

# **EXHIBIT A**

Filing # 126308305 E-Filed 05/06/2021 01:44:38 PM

IN THE CIRCUIT COURT FOR THE TWELFTH JUDICIAL  
CIRCUIT IN AND FOR SARASOTA COUNTY, FLORIDA

STEVEN K. FARMER,

on behalf of himself and all others  
similarly situated,

Plaintiff,

v.

HUMANA INC.,  
a Delaware corporation,

and

COTIVITI, INC.,  
a Delaware corporation,

Defendants.

Case No.:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Steven K. Farmer ("Plaintiff") brings this Class Action Complaint against Humana Inc. ("Humana") and Cotiviti, Inc. ("Cotiviti") (collectively, "Defendants"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

**I. INTRODUCTION**

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal and sensitive information that Cotiviti, with Humana's authorization and approval, collected from medical providers, including, without limitation, full Social Security numbers, partial Social Security numbers, names, dates of birth, addresses, cities, states, zip codes, phone numbers, email addresses, member identification numbers, subscriber identification numbers, dates of services, and/or dates of death (collectively, "personal identifiable information" or "PII") as well as provider names, medical record numbers, treatment related information, and/or

actual images (x-ray, photographs, etc.) (collectively, “protected health information” or “PHI”). Plaintiff also alleges Defendants failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former members of Humana (collectively, “Class Members”) that their PII and PHI had been exposed and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Humana provides medical benefit plans to approximately 17 million members. Humana’s members entrust Humana, either directly or through medical providers, with an extensive amount of their PII and PHI. Humana asserts that it understands the importance of protecting such information.

3. On or before December 22, 2020, Humana learned that PII and PHI for approximately 62,000 of its members had been exposed to unauthorized individuals through a personal “Google Drive” account (the “Data Breach”).

4. Humana determined that the Data Breach occurred because Cotiviti, with Humana’s authorization and approval, collected the PII and PHI from medical providers and then shared the PII and PHI with a subcontractor, “Visionary,” which, from October 12, 2020 through December 16, 2020, disclosed the PII and PHI to unauthorized individuals to promote a personal business endeavor.

5. More than two months later, in a “Notice of Privacy Incident,” dated March 1, 2021, Humana advised Plaintiff of the Data Breach.

6. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Humana admits that the unencrypted PII and PHI exposed to unauthorized individuals included names, Social

Security numbers, dates of birth, treatment related information, and/or actual images (x-ray, photographs, etc.

7. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and dates of birth.

8. This PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited more than two months to report it to the states' Attorneys General and affected individuals.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) ensure that the PII and PHI of Plaintiff and Class Members would be adequately safeguarded from misuse or exposure to unauthorized individuals whenever Defendants shared it with third parties. Defendants' conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendants'

conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

12. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

13. Plaintiff Steven Farmer ("Farmer") is a Citizen of Florida residing in Sarasota County, Florida. Mr. Farmer received Humana's *Notice of Privacy Incident*, dated March 1, 2021, on or about that date.<sup>1</sup> The notice stated that Plaintiff's full Social Security number, partial Social Security number, name, date of birth, address, city, state, zip code, phone number, email address,

---

<sup>1</sup> Ex. 1.

member identification number, subscriber identification number, date of service, date of death, provider name, medical record number, treatment related information, and actual images (x-ray, photographs, etc.) may have been exposed.<sup>2</sup>

14. Defendant Humana is a corporation organized under the laws of Delaware, headquartered at 500 West Main Street, Louisville, Kentucky, with its principal place of business in Louisville, Kentucky.

15. Defendant Cotiviti is a corporation organized under the laws of Delaware, headquartered at 10701 S River Front Pkwy, Unit 200, South Jordan, Utah, with its principal place of business in South Jordan, Utah.

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

17. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

### III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over Plaintiffs' claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of \$30,000.00 dollars, exclusive of interest and attorneys' fees.

19. The Court has personal jurisdiction over Defendants under Florida Stat. § 48.193, because Defendants personally or through their agents operated, conducted, engaged in, or carried on a business or business venture in Florida; Humana had offices in Florida; Defendants committed

---

<sup>2</sup> *Id.*

tortious acts in Florida; and Defendants breached an implied contract in Florida by failing to perform acts required by the contract to be performed in Florida.

20. Venue is proper in Sarasota County pursuant to Florida Stat. § 47.051 because Humana has an agent or other representative in Sarasota County and Sarasota County is where the cause of action accrued when Cotiviti, with Humana's authorization and approval, collected Plaintiff's PII and PHI from Plaintiff's medical provider(s) that treated Plaintiff in Sarasota County, Florida.

#### IV. FACTUAL ALLEGATIONS

##### *Background*

21. Humana provides medical benefit plans to approximately 17 million members. Cotiviti provides Humana quality and data reporting to the Centers for Medicare and Medicaid Services ("CMS"); as part of this, Cotiviti, with Humana's authorization and approval, collects medical records from health care providers to verify data reported to CMS. Cotiviti uses "Visionary" to review the medical records it collects for Humana for data reporting.

22. Plaintiff and Class Members entrusted Defendants with sensitive and confidential information, including full Social Security numbers, partial Social Security numbers, names, dates of birth, addresses, cities, states, zip codes, phone numbers, email addresses, member identification numbers, subscriber identification numbers, dates of services, dates of death, provider names, medical record numbers, treatment related information, actual images (x-ray, photographs, etc.), and other personal identifiable information, which include information that is static, does not change, and can be used to commit myriad financial crimes.

23. Plaintiff and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes

only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

24. Defendants had duties to adopt reasonable measures to protect the PII and PHI of Plaintiff and Class Members from involuntary disclosure to third parties.

### ***The Data Breach***

25. On or about March 1, 2021, Humana sent Plaintiff a *Notice of Privacy Incident*.<sup>3</sup> Humana informed Plaintiff that:

#### **What Happened**

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor, Visionary, inappropriately used their access to your information to disclose information, in the form of medical records, to unauthorized individuals in an effort to provide medical coding training to those individuals for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality and data reporting to Centers for Medicare and Medicaid Services (CMS). Cotiviti provides systems that allow Humana to contact health care providers and request medical records necessary to verify data reported to CMS. Cotiviti utilizes a subcontractor, Visionary, to review the collected medical records.

In the incident described above, the Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

\*\*\*

#### **What Information Was Involved**

The following information may have been included as part of the medical records involved in the incident:

---

<sup>3</sup> Ex. 1.

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

#### **What We Are Doing**

We preemptively shut down our systems to contain the incident and then undertook a secure, managed restoration. We also engaged a third-party cybersecurity firm to assist with our review and notified law enforcement and continue to cooperate with them. We have taken steps to further strengthen and enhance the security of systems in our network, including updating administrative and technical safeguards.<sup>4</sup>

26. On or about February 23, 2021, Humana notified various state Attorneys General, including Washington's Attorney General, of the Data Breach. Humana also provided the Attorneys General with "sample" notices of the Data Breach that suggest the information exposed in the Data Breach may include full Social Security numbers, partial Social Security numbers, names, dates of birth, addresses, cities, states, zip codes, phone numbers, email addresses, member identification numbers, subscriber identification numbers, dates of services, dates of death, provider names, medical record numbers, treatment related information, and actual images (x-ray,

---

<sup>4</sup> Ex. 1, p.1.

photographs, etc.).<sup>5</sup>

27. Humana admitted in the *Notice of Privacy Incident*, the letters to the Attorneys General, and the “sample” notices of the Data Breach that unauthorized third persons accessed files that contained sensitive information about Humana’s members, including names, Social Security numbers, dates of birth, treatment related information, and actual images.

28. In response to the Data Breach, Cotiviti has not claimed to undertake any remedial measures. Humana claims that it “has worked with Cotiviti to ensure it took immediate steps to enhance protections and ensure the safety and security of your information now and into the future. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.”<sup>6</sup> However, the deficiencies in the physical and technical safeguards at Cotiviti and Visionary have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

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

30. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 62,000 individuals.

***Cotiviti Acquires, Collects, Stores, and Shares the PII and PHI of Plaintiff and Class***

---

<sup>5</sup> Ex. 2.

<sup>6</sup> Exs. 1, 2.

*Members.*

31. Cotiviti, with Humana's authorization and approval, acquired, collected, and stored the PII and PHI of Plaintiff and Class Members and shared the PII and PHI with Visionary.

32. As a condition of membership with Humana, Humana requires that its members permit Humana to authorize Humana's vendors, such as Cotiviti, to collect the members' PII and PHI from health care providers.

33. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members and sharing it with Visionary, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

*Securing PII and PHI and Preventing Breaches*

35. Defendants could have prevented this Data Breach by ensuring that Cotiviti and Visionary had the appropriate technical safeguards in place prior to sharing the PII and PHI of Plaintiff and Class Members with Visionary.

36. Defendants' negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

37. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

38. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>7</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>8</sup>

39. The ramifications of Defendants’ failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information***

40. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>9</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>10</sup> Criminals can also purchase access to entire

<sup>7</sup> 17 C.F.R. § 248.201 (2013).

<sup>8</sup> *Id.*

<sup>9</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Apr. 26, 2021).

<sup>10</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Apr. 26, 2021).

company data breaches from \$900 to \$4,500.<sup>11</sup>

41. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>12</sup>

42. What is 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.

43. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

---

<sup>11</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Apr. 26, 2021).

<sup>12</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Apr. 26, 2021).

into the new Social Security number.”<sup>13</sup>

44. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number, name, and date of birth, and potentially government-issued ID number, mother’s maiden name, birth certificate, and biometric information.

45. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>14</sup>

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

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

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

[L]aw enforcement officials told us that in some cases, stolen data

<sup>13</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed Apr. 26, 2021).

<sup>14</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Apr. 26, 2021).

may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>15</sup>

49. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if the PII and PHI were not safeguarded, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

51. Defendants were, or should have been, fully aware of the unique type and the significant volume of data shared with Visionary, amounting to tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

52. To date, Defendants have offered Plaintiff and Class Members only two years of identity theft protection through a single credit bureau, Equifax. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

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

---

<sup>15</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Apr. 26, 2021).

PHI of Plaintiff and Class Members.

*Plaintiff Steven K. Farmer's Experience*

54. In or around January 2019, Plaintiff Steven K. Farmer became a Humana member through his Medicare Advantage Plan provided by the Kentucky Retirement System. As a condition of becoming a Humana member, Humana required that he provide his PII, including, but not limited to, his name, Social Security number, and date of birth.

55. Mr. Farmer received the Notice of Privacy Incident, dated March 1, 2021, on or about that date.

56. As a result of the Data Breach notice, Mr. Farmer spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Privacy Incident, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Humana, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

57. Additionally, Mr. Farmer is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

58. Mr. Farmer stores any documents containing his PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

59. Mr. Farmer suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Mr. Farmer entrusted to Defendants for the purpose of his Humana membership, which was compromised in and as a result of the Data Breach.

60. Mr. Farmer suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

61. Mr. Farmer has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in combination with his name and date of birth, being placed in the hands of unauthorized third parties and possibly criminals.

62. Mr. Farmer has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendants' possession, are protected and safeguarded from future breaches.

#### V. CLASS ALLEGATIONS

63. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure.

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

All individuals who reside in the United States and whose PII was compromised in the data breach that is the subject of the Notice of Privacy Incident that Humana sent to Plaintiff on or around March 1, 2021 (the "Nationwide Class").

65. Pursuant to Rule 1.220, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

All individuals who reside in Florida and whose PII was compromised in the data breach that is the subject of the Notice of Privacy Incident that Humana sent to Plaintiff on or around March 1, 2021 (the "Florida Class").

66. Excluded from the Classes are the following individuals and/or entities: Defendants and any Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

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

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

68. Numerosity, Fla. R. Civ. P. 1.220(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable. Humana has identified thousands of current and former Humana members whose PII and PHI may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records. Humana advised the U.S. Department of Health and Human Services that the Data Breach affected 62,950 individuals.

69. Commonality, Fla. R. Civ. P. 1.220(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendants had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendants had duties not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

70. Typicality, Fla. R. Civ. P. 1.220(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendants' misfeasance.

71. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to

the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

72. Adequacy, Fla. R. Civ. P. 1.220(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

73. Superiority and Manageability, Fla. R. Civ. P. 1.220(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

74. The nature of this action and the nature of laws available to Plaintiff and Class

Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

75. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

76. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

77. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and PHI of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

78. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 1.220(b)(2) of the Florida Rules of Civil Procedure.

79. Likewise, particular issues under Rule 1.220(d)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendants breached the implied contract;
- f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,
- i. Whether Class Members are entitled to actual damages, statutory damages,

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

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

80. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

81. As a condition of their membership with Humana, Humana's current and former members were obligated to entrust Defendants with certain PII and PHI, including their names, Social Security numbers, and dates of birth.

82. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

83. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

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

85. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

Defendants' security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

86. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former members' PII and PHI they were no longer required to retain pursuant to regulations.

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

88. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendants with their confidential PII and PHI, a necessary part of membership with Humana.

89. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Nationwide Class.

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

91. Plaintiff and the Nationwide Class were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting, storing, and sharing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI before sharing them and ensuring they were encrypted when stored on Defendants' systems or the systems of any entity with which Defendants shared the PII and PHI.

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

93. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

94. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

95. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendants' possession, custody, or control might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

96. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

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

98. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide

Class during the time the PII and PHI was within Defendants' possession, custody, or control.

99. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

101. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of Humana's current and former members' PII and PHI.

102. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove Humana's former members' PII and PHI they were no longer required to retain pursuant to regulations.

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

104. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

105. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendants'

failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

106. Additionally, Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendants’ duty in this regard.

107. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendants’ conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

108. Defendants’ violation of Section 5 of the FTC Act constitutes negligence *per se*.

109. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

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

111. As a direct and proximate result of Defendants’ negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated

with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession, custody and control and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

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

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

**COUNT II**  
**BREACH OF IMPLIED CONTRACT - HUMANA**  
**(On Behalf of Plaintiff and the Nationwide Class)**

114. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

115. Humana required Plaintiff and the Nationwide Class to provide and entrust their personal information to Humana, including full Social Security numbers, partial Social Security numbers, names, dates of birth, addresses, cities, states, zip codes, phone numbers, email addresses, member identification numbers, subscriber identification numbers, dates of services, dates of death, provider names, medical record numbers, treatment related information, and/or actual images (x-ray, photographs, etc.).

116. As a condition of their membership with Humana, Plaintiff and the Nationwide Class provided their personal information. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Humana by which Humana agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

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

118. Humana breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the data breach.

119. As a direct and proximate result of Humana's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing,

imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

**COUNT III**  
**INVASION OF PRIVACY**  
**(On Behalf of Plaintiff and the Nationwide Class)**

120. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

121. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

122. Defendants owed a duty to Humana's current and former members, including Plaintiff and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

123. Defendants failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

124. Defendants allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendants' failure to protect the PII and PHI.

125. The unauthorized release to, custody of, and examination by unauthorized third

parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

126. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendants as part of the current and former members' membership with Humana, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

127. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

128. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that their information security practices were inadequate and insufficient.

129. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

130. As a proximate result of the above acts and omissions of Defendants, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

131. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the

Nationwide Class in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

**COUNT IV**  
**BREACH OF CONFIDENCE**  
**(On Behalf of Plaintiff and the Nationwide Class)**

132. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

133. At all times during Plaintiff's and the Nationwide Class's interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class entrusted to Humana as its members.

134. As alleged herein and above, Defendants' relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

135. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

136. Plaintiff and the Nationwide Class also entrusted their PII and PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII and PHI from unauthorized disclosure.

137. Defendants voluntarily received in confidence Plaintiff's and the Nationwide Class's PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

138. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Nationwide Class's PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without their express permission.

139. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

140. But for Defendants' disclosure of Plaintiff's and the Nationwide Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the unauthorized disclosure of Plaintiff's and the Nationwide Class's PII and PHI as well as the resulting damages.

141. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and the Nationwide Class's PII and PHI. Defendants knew or should have known their methods of accepting and securing Plaintiff's and the Nationwide Class's PII and PHI were inadequate as they relate to, at the very least, ensuring their vendors entrusted with the PII and PHI properly safeguard it.

142. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI of current and former Humana members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

143. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

#### **COUNT V**

#### **Violation of the Florida Deceptive and Unfair Trade Practices Act, (Fla. Stat. §§ 501.201, *et seq.*) (On Behalf of Plaintiff and the Florida Class)**

144. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

145. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendants obtained Plaintiffs' and Florida Class members' PII and PHI through advertising, soliciting, providing, offering, and/or distributing

goods and services to Plaintiffs and Florida Class members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

146. As alleged herein this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

- a. failure to implement adequate data security practices to safeguard PII and PHI;
- b. failure to make only authorized disclosures of current and former members' PII and PHI;
- c. failure to disclose that their data security practices were inadequate to safeguard PII and PHI from theft; and
- d. failure to timely and accurately disclose the Data Breach to Plaintiffs and Florida Class members.

147. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Humana's current and former members.

148. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Humana's current and former members that they did not follow industry best practices for the collection, use, and storage of PII and PHI.

149. As a direct and proximate result of Defendants' conduct, Plaintiff and Florida Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs

associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

150. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Florida Class members have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

151. Also as a direct result of Defendants' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Florida Class members are entitled to damages as well as injunctive relief, including, but not limited to:

- a. Ordering that Defendants implement measures that ensure that the PII and PHI of Humana's current and former members is appropriately encrypted and safeguarded when shared with any other entity, including to the extent they are currently shared;
- b. Ordering that Defendants purge, delete, and destroy in a reasonable secure manner PII and PHI not necessary for their provision of services;
- c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- d. Ordering Defendant to meaningfully educate Humana's current and former members about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps Humana's current and former members must take to protect themselves.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

- A. For an Order certifying the Nationwide Class and the Florida Class and appointing Plaintiff and their Counsel to represent each such Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
  - iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII

and PHI of Plaintiff and Class Members;

- v. requiring Defendants to ensure that appropriate safeguards are in place when sharing PII or PHI with other entities, including vendors or subcontractors;
- vi. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;
- vii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- viii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- ix. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information; and
- x. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals

must take to protect themselves.

- D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

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

Date: May 6, 2021

Respectfully Submitted,

/s/ John A. Yanchunis

John A. Yanchunis

Ryan D. Maxey

**MORGAN & MORGAN COMPLEX  
LITIGATION GROUP**

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

(813) 223-5505

jyanchunis@ForThePeople.com

rmaxey@ForThePeople.com

*Attorneys for Plaintiff and the Proposed Class*

# EXHIBIT 1

HUMANA INC  
PRIVACY OFFICE  
101 E MAIN STREET  
LOUISVILLE KY 40202

March 1, 2021

Humana

RE: [REDACTED]

NOTICE OF PRIVACY INCIDENT

Dear Steven K Farmer:

Equifax Activation Code: [REDACTED]

We are writing to notify you, a valued member, of a recent incident involving unauthorized access to some of your personal information. While we do not think your personal information will be used inappropriately because of this incident, we want to share with you the steps we have taken to safeguard your personal information.

**What Happened?**

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor, Visionary, inappropriately used their access to your information to disclose information, in the form of medical records, to unauthorized individuals in an effort to provide medical coding training to those individuals for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality and data reporting to Centers for Medicare and Medicaid Services (CMS). Cotiviti provides systems that allow Humana to contact health care providers and request medical records necessary to verify data reported to CMS. Cotiviti utilizes a subcontractor, Visionary, to review the collected medical records.

In the incident described above, the Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

Humana requires executed Business Associate Agreements with all organizations that perform any services on our behalf involving our members' protected health information. This Business Associate Agreement requires Cotiviti to comply with federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations and to follow guidelines and policies established by Humana in maintaining the privacy and confidentiality of all protected health information. We also conduct assessments of our business associates to verify that processes are being followed. Similarly, Cotiviti has executed Business Associate Agreements

PRVC100010620v1  
180/81030001470010100

Humana.com



With their subcontractors that holds them to these same standards.

#### **What Information Was Involved?**

The following information may have been included as part of the medical records involved in the incident:

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

#### **What Are We Doing?**

Humana is committed to safeguarding your personal information. Humana has worked with Cotiviti to ensure it took immediate steps to enhance protections and ensure the safety and security of your information now and into the future. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.

Upon discovery, Visionary immediately disabled the access of the now former employee for both Visionary and Cotiviti systems. Visionary implemented a broad containment strategy to prevent any information that was subject to unauthorized disclosure, due to this incident, from further unauthorized disclosure. Both Visionary and Cotiviti launched a comprehensive investigation into the incident and hired cybersecurity firms to assist in the efforts.

#### **We know that you may be worried about what took place.**

To help relieve concerns and restore confidence following this incident, we have partnered with Equifax® to provide its Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product to you for two years. There is no cost for the service. A description of this product and instructions about how to enroll were included with the letter you received.

We strongly encourage you to enroll in this no cost service to protect yourself from the potential misuse of your information.

#### What You Can Do

We do not think your personal information will be used inappropriately because of the incident that took place. However, we ask you to remain vigilant. There are steps you can take to protect yourself. Review the following for suspicious activity:

- Explanation of Benefit (EOB) letters
- SmartSummary Statements
- Medical Records
- Account Statements and Credit Reports

Watch for services you did not receive or accounts you did not open. If you find unfamiliar activity on the statements you receive from Humana, please notify us immediately. Keep a copy of this notice in case of future problems with your medical records.

If you see suspicious activity on your credit report, call your local police office to file a report for identity theft. Get a copy of the report. Details are enclosed to obtain additional information from the Federal Trade Commission (FTC) and consumer reporting agencies. You can learn to place a fraud alert and/or security freeze on your account.

#### For More Information

Do you have any questions or need help with anything mentioned in this letter? Please contact us at 1-800-457-4708. If you have a speech or hearing impairment and use a TTY, call 1-800-833-3301.

Again, please accept our sincere apology for this incident. We value your membership and work hard to protect your information.

Sincerely,



Jim Theiss  
Chief Privacy Officer  
Humana, Inc.  
Privacy Office

Enclosures



# EXHIBIT 2

HUMANA INC  
PRIVACY OFFICE  
101 E MAIN STREET  
LOUISVILLE KY 40202

Humana

February 23, 2021

Attorney General  
SecurityBreach@atg.wa.gov

RE: Case 283533

### NOTICE OF PRIVACY INCIDENT

Dear Attorney General;

The purpose of this letter is to notify your office of a recent privacy incident that occurred and impacted residents of your state. First, let me state that Humana takes all privacy concerns seriously and is taking appropriate steps to prevent errors such as this in the future.

#### What Happened?

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor inappropriately used their access to individual information to disclose information, in the form of medical records, to unauthorized individuals in an effort to train medical coders for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality reporting and risk adjustment purposes. Risk adjustment is required of Medicare Advantage plans, like Humana, by the federal Medicare agency, the Centers for Medicare and Medicaid Services (CMS). By risk adjusting plan payments, CMS is able to make appropriate and accurate payments for enrollees with differences in expected costs. Cotiviti provides systems that allow Humana to contact health care providers and request medical records for this process.

Cotiviti utilizes a subcontractor, Visionary. A Visionary employee was attempting to train unauthorized individuals on how to conduct Medicare Risk Adjustment coding as part of a personal business endeavor. The Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

Humana requires executed Business Associate Agreements with all organizations that perform any services on our behalf involving our member's protected health information. This Business Associate Agreement requires Cotiviti to comply with federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations and to follow guidelines and policies established by Humana in maintaining the privacy and confidentiality of all protected health information. We also conduct assessments of our business associates to verify that processes

are being followed. Similarly, Cotiviti has executed Business Associate Agreements with their subcontractors that holds them to these same standards

#### **What Information Was Involved?**

The following information may have been included as part of the medical records involved in the incident:

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

#### **What Are We Doing?**

On February 25, 2021, notification letters will be sent to 675 residents of your state who were impacted by this situation. Attached you will find a copy of the letter that includes an application for free credit monitoring and free identity theft protection for two years. There is no cost to the individuals for this service.

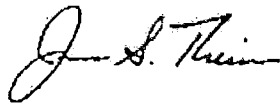
We deeply regret this incident, but want to assure you that Humana has safeguards to protect individual information including policies, procedures and technical safeguards. As a result of this incident Humana has worked with Cotiviti to ensure immediate steps were taken to enhance protections and ensure the safety and security of individual's information. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.

Upon discovery, Visionary immediately disabled the access of the now former employee into Visionary and Cotiviti systems. Visionary implemented a broad containment strategy to prevent any information that was subject to unauthorized disclosure, due to this incident, from further unauthorized disclosure. Both Visionary and Cotiviti launched a comprehensive investigation into the incident and hired cybersecurity firms to assist in the efforts.

Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,

A handwritten signature in black ink, appearing to read "James S. Theiss". The signature is fluid and cursive, with the first name "James" and last name "Theiss" clearly distinguishable.

James S. Theiss  
Chief Privacy Officer  
Humana Inc.  
502-580-4322  
[jtheiss@humana.com](mailto:jtheiss@humana.com)

Enclosures

HUMANA INC  
PRIVACY OFFICE  
101 E MAIN STREET  
LOUISVILLE KY 40202

Humana

February 25, 2021

FIRSTNAME LASTNAME  
ADDR1 ADDR2  
CITY STATE ZIP

RE: 283533

## NOTICE OF PRIVACY INCIDENT

Equifax Activation Code: xxxxxxxxxxxx

Dear FIRSTNAME LASTNAME;

We are writing to notify you, a valued member, of a recent incident involving some of your personal information.

### What Happened?

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor inappropriately used their access to your information to disclose information, in the form of medical records, to unauthorized individuals in an effort to train medical coders for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality reporting and risk adjustment purposes. Risk adjustment is required of Medicare Advantage plans, like Humana, by the federal Medicare agency, the Centers for Medicare and Medicaid Services (CMS). Cotiviti provides systems that allow Humana to contact health care providers and request medical records for this process.

Cotiviti utilizes a subcontractor, Visionary. A Visionary employee was attempting to train unauthorized individuals on how to conduct Medicare Risk Adjustment coding as part of a personal business endeavor. The Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

Humana requires executed Business Associate Agreements with all organizations that perform any services on our behalf involving our members' protected health information. This Business Associate Agreement requires Cotiviti to comply with federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations and to follow guidelines and policies established by Humana in maintaining the privacy and confidentiality of all protected health information. We also conduct assessments of our business associates to verify that processes are being followed. Similarly, Cotiviti has executed Business Associate Agreements with their subcontractors that holds them to these same standards.

PRVCY0001r0620v1

Humana.com

### **What Information Was Involved?**

The following information may have been included as part of the medical records involved in the incident:

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

### **What Are We Doing?**

Humana is committed to safeguarding your personal information. Humana has worked with Cotiviti to ensure it took immediate steps to enhance protections and ensure the safety and security of your information now and into the future. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.

Upon discovery, Visionary immediately disabled the access of the now former employee for both Visionary and Cotiviti systems. Visionary implemented a broad containment strategy to prevent any information that was subject to unauthorized disclosure, due to this incident, from further unauthorized disclosure. Both Visionary and Cotiviti launched a comprehensive investigation into the incident and hired cybersecurity firms to assist in the efforts.

### **We know that you may be worried about what took place.**

To help relieve concerns and restore confidence following this incident, we have partnered with Equifax® to provide its Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product to you for two years. There is no cost for the service. A description of this product and instructions about how to enroll were included with the letter you received.

We strongly encourage you to enroll in this no cost service to protect yourself from the potential misuse of your information.

### What You Can Do

We do not think your personal information will be used inappropriately because of the incident that took place. However, we ask you to remain vigilant. There are steps you can take to protect yourself. Review the following for suspicious activity:

- Explanation of Benefit (EOB) letters
- SmartSummary Statements
- Medical Records
- Account Statements and Credit Reports

Watch for services you did not receive or accounts you did not open. If you find unfamiliar activity on the statements you receive from Humana, please notify us immediately. Keep a copy of this notice in case of future problems with your medical records.

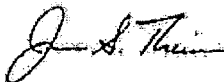
If you see suspicious activity on your credit report, call your local police office to file a report for identity theft. Get a copy of the report. Details are enclosed to obtain additional information from the Federal Trade Commission (FTC) and consumer reporting agencies. You can learn to place a fraud alert and/or security freeze on your account.

### For More Information

Do you have any questions or need help with anything mentioned in this letter? Please contact us at 1-800-457-4708. If you have a speech or hearing impairment and use a TTY, call **1-800-833-3301**.

Again, please accept our sincere apology for this incident. We value your membership and work hard to protect your information.

Sincerely,



Jim Theiss  
Chief Privacy Official  
Humana, Inc.  
Privacy Office

Enclosures

### Identity Theft Guide

You are advised to report any suspected identity theft to law enforcement. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

In addition, the Federal Trade Commission suggests the following:

1. **Fraud Alert.** Contact the toll-free number of any of the three consumer reporting companies below to place a fraud alert on your file. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two companies. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but delay you when you seek to obtain credit. Under federal law, you may place a fraud alert on your file free of charge.

<b>Equifax</b> P.O. Box 740256 Atlanta, GA 30348  <b>1-800-685-1111</b> <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013  <b>1-888-EXPERIAN or</b> <b>1-888-397-3742</b> <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016  <b>1-800-916-8800</b> <a href="http://www.transunion.com">www.transunion.com</a>
---	--	--

2. **Free Credit Report.** You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit-reporting agencies. To order your annual free credit report please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1- 877-322-8228. Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Services, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Contact the Federal Trade Commission and your state Attorney General.** If you believe you are the victim of identity theft or your personal information has been misused, you can contact the Attorney General's Office in your home state and/or the Federal Trade Commission at 1- 877-ID-THEFT, (1-877-438-4338) or by visiting the Federal Trade Commission website at

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**For residents of Maryland:** You may also obtain information about identity theft prevention from the:

**Maryland Office of the Attorney General**

Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202 1-

888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For residents of North Carolina:** You may also obtain information about identity theft prevention from the:

**North Carolina Attorney General's Office**

Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001

1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

**For residents of Rhode Island:** You may also obtain information about identity theft prevention from the:

**Office of the Rhode Island Attorney General**

Consumer Protection Unit 150 South Main Street

Providence, Rhode Island 02903

(401) 274-4400, [consumers@riag.ri.gov](mailto:consumers@riag.ri.gov)

**Security Freeze:** You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail to Equifax, Experian and TransUnion at the addresses above. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information above.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.





**About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product**

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian, and TransUnion** credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to \$1 million in identity theft insurance<sup>1</sup> with \$0 deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert<sup>2</sup> placement with automatic renewal functionality\* (available online only)

**How to Enroll: You can sign up online or over the phone**

To sign up online for **online delivery** go to [www.myservices.equifax.com/tri](http://www.myservices.equifax.com/tri)

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

**Directions for placing a Fraud Alert**

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit:

[www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com) or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

1 - Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age)

2 - The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

GCHJV5REN 0117