IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

HERIBERTO CASTILLO, individually and on behalf of all others similarly situated **Plaintiff,** **v.** **ILLINOIS GASTROENTEROLOGY GROUP, P.L.L.C.,** **Defendant.**	**No.** **CIVIL ACTION – CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Heriberto Castillo ("Plaintiff), individually and on behalf of the Class defined below of similarly situated persons, brings this Class Action Complaint against Illinois Gastroenterology Group, P.L.L.C. ("IGG" or "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against IGG for IGG's failure to properly secure and safeguard protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), personally identifiable information including names, addresses, and Social Security numbers, driver's licenses, Passports, financial account information, payment card information, employer-assigned identification numbers, (collectively, "personally identifiable information" or "PII"),[1] and other biometric data ("protected biometric information" or "PBI").

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number). PHI contains PII and PBI.

2. IGG is a medical center that was formed in 2010 and is the largest single specialty gastroenterology group in Illinois, with over 40 gastroenterologists.[2]

3. On October 22, 2021, Defendant discovered unusual activity within its computer network (the "Data Breach").[3] Defendant launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event.

4. On November 18, 2021, the investigation determined that an unauthorized actor gained access to Defendant's systems and that information contained in those systems may have been viewed or taken by the unauthorized actor.[4]

5. On March 22, 2022, approximately five months after Data Breach was confirmed, Defendant "determined the personal information of individuals including the following types of information that IGG maintains in its systems and that were, or may have been, impacted by this incident include: name, address, date of birth, Social Security number, driver's licenses, passports,[5] financial account information, payment card information, employer-assigned identification numbers, medical information, and biometric data." [3]

6. On April 22, 2022, Defendant reported to the Department of Health and Human Services that 227,943 individuals' unencrypted information had been compromised in the Data Breach.

7. By obtaining, collecting, using, and deriving a benefit from the PII, PHI, PBI of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits

---

[2] https://www.illinoisgastro.com/about (last visited May 24, 2022).
[3] Exhibit 1 ("Website Notice"), *available at* https://www.prnewswire.com/news-releases/illinois-gastroenterology-group-pllc-provides-notice-of-a-security-incident-301531255.html (last visited May 23, 2022).
[4] *Id.*
[5] Due to a vagueness in Defendant's reporting, it remains unclear whether the unauthorized actor obtained actual copies of Plaintiff and Class Members' driver's licenses and passports, to include their photographs, or whether this information was limited to driver's license and passport numbers.

that the unencrypted PII, PHI, and PBI impacted during the Data Breach included names, addresses, dates of birth, Social Security numbers, driver's licenses, passports, financial account information, payment card information, employer-assigned identification numbers, medical information, and biometric data.

8. The exposed PII, PHI, and PBI of Plaintiff and Class Members can now forever be misused by the hackers, including offering the unencrypted, unredacted PII, PHI, and PBI for sale on the dark web. Plaintiff and Class Members now face a present and continuing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

9. This PII, PHI, and PBI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the sensitive and personal information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the Breach, Defendant waited several months to report it to government agencies and affected individuals.

10. Upon information and belief, Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information. Further, this is not Defendant's first breach of sensitive patient information. According to public reporting, in 2019, IGG reported a hacking incident involving email that impacted 1,481 patients. Whether that attack shared any common vulnerability or vulnerabilities with the recent attack is unknown to Plaintiff and Class Members.[6]

11. As a result of IGG's delayed response, Plaintiff and Class Members had no idea their PII, PHI, and PBI had been compromised, and that they were, and continue to be, at

[6] https://www.databreaches.net/illinois-gastroenterology-group-is-providing-notification-of-breach-first-discovered-last-october/ (last visited May 23, 2022).

significant risk of identity theft and various other forms of personal, social, and financial harm. The risk is present and continuing.

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

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII, PHI, and PBI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, PHI, and PBI; (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 substantially increased risk to their PII, PHI, and PBI which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII, PHI, and PBI.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII, PHI, and PBI 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, PHI, and PBI 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

15. Plaintiff Heriberto Castillo is a citizen of Illinois residing in Cook County, Illinois.

16. Defendant Illinois Gastroenterology Group, P.L.L.C., is a corporation organized under the laws of Illinois, headquartered at 20 Tower Ct., Gurnee, Illinois, with its principal place of business in Gurnee, Illinois.

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

III. JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d). This is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

19. The Northern District of Illinois has personal jurisdiction over Defendant named in this action because Defendant and/or their parents or affiliates are headquartered in this District and Defendant conducts substantial business in Illinois and this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant Illinois Gastroenterology Group ("Defendant" or "IGG") is a healthcare practice made up of gastroenterologists and related medical providers. [7]

22. IGG was created through the merger of Elgin Gastroenterology, Lake Shore Gastroenterology, and Northwest Gastroenterologists in 2010. In subsequent years, the Midwest Center for Digestive Health, Gastrointestinal Health Associates of Geneva, and North Shore Gastroenterology joined the organization.[8]

23. Currently, IGG has 40 gastroenterologists that treat patients at 32 clinics located throughout Illinois. Illinois Gastroenterology Group employs more than 200 people and generates approximately $37 million in annual revenue.[9]

24. As a condition of obtaining healthcare from Defendant, Plaintiff and Class Members directly or indirectly entrusted Defendant with a massive amount of sensitive information, including their PII, PHI, and/or PBI, which included information that is static, does not change, and can be used to commit myriad financial crimes. This information also included highly confidential medical information.

25. Plaintiff and Class Members relied on Defendant to keep their PII, PHI, and PBI confidential and securely maintained, to use this information for business purposes only, and to

[7] *Illinois Gastroenterology Group, PLLC Announces Data Breach*, JDSUPRA (May 26, 2022) https://www.jdsupra.com/legalnews/illinois-gastroenterology-group-pllc-6300926/ (last visited May 23, 2022).
[8] *Id.*
[9] *Id.*

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

26. Defendant had a duty to adopt reasonable measures to protect the PII, PHI, and PBI of Plaintiff and Class Members from involuntary disclosure to third parties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII, PHI, and PBI from disclosure.

27. Defendant's Notice of Privacy Practices ("Privacy Policy") states, "Protecting the privacy of healthcare information is a responsibility we take very seriously. We understand that healthcare information is personal and the importance of keeping it confidential. We are committed to our established practices and procedures to protect the confidential nature of your healthcare information." [10]

28. Defendant's Privacy Policy further states, "We are required by law to maintain the privacy of your health information and provide you notice of our legal duties and privacy practices with respect to your health information. We will abide by the terms of this Notice."[11]

29. If Defendant stated that it would not abide by its privacy policies, Plaintiff and the other Class Members would have declined treatment with Defendant and not provided their PHI, PII, and PBI to Defendant.

30. On April 22, 2022, Defendant notified PRNewswire of the Data Breach ("Notice of Data Breach").[12] Defendant advised that the information potentially impacted in the Data Breach included names, addresses, dates of birth, Social Security numbers, driver's licenses,

[10] Exhibit 2 (Notice of Privacy Practices).
[11] *Id.*
[12] *Illinois Gastroenterology Group, PLLC Provides Notice of a Security Incident,* https://www.prnewswire.com/news-releases/illinois-gastroenterology-group-pllc-provides-notice-of-a-security-incident-301531255.html (last visited May 24, 2022).

passports, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data.

31. The Notice of Data Breach stated, in relevant part, the following:

> Illinois Gastroenterology Group, PLLC ("IGG") is providing notice of a recent incident that may affect the security of certain individuals' information.
>
> On October 22, 2021, IGG discovered unusual activity within its computer network. Defendant immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. On November 18, 2021, the investigation determined that an unauthorized actor gained access to certain IGG systems and that information contained in those systems may have been viewed or taken by the unauthorized actor.
>
> IGG reviewed the information contained within the systems to identify if any individuals' personal information or protected health information was potentially impacted. On March 20, 2022, IGG determined personal information of individuals including the following types of information that IGG maintains in its system and that were, or may have been, impacted by this incident include: name, address, date of birth, Social Security number, driver's licenses, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data. To date, IGG has not received any reports of fraudulent misuse of any information potentially impacted.
>
> IGG takes this incident and the security of personal information in its care seriously. IGG moved quickly to investigate and respond to this incident, assess the security of its systems, and notify potentially affected individuals. In response to this incident, IGG augmented its policies and procedures addressing network security. IGG accelerated the implementation of an enhanced managed Security Operations Center including the deployment of an endpoint detection and response platform in response to this event with policies enabled specifically for ransomware. IGG immediately reset passwords and employees with privileged access to sensitive systems were enrolled into our multifactor authentication platform. IGG is also notifying potentially affected individuals so that they

> may take further steps to protect their information, should they feel it is appropriate to do so.[13]

32. Defendant admitted in the Notice of Data Breach that unauthorized third persons accessed files that contained Plaintiff's and Class's Members' PII, PHI, and PBI.

33. The unencrypted PII, PHI, and PBI of Plaintiff and Class Members is in the hands of criminals where it is and will be misused. In addition to identity theft, the detailed PII, PHI, and PBI may be used for targeted solicitation and fraud upon Plaintiff and Class Members.

34. Following the Breach and admitting that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members identity theft protection for only twelve months through Experian.

35. 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, PHI, and PBI at issue here. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

Securing PII, PHI, and PBI and Preventing Breaches

36. Defendant 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, PHI, and PBI.

37. IGG could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII, PHI, and PBI of Plaintiff and Class Members. Alternatively, IGG could have destroyed the data, especially outdated information.

[13] *Id.*

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

39. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] 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."[15]

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

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

42. Notably, Defendant has a history of allowing breaches to the confidentiality of patient information. According to public reporting, in 2019, IGG reported a hacking incident involving email that impacted 1,481 patients.[16] Defendant had or should have had a heightened awareness of the prevalence of data breaches in the healthcare industry.

---

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] https://www.databreaches.net/illinois-gastroenterology-group-is-providing-notification-of-breach-first-discovered-last-october/ (last visited May 23, 2022).

43. Upon information and belief, as suggested by Defendant's Notice of Data Breach, the Data Breach was the result of a ransomware attack. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[17]

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read

[17] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited May 24, 2022).

specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

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

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

45. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often

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

> appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
>
> - **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
>
> - **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[19]

46. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;

[19] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited May 24, 2022).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[20]

47. Given that Defendant was storing the PII, PHI, and PBI of Plaintiff and Class Members, Defendant could and as required by law should have implemented all of the above measures to prevent and detect ransomware attacks.

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

[20] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited May 24, 2022).

The Healthcare Industry is Particularly Susceptible to Data Breaches

49. Defendant was on notice that companies in the healthcare industry are targets for data breaches, especially since IGG experienced a previous breach of private information in 2019.

50. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[21]

51. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[22]

52. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[23] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay

---

[21] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited May 24, 2022).

[22] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited May 24, 2022).

[23] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited May 24, 2022).

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[24] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[25]

53. In the context of data breaches, healthcare is "by far the most affected industry sector."[26] Further, breaches of cybersecurity in the healthcare industry are particularly devastating, given the frequency of breaches and the fact that healthcare providers maintain highly sensitive and detailed PII and PHI.[27] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[28]

54. Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[29] Indeed, shortly before Defendant announced the Data Breach, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[30]

---

[24] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited May 24, 2022).
[25] *Id.*
[26] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches
[27] *See id.*
[28] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (emphasis added).
[29] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/.
[30] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said

IGG's Conduct Violates The Rules and Regulations of HIPAA and HITECH

55. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

56. IGG's Data Breach resulted from a combination of insufficiencies that indicate IGG failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from IGG's Data Breach that IGG either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff's and Class Members' PHI.

57. Defendants are covered entities pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

58. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH")[31]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

59. Plaintiff's and Class Members' Personal and Medical Information is "protected health information" as defined by 45 CFR § 160.103.

reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

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

60. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

61. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

62. Plaintiff's and Class Members' Personal and Medical Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

63. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

64. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

65. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

66. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

67. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

68. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

69. In addition, IGG's Data Breach could have been prevented if IGG implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

70. IGG's security failures also include, but are not limited to: (a) failing to maintain an adequate data security system to prevent data loss; (b) failing to mitigate the risks of a data breach and loss of data; (c) failing to ensure the confidentiality and integrity of electronic protected health information IGG creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1); (d) failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1); (e) failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1); (f) failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii); (g) failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2); (h)

failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3); (i) failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94); and (j) impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

71. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

1. the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
2. the recipient of the PHI;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[32]

[32] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304.

72. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required IGG to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[33]

73. Because IGG has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure IGG's approach to information security is adequate and appropriate. IGG still maintains the protected health information and other sensitive information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff and Class Members' PHI remains at risk of subsequent Data Breaches.

IGG failed to protect Plaintiff's and Class Members' PBI

74. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing, yet unregulated technology. *See* 740 ILCS 14/5.

75. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which are unique biometric identifiers that can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate

[33] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Apr. 5, 2022).

protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

76. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to disclose information unless: "(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." ILCS 740 14/15(d)(1)-(4).

77. BIPA also states that "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers, and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." ILCS 740 14/15(d)(1)-(4).

78. Defendant violated ILCS 740 14/15(d)(1)-(4) because it disclosed or disseminated Plaintiff's and Class Members' PBI without authorization or under the approved exceptions.

79. As a result of the Data Breach, Defendant violated ILCS 740 14/15(e) because it failed to protect Plaintiff's and Class Members' PBI within the industry standard and failed to protect PBI the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

80. Defendant was negligent in unlawfully disclosing and failing to protect Plaintiff's and Class Members' PBI.

81. Defendant was reckless in unlawfully disclosing and failing to protect Plaintiff's and Class Members' PBI.

82. Defendant was intentional in unlawfully disclosing and failing to protect Plaintiff's and Class Members' PBI.

83. As a direct result of the Data Breach, Plaintiff and Class Members have suffered substantial harm due to the unlawful disclosure of their PBI.

84. As a direct of the Data Breach, Defendant has harmed Plaintiff and Class Members by failing to protect PBI from unauthorized third parties.

Value of PII, PHI, and PBI

85. 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.[34] Experian reports that a stolen credit or debit

[34] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs/ (last visited May 24, 2022).

card number can sell for $5 to $110 on the dark web.[35] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[36]

86. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety offraudulent 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.[37]

87. 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.

---

[35] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask- experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark- web/ (last visited May 24, 2022).

[36] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 24, 2022).

[37] 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 visited May 24, 2022).

88. 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 into the new Social Security number."[38]

89. 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—name and Social Security number.

90. 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, black market."[39]

91. 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.

92. The PII, PHI, and PBI of Plaintiff and Class Members was accessed by, disclosed to, and/or acquired by hackers to engage in identity theft or and or to sell it to other criminals who will misuse the PII, PHI, and PBI for identity theft and fraud. The fraudulent activity resulting from the Data Breach may not come to light for years.

[38] 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 visited May 24, 2022).

[39] 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 visited May 24, 2022).

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[40]

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

95. 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, PHI, and PBI.

96. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

97. Following the Breach and admitting that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members identity theft protection for only twelve months through Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come,

[40] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited May 24, 2022).

particularly in light of the PII, PHI, and PBI at issue here. As another element of damages. Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

98. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[41]

99. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[42] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[43] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

[41] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited May 23, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, available at* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last visited May 23, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.)

[42] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited May 23, 2022).

[43] *Id.*

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

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

Plaintiff's Experiences

102. Plaintiff Castillo was a patient of Defendant in 2019. As a condition of that relationship, Plaintiff was required to provide and entrust his PII, PHI, and PBI to Defendant.

103. Plaintiff received Defendant's Notice of Data Breach on or about May 5, 2022. The notice indicated that Plaintiff's private information was among the information accessed or acquired during the Data Breach.

104. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts for unusual activity. This time has been lost forever and cannot be recaptured. This time was spent at Defendant's direction. In particular, Defendant indicated in its Notice of Data Breach that Plaintiff should spend time to protect his identity in order to mitigate his losses.

105. Plaintiff is very careful about sharing his sensitive PII, PHI, and PBI. He has never knowingly transmitted unencrypted sensitive PII, PHI, and PBI over the internet or any other unsecured source.

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

107. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII, PHI, and PBI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff 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.

108. Plaintiff is suffering present and continuing injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, PHI, and PBI being placed in the hands of unauthorized third parties and possibly criminals.

109. Plaintiff has a continuing interest in ensuring that his PII, PHI, and PBI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

III. CLASS ALLEGATIONS

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

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

> All United States residents whose PII, PHI, and/or PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 22, 2022 (the "Nationwide Class").

112. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All Illinois residents whose PII, PHI, and/or PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 22, 2022 (the "Illinois Class").

113. In addition to the Nationwide and Illinois Classes, Plaintiff asserts claims on behalf of a separate subclass defined as follows:

> All United States residents whose PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around April 22, 2022 (the "PBI Class").

114. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff,

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

116. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide, Illinois, and PBI class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds, if not thousands, of individuals whose PII, PHI and/or PBI may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

117. Commonality, Fed. R. Civ. P. 23(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 Defendant had a duty to protect the PII, PHI, and PBI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII, PHI, and PBI of Plaintiff and Class Members to unauthorized third parties; Whether Defendant had duties not to use the PII, PHI, and PBI of Plaintiff and Class Members for non-business purposes;

c. Whether Defendant failed to adequately safeguard the PII, PHI, and PBI of Plaintiff and Class Members;

d. Whether and when Defendant actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

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

h. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

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

j. Whether Defendant violated the consumer protection statutes invoked herein;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Defendant unlawfully disclosed and/or disseminated Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15(d)(1)-(4);

m. Whether Defendant failed to protect Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15(e); Whether Defendant was negligent, intentional, or reckless in unlawfully disclosing and/or failing to protect Plaintiff's and Class Members' PBI;

n. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

o. 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.

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

119. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members

uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

120. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has 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 Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

121. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

122. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since 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 were 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.

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

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

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

126. Further, Defendant has 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 23(b)(2) of the Federal Rules of Civil Procedure.

127. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security; Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

d. Whether Defendant breached the implied contract;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

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

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

h. Whether Defendant unlawfully disclosed and/or failed to protect Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

IV. CAUSES OF ACTION

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

128. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 127.

129. Plaintiff and the Class entrusted Defendant with their PII, PHI, and PBI.

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

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

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

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

Defendant's security protocols to ensure that the PII, PHI, and PBI of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

134. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

135. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII, PHI, and PBI of Plaintiff and the Class.

136. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, PHI, and PBI, a necessary part of obtaining services from Defendant. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

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

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

139. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

their decisions not to comply with industry standards for the safekeeping of the PII, PHI, and PBI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

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

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

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

143. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII, PHI, and PBI of Plaintiff and the Class.

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

145. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols, including those mandated under HIPAA and HITECH, and exercise reasonable care in protecting and safeguarding the PII, PHI, and PBI of Plaintiff and the Class during the time the PII, PHI, and PBI was within Defendant's possession or control.

146. Defendant improperly and inadequately safeguarded the PII, PHI, and PBI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

147. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII, PHI, and PBI of Plaintiff and the Class in the face of increased risk of theft.

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

149. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII, PHI, and PBI they were no longer required to retain pursuant to regulations. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

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

151. There is a close causal connection between Defendant's failure to implement security measures to protect the PII, PHI, and PBI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII, PHI, and PBI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII, PHI, and PBI by adopting, implementing, and maintaining appropriate security measures.

152. 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, PHI, and PBI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

154. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

155. 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 Class.

156. IGG's violations of HIPAA also independently constitutes negligence *per se*.

157. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

158. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

159. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

160. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data breaches for health care providers and other industries.

161. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. IGG knew or should have known of the inherent risks in collecting and storing the PII, PHI, and PBI of Plaintiff and the Class, the critical importance of providing adequate security, and that it had inadequate employee training and education and IT security protocols in place to secure the information.

162. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the 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, PHI, and PBI is used; (iii) the compromise, publication, and/or theft of their PII, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, PHI, and PBI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing 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, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII, PHI, and PBI of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the 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.

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

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

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

165. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 164.

166. Plaintiff and the Class entrusted their PII, PHI, and PBI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and

to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

167. Defendant entered into contracts with Plaintiff and Class Members for healthcare services, among other things. As a condition of that relationship, Plaintiff and Class Members entrusted personal and sensitive information to Defendant, which gave rise to a duty to safeguard that information.

168. These contracts included, in part, promises regarding Defendant's commitment to the security of patient privacy. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

169. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

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

171. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

172. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 171.

173. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII, PHI, and PBI. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII, PHI, and PBI.

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

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

176. Defendant acquired the monetary benefit and PII, PHI, and PBI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

177. If Plaintiff and Class Members knew that Defendant had not secured their PII, PHI, and PBI, they would not have agreed to provide their PII, PHI, and PBI to Defendant and would have sought medical treatment elsewhere.

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

179. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (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, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (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 identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

181. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On behalf of Plaintiff and the Illinois Class)

182. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 181.

183. Plaintiff and the Illinois Class are "consumers" as defined in 815 ILCS 505/1(e). Plaintiff, the Illinois Class, and Defendant are "persons" as defined in 815 ILCS 505/1(c).

184. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 ILCS 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 ILCS 505/1(b) and (d). Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Illinois Class's sensitive PII, PHI, and PBI from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII, PHI, and PBI of Plaintiff and the Illinois Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII, PHI, and PBI of Plaintiff and the Illinois Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Illinois Class's PII, PHI, and PBI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

185. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Class and defeat their reasonable expectations about the security of their PII, PHI, and PBI.

186. Defendant intended that Plaintiff and the Illinois Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class. Plaintiff and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

187. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

188. As a result of Defendant's wrongful conduct, Plaintiff and the Illinois Class were injured in that they never would have provided their PII, PHI, and PBI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII, PHI, and PBI from being hacked and taken and misused by others.

189. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Illinois Class have suffered harm: (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, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (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 identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

190. Pursuant to 815 ILCS 505/10a(a), Plaintiff and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT V
Violation of Illinois Biometric Information Privacy Act
740 Ill. Comp. Stat. 14/, *et seq*.
(On behalf of Plaintiff and the PBI Class)

191. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 190.

192. Defendant is a "private entity" as defined by the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1.

193. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to disclose information unless *first*: "(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's

legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d)(1)-(4).

194. BIPA also requires the following: "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers, and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." ILCS 740 14/15(d)(1)-(4).

195. Defendant violated 740 ILCS 14/15(d)(1)-(4) because it disclosed Plaintiff's and Class Members' PBI without authorization or under the approved exceptions.

196. Defendant violated 740 ILCS 14/15(e) because it failed to protect Plaintiff's and Class Members' PBI.

197. Defendant acted negligently in violating 740 ILCS 14/15.

198. Defendant acted recklessly in violating 740 ILCS 14/15.

199. Defendant acted intentionally in violating 740 ILCS 14/15.

200. As a direct and proximate result of Defendant's violations of the BIPA, upon information and belief, Plaintiff and the Illinois Class have suffered harm: (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, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (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 identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members., Pursuant to 740 ILCS 14/1, *et seq*., Plaintiff on behalf of himself and Class Members seeks the following: (i) injunctive and equitable relief as necessary to protect the interests of the Plaintiff and Class by requiring Defendant to comply with BIPA's requirements for unlawful disclosure and duty to protect BIPA; (ii) injunctive and equitable relief as necessary to protect the public good and the public's right to issuance of a written policy to ensure that Defendant complies with the written policy; (iii) statutory damages of $1,000 per violation for each of Defendant's negligent violations of BIPA pursuant to 740 ILCS 14/20(1) or $5,000 for Defendant's intentional, or reckless violation of BIPA pursuant to 740 ILCS 14/20(2); and (iv) reasonably attorneys' fees and costs and expenses pursuant to 740 ILCS 14/20(3).

COUNT VI
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY OF MEDICAL RECORDS

201. The preceding factual statements and allegations are incorporated herein by reference.

202. At all times relevant hereto, Defendants owed, and owes, a fiduciary duty to Plaintiff and the Class Members pursuant to Illinois common law, to keep Plaintiff's and the Class Members' medical and other PHI, PBI and PII information confidential.

203. The fiduciary duty of privacy imposed by Missouri law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

204. Defendants breached their fiduciary duty to Plaintiff and the Class Members by disclosing Plaintiff PHI and PII to unauthorized third parties.

205. As a direct result of Defendants' breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's and the Class Members' confidential medical information, Plaintiff and the Class Members suffered damages.

206. Plaintiff suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breaches; (ii) improper disclosure of her PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon her by the Breaches; (v) the value of her time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and (vi) the increased risk of identity theft.

207. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the Class Members' confidential medical information, Plaintiff and the Class Members suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, humiliation and loss of enjoyment of life.

V. PRAYER FOR RELIEF

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

A. For an Order certifying the Nationwide Class, the Illinois Class, and the BIPA Class, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII, PHI, and PBI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; requiring Defendant 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;

ii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII, PHI, and PBI of Plaintiff and Class Members;

iv. prohibiting Defendant from maintaining the PII, PHI, and PBI of Plaintiff and Class Members on a cloud-based database;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees,

with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of statutory damages of $1,000 for each of Defendant's violation of BIPA, pursuant to 740 ILCS 14/20(1) and/or $5,000 for each of Defendant's violations of BIPA, pursuant to 740 ILCS 14/20(2);

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. 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: June 6, 2022

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878

JEAN S. MARTIN
(*Pro Hac Vice application forthcoming*)
FRANCESCA KESTER
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jean.martin@ForThePeople.com
fkester@ForThePeople.com

Maureen M. Brady MO #57800
(*Pro Hac Vice application forthcoming*)
Lucy McShane MO #57957
(*Pro Hac Vice application forthcoming*)
MCSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, Missouri 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-Mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

Attorneys for Plaintiff and the Putative Class