and citizen of Florida.

16. Plaintiff Robertson is a natural person and citizen of Pennsylvania, residing in Manheim, Pennsylvania.

17. Plaintiff Jasperson is a natural person and citizen of California, residing in Wilmington, California.

18. Plaintiff Gunther is a natural person and citizen of Ohio, residing in Warren, Ohio.

19. Plaintiff Zalewski is a natural person and citizen of Pennsylvania, residing in Greensburg. Pennsylvania.

20. Plaintiff Wooten is a natural person and citizen of Florida, residing in Cocoa, Florida.

21. Plaintiff Waddington is a natural person and citizen of New Jersey, residing in Williamstown, New Jersey.

22. Plaintiff Crocetto-Waddington is a natural person and citizen of New Jersey, residing in Williamstown, New Jersey.

23. Plaintiff McLaughlin is a resident and citizen of New Jersey, residing in Woolwich Township, New Jersey.

24. Plaintiff McCurdy is a natural person and citizen of Texas, residing in Houston, Texas.

25. Plaintiff Kohler is a natural person and citizen of Ohio, residing in Mason, Ohio.

26. Plaintiff Lilly is a natural person and citizen of Missouri, residing in Jefferson, Missouri.

27. Defendant is Massachusetts corporation with its principal place of business located at 75 Park Plaza, 4th Floor, Boston, Massachusetts 02116.

## JURISDICTION & VENUE

28. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members.

29. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts, and regularly conducts business in Massachusetts. Plaintiffs and Defendant are citizens of different states.

30. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

## FACTUAL ALLEGATIONS

***Defendant's Business***

31. Defendant "provides expert economic analysis and litigation support to a diverse group of domestic and international clients in the legal profession, the business community, and government agencies."[2] It boasts over $5 million in annual revenue.[3]

32. While administering services, Defendant accumulates the Private Information of consumers.

33. As a sophisticated economic advisor with an acute interest in maintaining the confidentiality of the Private Information entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding the Private Information in its possession.

---

[2] About GMA, Greylock McKinnon Associates, https://www.gma-us.com/

[3] Greylock McKinnon Associates Information, RocketReach, https://rocketreach.co/greylock-mckinnon-associates-profile_b7e6c2f9c07c2c34

34. Consequently, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information.

35. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect consumer Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Private Information.

***The Data Breach***

36. On information and belief, Defendant collects and maintains consumers' unencrypted Private Information in its computer systems.

37. In collecting and maintaining Private Information, Defendant implicitly agreed that it will safeguard the data using reasonable means according to their internal policies as well as state and federal law.

38. On or about February 23, 2024, Defendant sent Class Members a Notice Letter, stating, in part:

> **What Happened?**
>
> On May 30, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity specialists to assist with our response to the incident, and we notified law enforcement and the DOJ. We received confirmation of which individuals' information was affected and obtained their contact addresses on February 7, 2024.
>
> **What Information Was Involved?**
>
> Your personal and Medicare information was likely affected in this incident. This information may have included your name, date of birth, address, Medicare Health Insurance Claim Number (which contains a Social Security number associated with a

member) and some medical information and/or health insurance information.[4]

39. Omitted from the Notice Letter were the date(s) of the Data Breach, the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

41. Through its inadequate security practices, Defendant exposed Plaintiffs' and Class Member's Private Information for theft and sale on the dark web.

42. Despite its duties to safeguard Private Information, Defendant did not in fact follow industry standard practices in securing consumers' Private Information, as evidenced by the Data Breach.

43. In response to the Data Breach, Defendant contends that it "consulted with third-party cybersecurity specialists to assist with our response to and remediation of the incident."[5] Although Defendant fails to expand on what these hypothetical "remediation" efforts are, such actions, if implemented at all, should have been in place before the Data Breach.

44. Through its Notice Letter, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims "to activate the fraud

[4] *See, e.g.,* Ex. A.
[5] *Id.*

detection tools available," to "regularly review statements from your accounts and periodically obtain your credit report," and to "remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft."[6]

45. On information and belief, Defendant has offered a one year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Private Information that cannot be changed, such as Social Security numbers.

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

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

48. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' Private Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

***The Value of Private Information***

49. It is well known that Private Information, including Social Security numbers, is an

[6] *Id.*

invaluable commodity for which a "cyber black market" exists in which cybercriminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

50. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[7]

51. 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[8]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[9]; and other sources report that cybercriminals can also purchase access to entire company data breaches from $999 to $4,995.[10]

52. Moreover, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

53. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information

[7] Consumer Information, Dark Web Monitoring: What You Should Know, Consumer Federation of America (March, 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/

[8] Anita George, Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[9] Brian Stack, Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[10] VPNOverview, In the Dark, (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

increases."[11] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[12]

54. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[13] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[14]

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

56. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft.[15]

---

[11] Avoid Identity Theft: Protect Social Security Numbers, Social Security Admin. – Philadelphia Region, https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases

[12] *Id.*

[13] How to Protect Yourself from Social Security Number Identity Theft, Equifax (2014), https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/

[14] Julia Kagan, What Is an SSN? Facts to Know About Social Security Numbers, Investopedia (Feb. 15, 2024) https://www.investopedia.com/terms/s/ssn.asp

[15] *See, e.g., Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 272 (S.D.N.Y. 2021) (citations omitted) (noting plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and]

57. Similarly, driver's license numbers, which were also compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[16]

58. A driver's license can be a critical part of a fraudulent, synthetic identity—which can go for about $1200 on the dark web. On its own, a forged license can sell for around $200.[17]

59. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[18]

60. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[19] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were

---

employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

[16] Lee Matthews, Hackers Stole Customers' License Numbers From Geico In Months-Long Breach, Forbes (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658

[17] *Id.*

[18] Medical I.D. Theft, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected

[19] Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

never able to resolve their identity theft at all.[20]

61. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach. There, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" as it is difficult and/or undesirable to change one's Social Security number, PHI, date of birth, or name.

***Cyberattacks Put Consumers at an Increased Risk of Fraud and Identity Theft***

62. The link between a data breach and the risk of identity theft is simple and well established. Cybercriminals acquire and steal Private Information to monetize the information. Cybercriminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

63. Cybercriminals can post stolen Private Information on the dark web for years following a data breach, thereby making such information publicly available.

64. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[21] This gives thieves ample time to commit acts of fraud under the victim's name.

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

66. It is within this context that Plaintiffs must now live with the knowledge that their

[20] Brian O'Connor, Healthcare Data Breach: What to Know About them and What to Do After One, Experian (March 31, 2023) https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/

[21] Medical ID Theft Checklist, IdentiyForce (Jan. 11, 2023) https://www.identityforce.com/blog/medical-id-theft-checklist-2

Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

***The Data Breach was a Foreseeable Risk of Which Defendant was on Notice***

67. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting consulting firms that collect and store Private Information, like Defendant, preceding the date of the breach.

68. Data breaches, including those perpetrated against consulting firms that store Private Information in their systems, have become widespread.

69. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[22]

70. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), and numerous others,[23] Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

71. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so

[22] Q3 2023 Data Compromise Charts, ID Theft Resource Center (2023) https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

[23] Michael Hill and Dan Swinhoe, The 15 Biggest Data Breaches of the 21st Century, CSO Online (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

72. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep consumer's data secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

73. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

74. In October 2019, the FBI published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[25]

75. In April 2020, in an article titled "Ransomware mentioned in 1,000+ SEC filings

[24] Ben Kochman, FBI, Secret Service Warn Of Targeted Ransomware, Law360 (Nov. 18, 2019) https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[25] High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, FBI (Oct. 2, 2019) https://www.ic3.gov/media/y2019/psa191002

over the past year," ZDNet reported 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."[26]

76. 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."[27]

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

78. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands of its current and former consumers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

79. Before the Data Breach, Defendant knew or should have known that there was a

[26] Catalin Cimpanu, Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet (April 30, 2020) https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/

[27] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide

foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

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

***Plaintiff Tim Isaac's Experience and Injuries***

81. Plaintiff Tim Isaac received a Notice Letter from Defendant dated February 23, 2024, informing him that his Private Information—including his name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

82. Plaintiff Tim Isaac is very careful about sharing his sensitive information.

83. Plaintiff Tim Isaac stores any documents containing his Private Information in a safe and secure location. Plaintiff Tim Isaac has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

84. Since the Data Breach, Plaintiff Tim Isaac has experienced actual injury in the form of identity theft. In February 2024, an unauthorized actor tried obtaining a car loan in Plaintiff Tim Issac's name. In March 2024, someone tried to open a First Progress credit card in his name and in April 2024, someone tried to open a Republic Bank account in his name. Plaintiff Tim Isaac received an alert from Credit Karma notifying him that his information was found on the dark web in early 2024.

85. Plaintiff Tim Issac was also notified about two unauthorized hard inquiries on his credit report and he has been unable to remove the inquiries from his credit report at this time.

Plaintiff Tim Isaac has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Tim Isaac attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that he has never experienced anything like this prior to now.

86. As a result of the Data Breach, Plaintiff Tim Isaac has had no choice but to spend approximately twenty hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Tim Isaac has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

87. As a result of the Data Breach, Plaintiff TimIsaac has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Tim Isaac fears that criminals will use his information to commit identity theft.

***Plaintiff Mary Isaac's Experience and Injuries***

88. Plaintiff Mary Isaac received a Notice Letter from the U.S. Department of Justice dated April 5, 2024, informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

89. Plaintiff Mary Isaac is very careful about sharing her sensitive information.

90. Plaintiff Mary Isaac stores any documents containing her Private Information in a safe and secure location. Plaintiff Mary Isaac has never knowingly transmitted unencrypted

sensitive PII over the internet or any other unsecured source. She also diligently chooses unique usernames and passwords for her online accounts.

91. Since the Data Breach, Plaintiff Mary Isaac has experienced a substantial increase in spam and phishing phone calls and text messages. Also, an unauthorized party tried opening a T-Mobile account in her name. Additionally, she has had to change her debit card twice due to authorized charges appearing on her account. Plaintiff Mary Isaac attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that she has never experienced anything like this prior to now. Further, to Plaintiff Mary Isaac's knowledge, her Private Information has never been exposed in any other Data Breach.

92. As a result of the Data Breach, Plaintiff Mary Isaac has had no choice but to spend many hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Mary Isaac has already expended at least three hours and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including changing her debit cards and visiting the bank on three occasions, and taking other protective and ameliorative steps in response to the Data Breach.

93. As a result of the Data Breach, Plaintiff Mary Isaac has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Mary Isaac fears that criminals will use her information to commit identity theft.

***Plaintiff Wooten Jr.'s Experience and Injuries***

94. Plaintiff Wooten received a Notice Letter from the U.S. Department of Justice dated April 5, 2024, informing him that his Private Information—including his name and Social Security

number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

95. Plaintiff Wooten is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

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

97. Since the Data Breach, Plaintiff Wooten has experienced a substantial increase in spam and phishing phone calls about Medicare-related issues, as well as targeted spam emails. Plaintiff Wooten attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that (a) his Medicare information was among the Private Information accessed in the Data Breach, and (b) he has never experienced anything like this prior to now. Further, to Plaintiff Wooten's knowledge, his Private Information has never been exposed in any other Data Breach.

98. As a result of the Data Breach, Plaintiff Wooten has had no choice but to spend many hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Wooten has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, signing up for credit monitoring, freezing his credit with all three major credit bureaus, requesting and reviewing his credit report, and taking other protective and ameliorative steps in response to the Data Breach.

99. As a result of the Data Breach, Plaintiff Wooten has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing

and misusing his Private Information. Plaintiff Wooten fears that criminals will use his information to commit identity theft.

***Plaintiff McFadden's Experience and Injuries***

100. Plaintiff McFadden received a Notice Letter from Defendant informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

101. Plaintiff McFadden is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

102. Plaintiff McFadden stores any documents containing her Private Information in a safe and secure location. Plaintiff McFadden has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

103. Since the Data Breach, Plaintiff McFadden has experienced identity theft when at least three unauthorized purchases were charged to her PayPal account, forcing her to contact PayPal and close her account, and when she received a fraudulent letter and phone call about her Social Security number being frozen. Plaintiff McFadden has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff McFadden attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity.

104. As a result of the Data Breach, Plaintiff McFadden has had no choice but to spend over 3 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff McFadden has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

105. As a result of the Data Breach, Plaintiff McFadden has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff McFadden fears that criminals will use her information to commit identity theft.

***Plaintiff Robertson's Experience and Injuries***

106. Plaintiff Robertson received a Notice Letter from Defendant dated April 8, 2024, informing him that his Private Information—including his name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

107. Plaintiff Robertson is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

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

109. Since the Data Breach, Plaintiff Robertson has experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Robertson attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

110. As a result of the Data Breach, Plaintiff Robertson has had no choice but to spend approximately 3-4 hours reviewing his credit reports, attempting to mitigate the harms caused by the Data Breach, and addressing the future consequences of the Breach. Among other things,

Plaintiff Robertson has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

111. As a result of the Data Breach, Plaintiff Robertson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Robertson fears that criminals will use his information to commit identity theft.

***Plaintiff Gunther's Experience and Injuries***

112. Plaintiff Gunther received a Notice Letter from Defendant informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

113. Plaintiff Gunther is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

114. Plaintiff Gunther stores any documents containing her Private Information in a safe and secure location. Plaintiff Gunther has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

115. Since the Data Breach, Plaintiff Gunther has experienced identity theft when she was notified by a bank that a person attempted to fraudulently use her medical insurance in another state and when her computer was hacked, financial account information was taken, and she was asked to pay a $500-$600 ransom for the stolen data. Plaintiff Gunther has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Gunther attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time

proximity and the fact that she has never experienced anything like this prior to now.

116. As a result of the Data Breach, Plaintiff Gunther has had no choice but to spend approximately 5 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Gunther has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

117. As a result of the Data Breach, Plaintiff Gunther has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Gunther fears that criminals will use her information to commit identity theft.

118. Plaintiff Gunther anticipates spending considerable time and money on an ongoing basis.

***Plaintiff Zalewski's Experience and Injuries***

119. Plaintiff Zalewski received a Notice Letter from Defendant informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

120. Plaintiff Zalewski is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

121. Plaintiff Zalewski stores any documents containing her Private Information in a safe and secure location. Plaintiff Zalewski has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

122. Since the Data Breach, Plaintiff Zalewski has experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Zalewski attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

123. As a result of the Data Breach, Plaintiff Zalewski has had no choice but to spend approximately 5 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Zalewski has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

124. As a result of the Data Breach, Plaintiff Zalewski has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Zalewski fears that criminals will use her information to commit identity theft.

***Plaintiff Jasperson's Experience and Injuries***

125. Plaintiff Jasperson received a Notice Letter from Defendant on or around April 2024, informing him that his Private Information—including his name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

126. Plaintiff Jasperson is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

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

128. Since the Data Breach, Plaintiff Jasperson has experienced identity theft in the form of a $2,300 fraudulent purchase on his Discover card, forcing him to get a reissued card, fraudulent purchases on his Amazon account, which is linked to his debit card, forcing him to close his Amazon account and close and reopen his bank account, and stolen mail.

129. Plaintiff Jasperson has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails, forcing him to change his email address and phone number multiple times. Plaintiff Jasperson attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

130. As a result of the Data Breach, Plaintiff Jasperson has had no choice but to spend approximately 30-40 hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Jasperson has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

131. Plaintiff Jasperson purchased a $20 per month subscription to Experian to protect his credit following the Data Breach.

***Plaintiff Waddington's Experience and Injuries***

132. Plaintiff Waddington received a Notice Letter from the Department of Justice informing him that his Private Information—including his name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

133. Plaintiff Waddington is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

134. Plaintiff Waddington stores any documents containing his Private Information in a safe and secure location. Plaintiff Waddington has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

135. Since the Data Breach, Plaintiff Waddington has experienced identity theft in the form of fraudulent charges on his debit card and credit card, forcing him to get reissued cards. Plaintiff Waddington has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Waddington attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that he has never experienced anything like this prior to now.

136. As a result of the Data Breach, Plaintiff Waddington has had no choice but to spend over 30 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Waddington has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

137. Plaintiff Waddington additionally spent three to 4 hours researching Defendant and attempting to contact someone about the Data Breach and going to his bank to check his accounts.

138. As a result of the Data Breach, Plaintiff Waddington has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Waddington fears that criminals will use his information to commit identity theft.

***Plaintiff Crocetto-Waddington's Experience and Injuries***

139. Plaintiff Crocetto-Waddington received a Notice Letter from the Department of Justice informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

140. Plaintiff Crocetto-Waddington is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

141. Plaintiff Crocetto-Waddington stores any documents containing her Private Information in a safe and secure location. Plaintiff Crocetto-Waddington has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

142. Since the Data Breach, Plaintiff Crocetto-Waddington has experienced identity theft in the form of a fraudulently financed purchase from Empire Carpet from her Well Fargo bank account. Plaintiff Crocetto-Waddington has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Crocetto-Waddington attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity and the fact that she has never experienced anything like this prior to now.

143. As a result of the Data Breach, Plaintiff Crocetto-Waddington has had no choice but to spend time every few days for about a year attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff

Crocetto-Waddington has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

144. As a result of the Data Breach, Plaintiff Crocetto-Waddington has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Crocetto-Waddington fears that criminals will use her information to commit identity theft.

***Plaintiff Mclaughlin's Experience and Injuries***

145. Plaintiff McLaughlin received a Notice Letter from the Department of Justice dated April 5, 2024, informing him that his Private Information—including his name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

146. Plaintiff McLaughlin is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

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

148. Since the Data Breach, Plaintiff McLaughlin has received notification that his personal information has been found on the dark web. As a result, he had to close his American Express credit card and open a new account. Plaintiff McLaughlin has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff McLaughlin attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now and, to

his knowledge, his Private Information has never been exposed in any other Data Breach.

149. As a result of the Data Breach, Plaintiff McLaughlin has had no choice but to spend approximately 1-2 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff McLaughlin has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

150. As a result of the Data Breach, Plaintiff McLaughlin has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff McLaughlin fears that criminals will use his information to commit identity theft.

***Plaintiff McCurdy's Experience and Injuries***

151. Plaintiff McCurdy received a Notice Letter from the Department of Justice dated April 5, 2024, informing him that his Private Information—including his name, Social Security number, date of birth, address, telephone number, Medicare Beneficiary Identifier, driver's license number, healthcare provider, prescription information, and health insurance information—was specifically identified as having been exposed to cybercriminals in the Data Breach.

152. Plaintiff McCurdy is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

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

154. Since the Data Breach, Plaintiff McCurdy has experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff McCurdy attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

155. As a result of the Data Breach, Plaintiff McCurdy has had no choice but to spend time attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff McCurdy has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

156. As a result of the Data Breach, Plaintiff McCurdy has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff McCurdy fears that criminals will use his information to commit identity theft.

***Plaintiff Kohler's Experience and Injuries***

157. Plaintiff Kohler received a Notice Letter from Defendant dated April 8, 2024, informing her that her Private Information—including her name and Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

158. Plaintiff Kohler is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

159. Plaintiff Kohler stores any documents containing her Private Information in a safe

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

160. Since the Data Breach, Plaintiff Kohler has received notification that her personal information has been found on the dark web. Plaintiff Kohler has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails from individuals claiming to be Aetna representatives. Plaintiff Kohler attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

161. As a result of the Data Breach, Plaintiff Kohler has had no choice but to spend approximately ten hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Kohler has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate 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.

162. As a result of the Data Breach, Plaintiff Kohler has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Kohler fears that criminals will use her information to commit identity theft.

***Plaintiff Richard Lilly's Experience and Injuries***

163. Plaintiff Richard Lilly received a Notice Letter from the U.S. Department of Justice dated April 5, 2024, informing him that his Private Information – including his name and Social

Security number – was specifically identified as having been exposed to cybercriminals in the Data Breach.

164. Plaintiff Lilly is a reasonably cautious person and is very careful about sharing his sensitive Private Information. Plaintiff Lilly has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

165. Since the Data Breach, Plaintiff Lilly has experienced a substantial increase in spam texts and emails containing his personal information. Plaintiff Lilly attributes the foregoing suspicious activity to the Data Breach given the time proximity.

166. As a result of the Data Breach, Plaintiff Lilly has expended time and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including researching facts about Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

167. As a result of the Data Breach, Plaintiff Lilly has experienced stress, anxiety, and concern due to the loss of his privacy and concerns over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Lilly fears that criminals will use his information to commit identity theft.

168. The Notice Letters Plaintiffs received from Defendant specifically directed them to take the actions described *supra*. Indeed, the Notice Letters advised Plaintiffs and all Class Members that they should "regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies." They further stated: "Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft." In addition, the Notice Letters

recommended that victims of the Data Breach protect themselves by, among other things, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.

169. Because of the Data Breach, Plaintiffs' Private Information is now in the hands of cyber criminals.

170. Defendant deprived Plaintiffs of the earliest opportunity to guard themselves against the Data Breach's effects by failing to notify them about it for nine months.

171. Plaintiffs have suffered actual injuries from the exposure and theft of their Private Information—which violates their right to privacy.

172. Defendant's Data Breach exposed Plaintiffs' highly valuable information, such as their Social Security numbers, to cybercriminals. Plaintiffs are now subject to a present and continuing risks of crippling identity theft and fraud.

173. Plaintiffs have also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of their valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiffs' Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiffs' Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiffs, including the difference in value between what Plaintiffs 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 Plaintiffs' Private Information; and (e) continued risk to Plaintiffs' Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to

undertake appropriate and adequate measures to protect the Private Information that was entrusted to it.

174. Plaintiffs request that Defendant remove and destroy their and Class Member's Private Information, which, upon information and belief, remains backed up in Defendant's possession.

175. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

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

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

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

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and

fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

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

178. The value of Plaintiffs' and Class Member's Private Information on the black market is considerable. One such example of cybercriminals using consumer's stolen data for profit is the development of "Fullz" packages.[28]

179. "Fullz" packages are the result of cybercriminals cross-referencing two sources of Private 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.

180. The development of "Fullz" packages means that stolen Private Information from

[28] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.

the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Member's 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 Private Information stolen by the cybercriminals in the Data Breach, cybercriminals can easily create a "Fullz" package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

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

182. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated their injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

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

183. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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 FTCA.

184. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

185. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[29] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

186. 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.

187. 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.

188. The FTC has brought enforcement actions against businesses for failing to

[29] Protecting Personal Information – A Guide for Business, United States Federal Trade Comm'n (2016) https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

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

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

***Defendant Failed to Follow Industry Standards***

190. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] 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 . . . ."[32]

191. "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*."[33]

---

[30] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[31] *Id.* at 17.
[32] *Id.* at 28.
[33] *Id.*

192. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: 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.

193. Other industry standard best practices 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; and training staff regarding critical points.

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

***Defendant Fails to Comply With HIPAA Guidelines***

195. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the cybercriminals—thereby causing the Data Breach.

196. Defendant is a business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

197. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[34] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

198. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

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

200. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

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

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[34] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

203. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

204. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

205. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[35]

206. HIPAA requires a business associate to have and apply appropriate sanctions

[35] Breach Notification Rule, U.S. Dep't of Health & Human Services (July 26, 2013) https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added)

against members of its workforce who fail to comply with the privacy policies and procedures of the business associate or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

207. HIPAA requires a business associate to mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

208. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[36] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[37]

**CLASS ACTION ALLEGATIONS**

209. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

210. Plaintiffs are suing on behalf of themselves and the proposed Classes (together the "Class"), defined as follows:

---

[36] Security Rule Guidance Material, U.S. Dep't of Health & Human Services (Feb. 16, 2024) http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

[37] Guidance on Risk Analysis, U.S. Dep't of Health & Human Services (July 22, 2019) https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

**Nationwide Class: All individuals residing in the United States whose Private Information was compromised in Defendant's Data Breach, including all those who received a Notice Letter.**

**California Subclass: All individuals residing in California whose Private Information was compromised in Defendant's Data Breach, including all those who received a Notice Letter.**

**New Jersey Subclass: All individuals residing in New Jersey whose Private Information was compromised in Defendant's Data Breach, including all those who received a Notice Letter.**

211. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

212. Plaintiffs reserve the right to amend the Class definitions.

213. This action satisfies the numerosity, commonality, adequacy, and appropriateness requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. Plaintiffs' claims are representative of the proposed Class, consisting of at least 300,000 individuals, far too many to join in a single action;

b. **Ascertainability**. Class Members are readily identifiable from information in Defendant's possession, custody, and control;

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

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class' interests. Plaintiffs' interest does not conflict with Class Members' interests, and Plaintiffs have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class' behalf, including as lead counsel.

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

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs and the Class' Private Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class' Private Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Notice Letter was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

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

**FIRST CLAIM FOR RELIEF**
**Negligence**
**(On Behalf of Plaintiff and the Class)**

215. Plaintiffs re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully set forth herein.

216. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

217. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise the Private Information in its custody in a data breach. And here, that foreseeable danger came to pass.

218. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

219. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

220. Defendant owed at least the following duties to to Plaintiffs and Class Members:

a. to exercise reasonable care in handling and using the Private Information in its care and custody;

b. to implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized access;

c. to promptly detect attempts at unauthorized access; and

d. to notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

221. Also, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. Such duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

222. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

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

224. By being entrusted by Plaintiffs and the Class to safeguard their Private Information, Defendant had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class agreed to provide their Private Information with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiffs and the Class of any security concerns that might call for action by Plaintiffs and the Class.

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

226. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

227. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

228. Defendant breached these duties as evidenced by the Data Breach.

229. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties; and,

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

230. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

231. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

232. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

233. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

**SECOND CLAIM FOR RELIEF**
**Negligence *per se***
**(On Behalf of Plaintiff and the Class)**

235. Plaintiffs re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully set forth herein.

236. Under the FTCA, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

237. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTCA also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive Private Information.

238. Defendant breached its respective duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security

practices to safeguard PII.

239. Defendant violated its duty under Section 5 of the FTCA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

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

243. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

244. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed, *supra*).

**THIRD CLAIM FOR RELIEF**
**Breach of Third-Party Beneficiary Contract**
**(On Behalf of Plaintiff and the Class)**

245. Plaintiffs re-allege and incorporate the allegations in paragraphs 1 through 202 as

if fully set forth herein.

246. Defendant entered into various contracts with its clients, to provide services to its clients.

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

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

249. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Private Information.

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

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

**FOURTH CLAIM FOR RELIEF**
**Unjust Enrichment**
**(On Behalf of the Plaintiff and the Class)**

252. Plaintiffs re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully set forth herein.

253. This claim is pled in the alternative to Plaintiffs' Third Claim for Relief (breach of third-party beneficiary contract).

254. Plaintiffs and Class Members conferred a benefit upon Defendant in providing their Private Information to Defendant.

255. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members. And Defendant benefited from receiving Plaintiffs' and Class Members' Private Information, as this was used to facilitate its business.

256. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

257. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

258. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' Private Information because Defendant failed to adequately protect their Private Information. Plaintiffs and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

259. Defendant should be compelled to establish a common fund to benefit Plaintiffs and members of the Class for all unlawful or inequitable proceeds it received as a result of its conduct and Data Breach alleged here.

**FIFTH CLAIM FOR RELIEF**
**Invasion of Privacy**

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

260. Plaintiffs re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully set forth herein.

261. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

262. Defendant owed a duty to the consumers whose data it retained, including Plaintiffs and the Class, to keep such data confidential.

263. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

264. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

265. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interests in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

266. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

267. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

268. Acting with knowledge, Defendant had notice and knew that its inadequate

cybersecurity practices would cause injury to Plaintiffs and the Class.

269. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

270. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

271. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

272. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**SIXTH CLAIM FOR RELIEF**
**CALIFORNIA CONSUMER RECORDS ACT**
**Cal. Civ. Code § 1798.82, et seq.**
**(on behalf of Plaintiff Jasperson and the California Subclass)**

273. Plaintiff Jasperson, on behalf of himself and the California Subclass, re-alleges and incorporates the allegations in paragraphs 1 through 202 as if fully set forth herein.

274. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or

notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay."

275. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code, § 1798.82(b)).

276. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

    i. The name and contact information of the reporting person or business subject to this section;

    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

    i. The date of the breach;

    ii. The estimated date of the breach; or

    iii. The date range within which the breach occurred. The notification shall

also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

277. The Data Breach described herein constituted a "breach of the security system" of Defendant.

278. As alleged above, Defendant unreasonably delayed informing Plaintiff and California Subclass Members about the Data Breach, affecting their PII and PHI, after Defendant knew the Data Breach had occurred.

279. Defendant failed to disclose to Plaintiff and the California Subclass Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when Defendant knew or reasonably believed such information had been compromised.

280. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

281. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and the California Subclass Members would impede its investigation.

282. As a result of Defendant's violation of California Civil Code section 1798.82,

Plaintiff and the California Subclass Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and California Subclass Members because their stolen information would have had less value to identity thieves.

283. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff and the California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

284. Plaintiff and the California Subclass Members seek all remedies available under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiff and the other California Subclass Members, including but not limited to benefit-of-the-bargain and time spent monitoring their accounts for identity theft and medical identity theft, and equitable relief.

285. Defendant's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff and the California Subclass Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and the California Subclass Members and despicable conduct that has subjected Plaintiff and the California Subclass Members to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff and the California Subclass Members are entitled to punitive damages against Defendant under California Civil Code

section 3294(a).

**SEVENTH CLAIM FOR RELIEF**
**CALIFORNIA UNFAIR COMPETITION LAW**
**Cal. Bus. & Prof. Code § 17200, et seq.**
**(on behalf of Plaintiff Jasperson and the California Subclass)**

286. Plaintiff Jasperson, on behalf of himself and the California Subclass, re-alleges and incorporates the allegations in paragraphs 1 through 202 as if fully set forth herein.

287. Defendant regularly does business in California. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, et seq.) by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard PII and PHI from unauthorized disclosure, release, data breach, and theft; representing and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the California Subclass's PII and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the California Subclass's PII and PHI;

b. by soliciting and collecting California Subclass Members' PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass Members' PII and PHI in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, et seq.;

e. by violating the CMIA, California Civil Code section 56, et seq.; and

f. by violating the CCRA, California Civil Code section 1798.82.

288. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., CMIA, Cal. Civ. Code, § 56, et seq., and the CCRA, Cal. Civ. Code, § 1798.81.5.

289. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

290. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and California Subclass Members' PII and PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

291. Plaintiff seeks relief under the UCL, including restitution to the California Subclass of money or property that the Defendant may have acquired by means of Defendant's deceptive,

unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

**EIGHTH CLAIM FOR RELIEF**
**CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")**
**Cal. Civ. Code § 1798, *et seq.***
**(On behalf of Plaintiff Jasperson and the California Subclass)**

292. Plaintiff Jasperson, on behalf of himself and the California Subclass, re-alleges and incorporates the allegations in paragraphs 1 through 202 as if fully set forth herein.

293. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."38

294. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

295. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

296. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose

[38] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

297. Plaintiff and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

298. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling

consumers' personal information.

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

300. Plaintiff and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

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

302. Simultaneously herewith, Plaintiff is providing notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges GMA has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) GMA is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

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

304. As a result of Defendant's failure to implement and maintain reasonable security

procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

**NINETH CLAIM FOR RELIEF**
**NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT,**
**N.J. Stat. Ann. §§ 56:8-163, et seq.**
**(On Behalf of Plaintiffs Waddington and Crocetto-Waddington and the New Jersey Subclass)**

305. Plaintiffs Waddington and Crocetto-Waddington ("Plaintiffs," for purposes of this Count), individually and on behalf of the New Jersey Subclass, re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully alleged herein.

306. Defendant is a business that compiles or maintains computerized records that include personal information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

307. Plaintiffs' and New Jersey Subclass Members' PII includes personal information covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

308. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

309. Because Defendant discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Defendant had an obligation to disclose the Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

310. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.J. Stat. Ann. § 56:8-163(b).

311. As a direct and proximate result of Defendant's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiffs and New Jersey Subclass Members suffered the damages described above.

312. Plaintiffs and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

**TENTH CLAIM FOR RELIEF**
**NEW JERSEY CONSUMER FRAUD ACT**
**N.J. Stat. Ann. §§ 56:8-1, et seq.**
**(On Behalf of Plaintiffs Waddington and Crocetto-Waddington and the New Jersey Subclass)**

313. Plaintiffs Waddington and Crocetto-Waddington ("Plaintiffs," for purposes of this Count), individually and on behalf of the New Jersey Subclass, re-allege and incorporate the allegations in paragraphs 1 through 202 as if fully alleged herein.

314. Defendant is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

315. Defendant sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

316. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

317. Defendant's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and New Jersey Subclass Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass Members' PII and PHI, including duties imposed by the FTCA, 15 U.S.C. § 45 which was a direct and proximate cause of the Defendant data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and New Jersey Subclass Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass Members' PII and PHI, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Subclass Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass Members' PII and PHI, including duties imposed by the FTCA, 15 U.S.C. § 45.

318. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII and PHI.

319. Defendant intended to mislead Plaintiffs and New Jersey Subclass Members and induce them to rely on its misrepresentations and omissions.

320. Defendant acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs and New Jersey Subclass Members' rights. Past breaches put Defendant on notice that its security and privacy protections were inadequate.

321. As a direct and proximate result of Defendant's unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

322. Plaintiffs and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs

**PRAYER FOR RELIEF**

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

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

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

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and

the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

**JURY DEMAND**

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

Dated: June 17, 2024

Respectfully submitted,

*/s/ Raina C. Borrelli*

Raina Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263.1100
raina@straussborrelli.com

*Counsel for Plaintiff Tim Isaac and the Putative Class*

Jeff Ostrow*
Kristen Lake Cardoso*
KOPELOWITZ OSTROW P.A.
1 West Las Olas. Blvd., Ste. 500

Fort Lauderdale, FL 33301
(954) 332-4200
ostrow@kolawyers.com
cardoso@kolawyers.com

*Counsel for Plaintiff Mary Isaac and the Putative Class*

Robert T. Naumes Jr., Esq.*
Attorneys for Representative Plaintiff
and the Plaintiff Class(es)
JEFFREY GLASSMAN INJURY LAWYERS
One International Place, 18th Floor
Boston, Massachusetts 02186
(617) 777-7777
bnaumes@jeffreysglassman.com

Scott Edward Cole, Esq.*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
(510) 891-9800
sec@colevannote.com

*Counsel for Plaintiff Richard Lilly and the Putative Class*

Christina Xenides*
Mason A. Barney*
Tyler Bean*
SIRI & GLIMSTAD LLP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
(512) 265-5622
cxenides@sirillp.com
mbarney@sirillp.com
tbean@sirillp.com

*Counsel for Plaintiffs McFadden, Gunther and the Putative Class*

Randi Kassan*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530

(212) 594-5300
rkassan@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
(866) 252-0878
dlietz@milberg.com

*Counsel for Plaintiff Robertson and the Putative Class*

Sean K. Collins*
LAW OFFICES OF SEAN K. COLLINS
184 High Street, Suite 503
Boston, MA 02110
(855) 693-9256
sean@neinsurancelaw.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
(513) 345-8291
jgoldenberg@gs-legal.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
(215) 592-1500
cschaffer@lfsblaw.com

*Counsel for Plaintiffs Jasperson, Waddington, and Crocetto-Waddington and Putative Class*

James J. Reardon*
REARDON SCANLON LLP
45 South Main Street, 3rd Floor
West Hartford, CT 06107
(860) 944-9455
james.reardon@reardonscanlon.com

Kevin Laukaitis*

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

*Counsel for Plaintiff McLaughlin and Putative Class*

William B. Federman*
Kennedy M. Brian*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
(405) 235-1560
wbf@federmanlaw.com
kpb@federmanlaw.com

*Counsel for Plaintiff McCurdy and the Putative Class*

Marc H. Edelson*
Liberato P. Verderame Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
(215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

*Counsel for Plaintiffs Kohler and Zalewski and Putative Class*

Edward F. Haber*
Ian J. McLoughlin*
Patrick J. Vallely*
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
(617) 439-3939
ehaber@shulaw.com
imcloughlin@shulaw.com
pvallely@shulaw.com

Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
(415) 788-4220
aschubert@sjk.law

*Counsel for Wooten, Jr. and the Putative Class*

**pro hac vice* forthcoming

**CERTIFICATE OF SERVICE**

I, Raina C. Borrelli, hereby certify that on June 17, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record, below, via the ECF system.

DATED this 17th day of June, 2024.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109

# — EXHIBIT A —

Greylock McKinnon Associates, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Greylock McKinnon Associates
*Boston, MA ■ Washington, DC ■ Hanover, NH*
*www.gma-us.com*



April 8, 2024

**Notice of Data Breach**

Dear :

Greylock McKinnon Associates, Inc. ("GMA") was the victim of a sophisticated cyberattack involving your personal information. We are writing to notify you of this incident as well as provide you with information on the actions that we have taken in response, resources available to you, and steps you can take to protect yourself. GMA is a consulting firm that provides litigation support services in civil litigation matters. Your information was obtained by the U.S. Department of Justice ("DOJ") as part of a civil litigation matter. We received your information in our provision of services to the DOJ in support of that matter.

DOJ has advised us that you are not the subject of this investigation or the associated litigation matters. The DOJ informed GMA that this incident does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**
On May 30, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity specialists to assist with our response to the incident, and we notified law enforcement and the DOJ. We received confirmation of which individuals' information was affected and obtained their contact addresses on February 7, 2024.

**What Information Was Involved?**
Your personal and Medicare information was likely affected in this incident. This information may have included your name, date of birth, address, Medicare Health Insurance Claim Number (which contains a Social Security number associated with a member) and some medical information and/or health insurance information.

**What Are We Doing?**
We consulted with third-party cybersecurity specialists to assist with our response to and remediation of the incident, and we notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

**What Can You Do?**
To help protect your identity, we are offering complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

**How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/gmaus and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For additional information and steps that you can take to protect yourself from identity theft, see enclosure.

At this time, GMA is not aware of any reports of identity fraud or improper use of your information as a result of this incident. We have been informed by the DOJ that the Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**
If you have any questions or need any additional information, please call our dedicated call center at 1-833-914-4067. Representatives are available for 90 days from the date of this letter to assist you between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-914-4067 and be prepared to supply the fraud specialist with your unique code listed within.

Sincerely,

Rene Rushnawitz, Managing Director

**Information about Identity Theft Protection**

**Monitor Your Accounts**

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

| | | |
|---|---|---|
| Equifax®<br>P.O. Box 740241<br>Atlanta, GA 30374-0241<br>1-800-685-1111<br>www.equifax.com | Experian<br>P.O. Box 9701<br>Allen, TX 75013-9701<br>1-888-397-3742<br>www.experian.com | TransUnion®<br>P.O. Box 1000<br>Chester, PA 19016-1000<br>1-800-888-4213<br>www.transunion.com |

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

**Credit Freeze**

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

| | | |
|---|---|---|
| Equifax<br>P.O. Box 105788<br>Atlanta, GA 30348-5788<br>1-800-685-1111<br>www.equifax.com/personal/<br>credit-report-services | Experian<br>P.O. Box 9554<br>Allen, TX 75013-9554<br>1-888-397-3742<br>www.experian.com/<br>freeze/center.html | TransUnion<br>P.O. Box 2000<br>Chester, PA 19016-2000<br>1-888-909-8872<br>www.transunion.com/<br>credit-freeze |

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

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

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

**Fraud Alerts**

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

| Equifax | Experian | TransUnion |
|---|---|---|
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5788 | Allen, TX 75013-9554 | Chester, PA 19016-2000 |
| 1-888-766-0008 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com/personal/ credit-report-services | www.experian.com/ fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert |

**Additional Information**

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

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

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at http://www.irs.gov. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at http://www.irs.gov/pub/irs-pdf/f14039.pdf. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

You may also have the right to file or obtain a police report with your local law enforcement office if you believe you have been a victim of identity theft or fraud.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

**California Residents**: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225.

**Kentucky Residents**: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

**District of Columbia Residents**: For more information you can contact the Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001, 202-442-9828, consumer.protection@dc.gov. You can also visit the Office of Consumer Protection's website at https://oag.dc.gov/consumer-protection for more information.

**Iowa Residents**: You may wish to report suspected incidents of identity theft to local law enforcement or the Attorney General, Consumer Protection Division, at Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, by phone at 515-281-5926 or 888-777-4590, or by email at consumer@ag.iowa.gov. You can also visit the Consumer Protection Division website at https://www.iowaattorneygeneral.gov/forconsumers for more information.

**Maryland Residents**: You may wish to contact the Attorney General, Consumer Protection Division, for more information at 200 St. Paul Place, Baltimore, MD 21202, by telephone at 410-528-8662 or 888-743-0023, or by email at Consumer@oag.state.md.us. You can also visit the Consumer Protection Division website at https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx for more information.

**Massachusetts Residents**: Please note that you have the right to file or obtain a police report related to this incident.

**New Mexico Residents**: Please note your rights under the Fair Credit Reporting Act, which can be viewed here https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

**New York Residents**: You may wish to contact the Attorney General's Office at The Capitol, Albany, NY 12224-0341, or by telephone at 800-771-7755 or 800-788-9898. You may also contact the Department of State, Consumer Protection Division at 800-697-1220 or to visit https://www.dos.ny.gov/consumerprotection/ for more information.

**North Carolina Residents**: You may wish to contact the Attorney General's Office at 9001 Mail Service Center Raleigh, NC 27699-9001, or by telephone at 919-716-6000. You can also find more information from the Consumer Protection Division by visiting https://ncdoj.gov/protectingconsumers/.

**Oregon Residents**: You may wish to contact the Attorney General's Consumer Protection Division by email at help@oregonconsumer.gov or by telephone at 877-877-9392. You may also visit https://www.doj.state.or.us/consumer-protection/ for more information.

**Puerto Rico Residents**: Please note that there were 171 affected individuals residing in Puerto Rico.

**Rhode Island Residents**: You may wish to contact the Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Please note that there were 154 affected individuals residing in Rhode Island.

**Texas Residents**: Please note that there were 13,379 affected individuals residing in Texas.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

0000103O3O0000 P

# — EXHIBIT B —

1 of 3

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJTCCO00811265
ALBERT S WADDINGTON

U.S. Department of Justice

Executive Office for United States Attorneys

April 8, 2024

PJTCCO00811265*2650102T0400

Notice of Breach

Dear ALBERT WADDINGTON,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

2 of 3

- Health Benefits and Enrollment Information
- In some cases, Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).

**What Are We Doing?**

GMA consulted with third-party cybersecurity specialists to assist with their response to and remediation of the incident and notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

DOJ is committed to protecting the personal information we collect and maintain. And, while this ransomware attack did not involve a DOJ system, we have also taken the appropriate steps to ensure the protection of your information and identity, including the offer of free credit monitoring through Sontiq.

**What Can You Do?**

1. Enroll in Sontiq, Inc. Data Breach and Identity Protection Services

DOJ is offering a complimentary 12 months of credit monitoring from Sontiq at no cost to you. Please see the enclosed information for details on how to enroll. You will also need to reference the enrollment code below when enrolling online, so please **do not** discard this letter.

2. Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies listed above. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. At the same time, you may also wish to place a credit freeze or a fraud alert on your credit report. A credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. A fraud alert advises creditors to contact you before opening any new accounts. There is no charge for you to do this.

By calling or writing any one of the three credit reporting companies, you will be able to place a credit freeze or fraud alerts with all of the credit reporting companies. You will then receive letters from each of them with instructions on how to obtain a copy of your credit reports from each of the companies at no cost if you have not done so already. Sample written notifications are provided for you, attached to this correspondence. Also provided for you are the relevant sections of the Fair Credit Reporting Act. You may want to reference the appropriate Sections of the Act in your correspondence to the credit reporting company.

When you receive your credit reports, review them for problems. Identify any accounts you didn't open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you don't find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you still check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

In addition, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This affidavit can be found at https://www.identitytheft.gov/. This will allow you to notify your creditors that personally identifying information relating to your identity may have been compromised. Depending on the specific circumstances, any debt related to identify theft incurred after you provide this notification to your creditors may not be assigned to you.

3. Continue to Use Your Existing Medicare Card

At this time, DOJ are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. The Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any further questions regarding this incident, please call our toll-free number at 1-844-979-6702. Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Norm Wong
Acting Director
Executive Office for United States Attorneys

1 of 3

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJTCCO00A01783
DINA M CROCETTO WADINGTON

U.S. Department of Justice

Executive Office for United States Attorneys

April 8, 2024

PJTCCO00A01783017830102/0400

Notice of Breach

Dear DINA CROCETTO WADINGTON,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

2 of 3

- Health Benefits and Enrollment Information
- In some cases, Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).

**What Are We Doing?**

GMA consulted with third-party cybersecurity specialists to assist with their response to and remediation of the incident and notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

DOJ is committed to protecting the personal information we collect and maintain. And, while this ransomware attack did not involve a DOJ system, we have also taken the appropriate steps to ensure the protection of your information and identity, including the offer of free credit monitoring through Sontiq.

**What Can You Do?**

1. Enroll in Sontiq, Inc. Data Breach and Identity Protection Services

DOJ is offering a complimentary 12 months of credit monitoring from Sontiq at no cost to you. Please see the enclosed information for details on how to enroll. You will also need to reference the enrollment code below when enrolling online, so please **do not** discard this letter.

2. Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies listed above. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. At the same time, you may also wish to place a credit freeze or a fraud alert on your credit report. A credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. A fraud alert advises creditors to contact you before opening any new accounts. There is no charge for you to do this.

By calling or writing any one of the three credit reporting companies, you will be able to place a credit freeze or fraud alerts with all of the credit reporting companies. You will then receive letters from each of them with instructions on how to obtain a copy of your credit reports from each of the companies at no cost if you have not done so already. Sample written notifications are provided for you, attached to this correspondence. Also provided for you are the relevant sections of the Fair Credit Reporting Act. You may want to reference the appropriate Sections of the Act in your correspondence to the credit reporting company.

When you receive your credit reports, review them for problems. Identify any accounts you didn't open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you don't find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you still check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

[redacted] ALBERT S WADDINGTON [redacted] P 8/ 8

3 of 3

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

In addition, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This affidavit can be found at https://www.identitytheft.gov/. This will allow you to notify your creditors that personally identifying information relating to your identity may have been compromised. Depending on the specific circumstances, any debt related to identify theft incurred after you provide this notification to your creditors may not be assigned to you.

3. Continue to Use Your Existing Medicare Card

At this time, DOJ are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. The Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any further questions regarding this incident, please call our toll-free number at 1-844-979-6702. Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Norm Wong
Acting Director
Executive Office for United States Attorneys

PJTCC000A01783017830202G0000

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998
866-5100
PJSV5100A03270
[redacted]

U.S. Department of Justice

Executive Office for United States Attorneys

2 yrs to settle

April 4, 2024

PJSV5100A0327003270010 2N0400

Notice of Breach

Dear LYNNETTE KOHLER,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted. Human

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

866-5100

PJSV5100A03270

[redacted]

2 yrs to settle

U.S. Department of Justice

Executive Office for United States Attorneys

April 4, 2024



Notice of Breach

Dear LYNNETTE KOHLER,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted. Human

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

- Health Benefits and Enrollment Information
- In some cases, Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).

**What Are We Doing?**

GMA consulted with third-party cybersecurity specialists to assist with their response to and remediation of the incident and notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

DOJ is committed to protecting the personal information we collect and maintain. And, while this ransomware attack did not involve a DOJ system, we have also taken the appropriate steps to ensure the protection of your information and identity, including the offer of free credit monitoring through Sontiq.

**What Can You Do?**

1. Enroll in Sontiq, Inc. Data Breach and Identity Protection Services BBB Rate 1.0

DOJ is offering a complimentary 12 months of credit monitoring from Sontiq at no cost to you. Please see the enclosed information for details on how to enroll. You will also need to reference the enrollment code below when enrolling online, so please **do not** discard this letter.

2. Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies listed above. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. At the same time, you may also wish to place a credit freeze or a fraud alert on your credit report. A credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. A fraud alert advises creditors to contact you before opening any new accounts. There is no charge for you to do this.

By calling or writing any one of the three credit reporting companies, you will be able to place a credit freeze or fraud alerts with all of the credit reporting companies. You will then receive letters from each of them with instructions on how to obtain a copy of your credit reports from each of the companies at no cost if you have not done so already. Sample written notifications are provided for you, attached to this correspondence. Also provided for you are the relevant sections of the Fair Credit Reporting Act. You may want to reference the appropriate Sections of the Act in your correspondence to the credit reporting company.

When you receive your credit reports, review them for problems. Identify any accounts you didn't open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you don't find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you still check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

Free
Annualcreditreport.com 7 days
877-322 8228

It [illegible]d suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

In addition, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This affidavit can be found at https://www.identitytheft.gov/. This will allow you to notify your creditors that personally identifying information relating to your identity may have been compromised. Depending on the specific circumstances, any debt related to identify theft incurred after you provide this notification to your creditors may not be assigned to you.

3. Continue to Use Your Existing Medicare Card

At this time, DOJ are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. The Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any further questions regarding this incident, please call our toll-free number at 1-844-979-6702. Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Norm Wong
Acting Director
Executive Office for United States Attorneys

PJSV5100A0327003270020 2F0000

Credit Monitoring Services Information

To enroll in Credit Monitoring services at no charge, please log on to **https://benefit.identityforce.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Greylock McKinnon Associates, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Greylock McKinnon Associates
*Boston, MA ■ Washington, DC ■ Hanover, NH*
*www.gma-us.com*

PJTBN000504603
DANIEL G JASPERSON
[redacted]

April 5, 2024

PJTBN000504603046030103604 00

**Notice of Data Breach**

Dear DANIEL JASPERSON:

Greylock McKinnon Associates, Inc. ("GMA") was the victim of a sophisticated cyberattack involving your personal information. We are writing to notify you of this incident as well as provide you with information on the actions that we have taken in response, resources available to you, and steps you can take to protect yourself. GMA is a consulting firm that provides litigation support services in civil litigation matters. Your information was obtained by the U.S. Department of Justice ("DOJ") as part of a civil litigation matter. We received your information in our provision of services to the DOJ in support of that matter.

DOJ has advised us that you are not the subject of this investigation or the associated litigation matters. The DOJ informed GMA that this incident does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**
On May 30, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity specialists to assist with our response to the incident, and we notified law enforcement and the DOJ. We received confirmation of which individuals' information was affected and obtained their contact addresses on February 7, 2024.

**What Information Was Involved?**
Your personal and Medicare information was likely affected in this incident. This information may have included your name, date of birth, address, Medicare Health Insurance Claim Number (which contains a Social Security number associated with a member) and some medical information and/or health insurance information.

**What Are We Doing?**
We consulted with third-party cybersecurity specialists to assist with our response to and remediation of the incident, and we notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

**What Can You Do?**
To help protect your identity, we are offering complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

**How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/gmaus and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For additional information and steps that you can take to protect yourself from identity theft, see enclosure.

At this time, GMA is not aware of any reports of identity fraud or improper use of your information as a result of this incident. We have been informed by the DOJ that the Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any questions or need any additional information, please call our dedicated call center at 1-833-914-4067. Representatives are available for 90 days from the date of this letter to assist you between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-914-4067 and be prepared to supply the fraud specialist with your unique code listed within.

Sincerely,

Rene Rushnawitz, Managing Director

## Information about Identity Theft Protection

**Monitor Your Accounts**

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

| | | |
|---|---|---|
| Equifax®<br>P.O. Box 740241<br>Atlanta, GA 30374-0241<br>1-800-685-1111<br>www.equifax.com | Experian<br>P.O. Box 9701<br>Allen, TX 75013-9701<br>1-888-397-3742<br>www.experian.com | TransUnion®<br>P.O. Box 1000<br>Chester, PA 19016-1000<br>1-800-888-4213<br>www.transunion.com |

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

**Credit Freeze**

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

| | | |
|---|---|---|
| Equifax<br>P.O. Box 105788<br>Atlanta, GA 30348-5788<br>1-800-685-1111<br>www.equifax.com/personal/<br>credit-report-services | Experian<br>P.O. Box 9554<br>Allen, TX 75013-9554<br>1-888-397-3742<br>www.experian.com/<br>freeze/center.html | TransUnion<br>P.O. Box 2000<br>Chester, PA 19016-2000<br>1-888-909-8872<br>www.transunion.com/<br>credit-freeze |

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

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

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

PJTBN00050460304603020 3M0000

**Fraud Alerts**

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

| | | |
|---|---|---|
| Equifax<br>P.O. Box 105788<br>Atlanta, GA 30348-5788<br>1-888-766-0008<br>www.equifax.com/personal/<br>credit-report-services | Experian<br>P.O. Box 9554<br>Allen, TX 75013-9554<br>1-888-397-3742<br>www.experian.com/<br>fraud/center.html | TransUnion<br>P.O. Box 2000<br>Chester, PA 19016-2000<br>1-800-680-7289<br>www.transunion.com/fraud-<br>victim-resource/place-fraud-alert |

**Additional Information**

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

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

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at http://www.irs.gov. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at http://www.irs.gov/pub/irs-pdf/f14039.pdf. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

You may also have the right to file or obtain a police report with your local law enforcement office if you believe you have been a victim of identity theft or fraud.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]
LELAND W WOOTEN JR
[redacted]

U.S. Department of Justice

Executive Office for United States Attorneys

April 5, 2024

PJT24K0051105411054010240400

Notice of Breach

Dear LELAND WOOTEN JR,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

- Health Benefits and Enrollment Information
- In some cases, Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).

**What Are We Doing?**

GMA consulted with third-party cybersecurity specialists to assist with their response to and remediation of the incident and notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

DOJ is committed to protecting the personal information we collect and maintain. And, while this ransomware attack did not involve a DOJ system, we have also taken the appropriate steps to ensure the protection of your information and identity, including the offer of free credit monitoring through Sontiq.

**What Can You Do?**

1. Enroll in Sontiq, Inc. Data Breach and Identity Protection Services

DOJ is offering a complimentary 12 months of credit monitoring from Sontiq at no cost to you. Please see the enclosed information for details on how to enroll. You will also need to reference the enrollment code below when enrolling online, so please **do not** discard this letter.

2. Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies listed above. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. At the same time, you may also wish to place a credit freeze or a fraud alert on your credit report. A credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. A fraud alert advises creditors to contact you before opening any new accounts. There is no charge for you to do this.

By calling or writing any one of the three credit reporting companies, you will be able to place a credit freeze or fraud alerts with all of the credit reporting companies. You will then receive letters from each of them with instructions on how to obtain a copy of your credit reports from each of the companies at no cost if you have not done so already. Sample written notifications are provided for you, attached to this correspondence. Also provided for you are the relevant sections of the Fair Credit Reporting Act. You may want to reference the appropriate Sections of the Act in your correspondence to the credit reporting company.

When you receive your credit reports, review them for problems. Identify any accounts you didn't open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you don't find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you still check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

In addition, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This affidavit can be found at https://www.identitytheft.gov/. This will allow you to notify your creditors that personally identifying information relating to your identity may have been compromised. Depending on the specific circumstances, any debt related to identify theft incurred after you provide this notification to your creditors may not be assigned to you.

3. Continue to Use Your Existing Medicare Card

At this time, DOJ are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. The Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any further questions regarding this incident, please call our toll-free number at 1-844-979-6702. Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Norm Wong
Acting Director
Executive Office for United States Attorneys

PJT24K0051105411054020 2K0000

## Credit Monitoring Services Information

To enroll in Credit Monitoring services at no charge, please log on to **https://benefit.identityforce.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJT24K00800644
CHARLES MCCURDY
[redacted]

U.S. Department of Justice

Executive Office for United States Attorneys

April 5, 2024

Notice of Breach

Dear CHARLES MCCURDY,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting several of their systems. After taking immediate steps to contain the incident, GMA's initial investigation determined that the group behind the ransomware attack obtained copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

PJT24K00800644006440040102104000

- Health Benefits and Enrollment Information
- In some cases, Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).

**What Are We Doing?**

GMA consulted with third-party cybersecurity specialists to assist with their response to and remediation of the incident and notified law enforcement of the incident. GMA deleted DOJ data from its systems after the incident.

DOJ is committed to protecting the personal information we collect and maintain. And, while this ransomware attack did not involve a DOJ system, we have also taken the appropriate steps to ensure the protection of your information and identity, including the offer of free credit monitoring through Sontiq.

**What Can You Do?**

1. Enroll in Sontiq, Inc. Data Breach and Identity Protection Services

DOJ is offering a complimentary 12 months of credit monitoring from Sontiq at no cost to you. Please see the enclosed information for details on how to enroll. You will also need to reference the enrollment code below when enrolling online, so please **do not** discard this letter.

2. Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies listed above. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. At the same time, you may also wish to place a credit freeze or a fraud alert on your credit report. A credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. A fraud alert advises creditors to contact you before opening any new accounts. There is no charge for you to do this.

By calling or writing any one of the three credit reporting companies, you will be able to place a credit freeze or fraud alerts with all of the credit reporting companies. You will then receive letters from each of them with instructions on how to obtain a copy of your credit reports from each of the companies at no cost if you have not done so already. Sample written notifications are provided for you, attached to this correspondence. Also provided for you are the relevant sections of the Fair Credit Reporting Act. You may want to reference the appropriate Sections of the Act in your correspondence to the credit reporting company.

When you receive your credit reports, review them for problems. Identify any accounts you didn't open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you don't find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you still check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

[redacted]

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

In addition, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This affidavit can be found at https://www.identitytheft.gov/. This will allow you to notify your creditors that personally identifying information relating to your identity may have been compromised. Depending on the specific circumstances, any debt related to identify theft incurred after you provide this notification to your creditors may not be assigned to you.

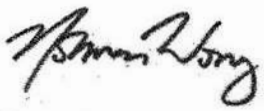
3. Continue to Use Your Existing Medicare Card

At this time, DOJ are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. The Centers for Medicare and Medicaid Services will begin to monitor for any improper use of your Medicare information.

**For More Information**

If you have any further questions regarding this incident, please call our toll-free number at 1-844-979-6702. Representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

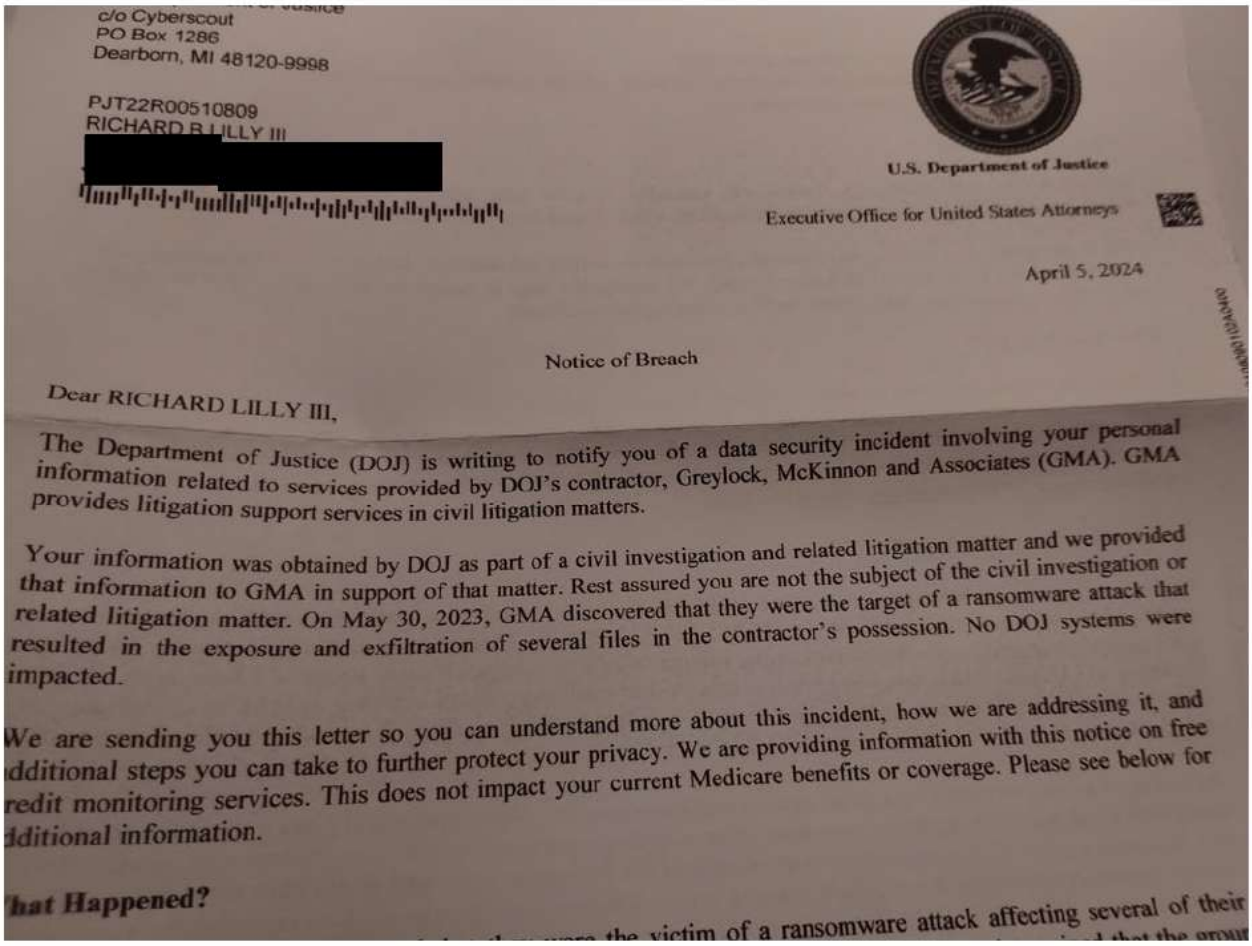


Norm Wong
Acting Director
Executive Office for United States Attorneys

Credit Monitoring Services Information

To enroll in Credit Monitoring services at no charge, please log on to **https://benefit.identityforce.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJT22R00510809
RICHARD B LILLY III
[redacted]

U.S. Department of Justice

Executive Office for United States Attorneys

April 5, 2024

Notice of Breach

Dear RICHARD LILLY III,

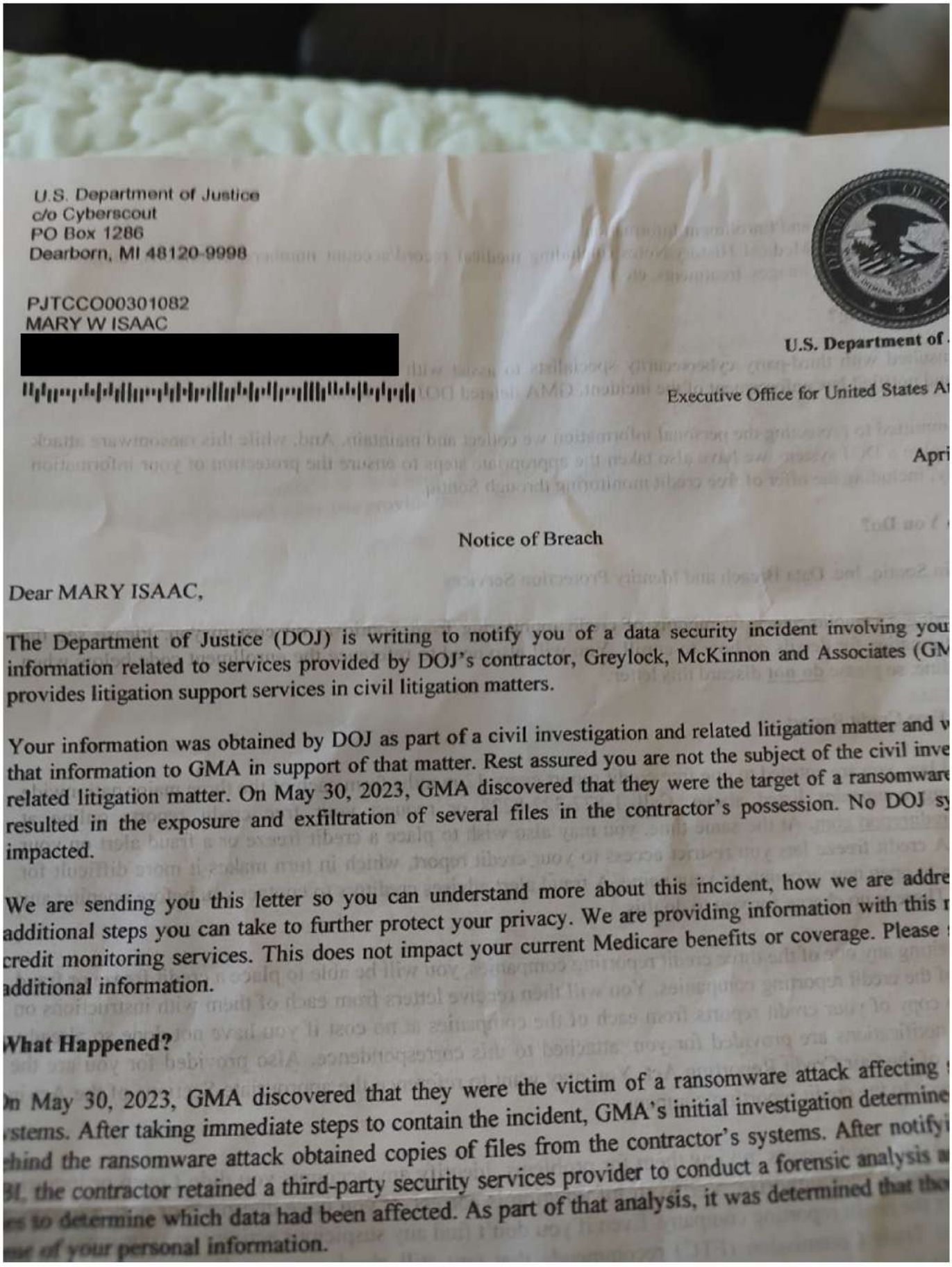
The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free redit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for dditional information.

**hat Happened?**

victim of a ransomware attack affecting several of their



U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJTCCO00301082
MARY W ISAAC
[redacted]

U.S. Department of

Executive Office for United States A

Apri

Notice of Breach

Dear MARY ISAAC,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving you information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GM provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and v that information to GMA in support of that matter. Rest assured you are not the subject of the civil inve related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ sy impacted.

We are sending you this letter so you can understand more about this incident, how we are addre additional steps you can take to further protect your privacy. We are providing information with this r credit monitoring services. This does not impact your current Medicare benefits or coverage. Please additional information.

**What Happened?**

On May 30, 2023, GMA discovered that they were the victim of a ransomware attack affecting stems. After taking immediate steps to contain the incident, GMA's initial investigation determine ehind the ransomware attack obtained copies of files from the contractor's systems. After notifyi 31, the contractor retained a third-party security services provider to conduct a forensic analysis a es to determine which data had been affected. As part of that analysis, it was determined that tho se of your personal information.

U.S. Department of Justice
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PJT24K00901563
JOHN R MCLAUGHLIN
[redacted]

U.S. Department of Justice

Executive Office for United States Attorneys

April 5, 2024

PJT24K00901563015630102J0400

Notice of Breach

Dear JOHN MCLAUGHLIN,

The Department of Justice (DOJ) is writing to notify you of a data security incident involving your personal information related to services provided by DOJ's contractor, Greylock, McKinnon and Associates (GMA). GMA provides litigation support services in civil litigation matters.

Your information was obtained by DOJ as part of a civil investigation and related litigation matter and we provided that information to GMA in support of that matter. Rest assured you are not the subject of the civil investigation or related litigation matter. On May 30, 2023, GMA discovered that they were the target of a ransomware attack that resulted in the exposure and exfiltration of several files in the contractor's possession. No DOJ systems were impacted.

We are sending you this letter so you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy. We are providing information with this notice on free credit monitoring services. This does not impact your current Medicare benefits or coverage. Please see below for additional information.

***What Happened?***

*On May 30, 2023, GMA discovered* that they were the victim of a ransomware attack affecting several of their *systems. After taking immediate steps* to contain the incident, GMA's initial investigation determined that the group *behind the ransomware attack obtained* copies of files from the contractor's systems. After notifying DOJ and the FBI, the contractor retained a third-party security services provider to conduct a forensic analysis and to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

**What Information Was Involved?**

Your personal and Medicare information was likely impacted in this incident. This information may have included:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

# Greylock McKinnon Associates

*Boston, MA ▪ Washington, DC ▪ Hanover, NH*
*www.gma-us.com*

Return Mail Processing
PO Box 999
Suwanee, GA 30024

41 1064 ********** AUTO**MIXED AADC 300
GLENDA ISAAC
[redacted]

February 23, 2024

**RE: Notice of a Security Incident**

Dear Glenda Isaac:

Greylock McKinnon Associates, Inc. ("GMA") was the victim of a sophisticated cyberattack that may have affected your personal information. We are writing to notify you of this incident as well as provide you with information on the actions that we have taken in response, resources available to you, and steps you can take to protect yourself.

GMA is a consulting firm that provides economic analysis and litigation support for legal, business, and government stakeholders. We received your data in our provision of services to our clients.

**What Happened?**
On May 30, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity specialists to assist with our response to the incident, and we notified law enforcement. On February 5, 2024, after an extensive forensic review, we determined that your personal information may have been affected.

**What Information Was Involved?**
Information that may have been affected includes your name and Social Security number.

**What Are We Doing and What Measures Have We Taken to Remedy the Situation?**
We consulted with third-party cybersecurity specialists to assist with our response to and remediation of the incident, and we notified law enforcement of the incident.

***What You Can Do***
To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.