49D01-2301-CT-000583
Filed: 1/5/2023 5:09 PM
Clerk
Marion Superior Court 1
Marion County, Indiana

**INDIANA COMMERCIAL COURT**

| | | |
|---|---|---|
| STATE OF INDIANA | ) | IN THE MARION SUPERIOR COURT 1 |
| | ) SS: | |
| COUNTY OF MARION | ) | CAUSE NO. |

| | | |
|---|---|---|
| BRANDON DREW, and JEREMY FATER, individually, and on behalf of a class of similarly situated persons, | ) | JURY TRIAL DEMANDED |
| *Plaintiffs*, | ) | |
| v. | ) | |
| TIC INTERNATIONAL CORPORATION, | ) | |
| *Defendant*, | ) | |

**CLASS ACTION COMPLAINT**

Plaintiffs, Brandon Drew and Jeremy Fater (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant TIC International Corporation ("TIC"), and allege as follows:

**NATURE OF THE ACTION**

1. Defendant TIC is a benefit administration company specializing in consulting and third-party administration for multiemployer health care, defined benefit pension, and defined contribution/401(k) plans.

2. On or about September 6 or September 7 of 2022, TIC notified Plaintiffs and thousands of other current and former fund participants that it experienced a "system disruption due to an encryption attack". *Notice of Data Security Incident*, TIC INTERNATIONAL CORPORATION, annexed hereto as *Pls.' Ex. A* at 1 (the "Notice Letter").

3. Specifically, upon information and belief, TIC was the target of a ransomware attack by the notorious Conti ransomware group on March 30, 2022 (the "Data Breach"). *See Pls.'*

*Ex. A* at 1.[1] Subsequently, TIC engaged "cybersecurity experts" to "determine what personal information may have been involved, to locate mailing information, and to set up the identity protection services being offered." *Ibid.* Accordingly, TIC was completely unaware of the Conti ransomware group's infiltration of its systems for months, until the cybercriminals began deploying ransomware and encrypting the files stored in TIC's systems.

4. It is unknown whether TIC made a ransom payment to the Conti group.

5. As a result of the Data Breach, TIC reported that certain Personally Identifying Information[2] and Protected Health Information[3] (collectively "Personal Information") of 187,341

[1] *See also Conti Ransomware Victim: https-www-tici-co,* RED PACKET SECURITY (Apr. 2022), https://www.redpacketsecurity.com/conti-ransomware-victim-https-www-tici-co/.

[2] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to TIC, not every type of information included in that definition was compromised in the breach.

[3] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, *inter alia*, a group health plan. *Id. Covered entity, Health plan*. A "business associate" is defined as, with respect to a covered entity, a person who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing…" *Id. Business associate*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 5, 2022). As the administrator of a group health plan, TIC is clearly a "business associate" of a "covered entity" and some of the data compromised in the Data Breach that this action arises out of is "protected health information", subject to HIPAA.

of TIC's current and former fund participants was targeted, stolen, and exfiltrated from TIC's systems.[4]

6. The compromised Personal Information included fund participants' "name, address, Social Security number, date of birth, and protected health information." *Pls.' Ex. A* at 1.

7. Upon information and belief, the Personal Information the Conti group purloined was posted on the Dark Web on the Conti .onion Dark Web Tor Blog page for all the world to access and misuse.[5] Despite the Conti group releasing Plaintiffs' and Class Members' Personal Information on the dark web, TIC represented that it was "not aware of the misuse of any potentially affected individuals' information…" in the Notice Letter. *Ibid.*

8. Upon information and belief, Data Breach victims did not start receiving letters notifying them of the Data Breach or detailing which specific types of their Personal Information was compromised until September 6 or September 7 of 2022—nearly six months after the Data Breach began and several months after TIC discovered it. *See generally id*. TIC has offered no explanation for the delay between the initial discovery of the Data Breach and the belated notification to affected fund participants, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely notification been made.

9. Shifting the onus of dealing with the Data Breach to impacted persons, the Notice Letter urged Plaintiffs and the scores of other victims of the Data Breach to "notify [their] financial institution immediately if [they] detect any suspicious activity on any of [their] accounts, including unauthorized transactions or new accounts opened in [their] name that [they] do not recognize"

[4] *See* Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches, OFFICE OF THE MAINE ATTORNEY GENERAL, available at https://apps.web.maine.gov/online/aeviewer/ME/40/a08c2070-eb21-4246-9b25-7dadbb21919a.shtml (last accessed Jan. 4, 2022).

[5] *See* n.1, *supra*.

and to "promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities." *Id.* at 1. The Notice Letter also encouraged Plaintiffs and other victims of the Data Breach to consider, *inter alia*, placing security freezes on their credit reports, placing or extending fraud alerts on their credit reports, ordering copies of their credit reports, and notifying the three major credit bureaus if a deceased family member was involved in the Data Breach. *Id.* at 1-2.

10. Because of the Data Breach, Plaintiffs and Class members' sensitive Personal Information has been released into the public domain and published on the dark web. Plaintiffs and Class members have had to, and will continue to have to, spend time and money to protect themselves from ongoing and imminent fraud and identity theft.

11. Plaintiffs and members of the proposed Class are victims of TIC's negligence and failure to honor its express and implied promises to safeguard their Personal Information. Plaintiffs and members of the proposed Class entrusted TIC with their Personal Information.

12. But TIC betrayed that trust and the duty owed to Plaintiffs and the other Class members. TIC failed to employ data security best practices and use up-to-date data security measures to prevent the Data Breach. When the Data Breach was discovered, TIC failed to promptly notify victims of the Data Breach of the types of information that was stolen.

13. TIC's negligence and failure to abide by its promises caused real and substantial damage to Plaintiffs and members of the proposed Class.

14. Further, because this same information remains stored in TIC's systems, Plaintiffs and Class members have an interest in ensuring that TIC takes the appropriate measures to protect their Personal Information against future unauthorized disclosures.

15. Plaintiffs, individually and on behalf of all others similarly situated, bring this class action against TIC for failing to adequately secure and safeguard their Personal Information, breaching the terms of TIC's express and implied contracts with its fund participants, unjustly enriching itself at Plaintiffs' and Class members' expense, and negligently failing to secure the Personal Information entrusted to it.

## PARTIES

16. Plaintiff Brandon Drew is a citizen and resident of Michigan. Plaintiff Drew has been a member of the Millwrights Local 1102 Detroit for the past 20 years ("Local 1102"). The Local 1102 has negotiated defined benefits that are administered by TIC, and Plaintiff Drew's Personal Information was stored on TIC's systems at all times material hereto. Plaintiff Drew received a Notice Letter from TIC notifying him that his Personal Information was stolen in the Data Breach.

17. Plaintiff Jeremy Fater is a citizen and resident of Michigan. Plaintiff Fater has been a member of the Union Local 102 for approximately 17 years ("Local 102"). The Local 102 has negotiated defined benefits that are administered by TIC, and Plaintiff Fater's Personal Information was stored on TIC's systems at all times material hereto. Plaintiff Fater received a Notice Letter from TIC notifying him that his Personal Information was stolen in the Data Breach.

18. Defendant TIC International Corporation is a Foreign For-Profit Corporation, incorporated under the laws of the State of Delaware, with a principal office address located at 11590 North Meridian Street, Suite 600, Carmel, Indiana, 46032.

## JURISDICTION AND VENUE

19. This Court has general *in personam* jurisdiction over TIC because TIC's principal office is located in Indiana, such that it is at home within the state.

20. Venue lies in Marion County under Trial Rule 75(A).

## FACTUAL ALLEGATIONS

21. Plaintiffs and members of the proposed Class are among the 187,341 fund participants whose Personal Information was disclosed during the Data Breach.

22. Plaintiffs and members of the proposed Class received the Notice Letter from TIC, directly informing them that their Personal Information had been compromised in the Data Breach.

23. As a condition for participating in the benefit plans TIC administered, Plaintiffs and Class members were required by TIC to confide and make available to it, its agents, and its employees sensitive and confidential Personal Information, including, but not limited to, their names, addresses, Social Security numbers, dates of birth, and protected health information.

24. TIC acquired, collected, and stored a massive amount of its fund participants' Personal Information.

25. By obtaining, collecting, using, and deriving a benefit from its fund participants' Personal Information, TIC assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Personal Information from unauthorized disclosure.

26. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Personal Information. Plaintiffs, as fund participants at TIC, relied on TIC to keep their Personal Information confidential and securely maintained, to use and disclose this information for authorized purposes only, and to take reasonable steps to ensure that its vendors would make only authorized disclosures of this information.

### A. The Data Breach and the Security of Fund Participants' Personal Information

27. When Plaintiffs elected to participate in benefit plans administered by TIC, it provided Plaintiffs with various disclosure statements regarding TIC's privacy policies and its obligations under HIPAA to safeguard fund participants' Personal Information, as TIC was required to do by law.[6]

28. As a prerequisite to participating in those benefit plans, Plaintiffs divulged their personal and highly sensitive Personal Information to TIC, with the implicit understanding that the Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to participating in the plans, and the express and implied representations made by TIC and its agents.

29. Plaintiffs reasonably relied upon TIC's representations to their detriment and would not have provided their sensitive Personal Information to TIC if not for TIC's explicit and implicit promises to adequately safeguard that information.

30. According to TIC, on or around March 30, 2022, cybercriminals gained access to TIC's network and caused a "system disruption".

31. Per the Notice Letter, these cybercriminals had uninhibited access to Plaintiffs and Class members' Personal Information for months prior to detection.

32. Indeed, these cybercriminals went undiscovered until they began encrypting files stored in TIC's systems, alerting TIC to the ransomware attack.

33. TIC acknowledges that its fund participants' highly sensitive Personal Information was stolen from its network by the cybercriminals during the Data Breach. *See Pls.' Ex. A* at 1.

[6] *See, e.g.*, 45 C.F.R. §§ 164.520(a)(2), (c)(1).

34. Although TIC does not acknowledge it, upon information and belief, The Conti ransomware group was responsible for the Data Breach, and they released the stolen Personal Information on the dark web.

35. The stolen and published Personal Information includes fund participants' "name, address, Social Security number, date of birth, and protected health information." *Pls.' Ex. A* at 1.

36. Despite the highly sensitive nature of the stolen Personal Information and the severe risks associated with its theft, distribution, and publication, upon information and belief, TIC did not notify victims of the Data Breach or about what types of their Personal Information was compromised until on or around September 6 or September 7 of 2022, months after TIC discovered the Data Breach and nearly seven months after the Data Breach began.

37. In the Notice Letter, TIC recommended that Plaintiffs and members of the Class to "notify [their] financial institution immediately if [they] detect any suspicious activity on any of [their] accounts, including unauthorized transactions or new accounts opened in [their] name that [they] do not recognize" and to "promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities." *Pls.' Ex. A* at 1.

38. The Notice Letter also recommended that Plaintiffs and members of the Class consider, *inter alia*, placing security freezes on their credit reports, placing or extending fraud alerts on their credit reports, ordering copies of their credit reports, and notifying the three major credit bureaus if a deceased family member was involved in the Data Breach. *Id.* at 1-2.

39. TIC has placed the burden of protecting against fraud and dealing with the risk of the Data Breach on Plaintiffs and Class members by creating a laundry list of burdensome and expensive tasks for them to undertake in order to hopefully achieve data security.

40. TIC offered Plaintiffs and Class members one year of credit and identity monitoring through Kroll. All the while, TIC knew or should have known the risk continues for a far longer period than the one year, if not the Class members' entire lives. One year of credit monitoring is thus insufficient to protect Plaintiffs and Class members from identity theft and fraud resulting from the Data Breach.

41. As a result of the Data Breach, the Personal Information of more than 187,341 individuals whose Personal Information was entrusted to TIC was compromised.

42. The Data Breach was preventable and a direct result of TIC's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect fund participants' Personal Information.

**B. Storehouses of PHI are a Prime Target for Cybercriminals**

43. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[7] The next year, that number increased by nearly 45%.[8] The following year the healthcare sector—which encompasses plan administrators, such as TIC—was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[9]

44. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity

[7] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"].

[8] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"].

[9] *2018 End-of-Year Data Breach Report*, ITRC (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[10]

45. 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)."[11]

46. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting 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 fund participants' health and financial information, but also patient access to care.[12]

47. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[13] In 2017, a new record high of 1,579 such breaches were reported—representing a 44.7 percent increase.[14] That trend continues.

48. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[15] Indeed, when

---

[10] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6.

[11] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://reut.rs/3x2kCib.

[12] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://bit.ly/33AlXjS.

[13] *Data Breaches Increase 40 Percent in 2016*, *supra* note 7.

[14] *Data Breaches Up Nearly 45 Percent*, *supra* note 8.

[15] *2018 End-of-Year Data Breach Report*, *supra* note 9.

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 out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16] 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.[17]

49. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of fund participants at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[18]

50. As the FBI explained, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[19]

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

- 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.

---

[16] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v.

[17] *Id.*

[18] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

[19] *See How to Protect Your Networks from Ransomware*, FBI 3 (2016), https://bit.ly/3FoLd9C.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

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

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

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

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

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using 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.[20]

52. 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:

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

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

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

- **Keep your personal information safe.** Check a website's security to ensure 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 stay 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.

[20] Natale Goriel, *14 Tips to Protect Your business from Ransomware Attacks*, U.S. SMALL BUSINESS ADMINISTRATION (May 18, 2017), https://bit.ly/33zd9uc.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[21]

53. Charged with handling highly sensitive Personal Information including healthcare information, financial information, and insurance information, TIC knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. TIC also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on TIC's fund participants as a result of a breach. TIC nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

54. The Personal Information stolen in the Data Breach is significantly more valuable than the loss of credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name, date of birth, and Social Security number—is difficult, if not impossible, to change.

55. This kind of data demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[22] The FBI likewise has warned healthcare organizations that Personal Information data is worth ten times as much as personal credit card data on the black market.[23]

---

[21] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://bit.ly/3niRHkk.

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://bit.ly/3KeFdUb.

[23] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information.

56. Personal Information data for sale is so valuable because Personal Information is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

57. The value of Plaintiffs' Personal Information on the black market is considerable. Stolen Personal Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee, of course.

58. Considering these substantial risks, consumers place a high value on the privacy of their data. Indeed, studies confirm that "once privacy information is made more salient, some consumers are willing to pay a premium to purchase from more privacy protective websites."[24]

59. Upon information and belief, the Personal Information stolen in the Data Breach has been published on the dark web.[25]

60. Plaintiffs would not have provided their highly sensitive Personal Information to TIC if they had known TIC would not adequately protect it from unauthorized access, theft, or use.

## C. TIC Failed to Sufficiently Protect the Personal Information that Fund Participants Entrusted to It

### *i. TIC Failed to Adhere to HIPAA*

61. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep fund participants' medical information safe. HIPAA compliance provisions,

---

*See* Humer, Caroline & Finkle, Jim, *Your Medical Record Is Worth More to Hackers than Your Credit Card*, REUTERS (Sep. 24, 2014), https://reut.rs/3qNZZ6o. Dark web monitoring is a commercially available service which, at a minimum, TIC can and should perform (or hire a qualified third-party expert to perform).

[24] Janice Tsai et. al, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, INFORMATION SYSTEMS RESEARCH 22(2):254-268, https://bit.ly/3vfzurh.

[25] *See* n.1, *supra*.

commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[26]

62. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Personal Information is properly maintained.[27]

63. The Data Breach itself resulted from a combination of inadequacies showing TIC failed to comply with safeguards mandated by HIPAA. TIC's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by TIC's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

[26] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[27] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

***ii. TIC Failed to Adhere to FTC Guidelines***

64. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[28] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as TIC, should employ to protect against the unlawful exposure of Personal Information.

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

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

[28] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF.

[29] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre.

e. implement policies to correct security problems.

66. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

67. The FTC recommends that companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[30]

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

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

### *iii. TIC Failed to Adhere to Industry Standards*

70. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[31] The costs of healthcare data breaches are among

[30] *See Start with Security*, *supra* note 28.
[31] *2018 End-of-Year Data Breach Report*, *supra* note 9.

the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record.[32] As a result, both the government and private sector have developed industry best standards to address this growing problem.

71. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[33] The DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[34] Notably, organizations must properly encrypt Personal Information in order to mitigate against misuse.

72. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, TIC failed to adopt sufficient data security processes.

73. TIC's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

**D. Plaintiffs and the Class Members Were Significantly Harmed by the Data Breach**

74. As discussed above, Personal Information is among the most sensitive, and personally damaging information. A report focusing on breaches in the healthcare industry found that the "average total cost to resolve an identity theft-related incident . . . came to about

[32] *Id.*

[33] Steve Alder, *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://bit.ly/3NPhJav.

[34] *Id.*

$20,000.00" per person, and that the victims were further routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[35]

75. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they [must pay] the healthcare provider, repa[y] the insurer for services obtained by the thief, or . . . engage[] an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[36]

76. Moreover, nearly half of identity theft victims lost their health care coverage as a result of a data breach incident, nearly one-third reported that their premiums went up, and forty percent never resolved their identity theft at all.[37]

77. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve."[38]

78. Moreover, resolution of medical identity theft is time consuming to remedy. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident."[39] Consequently, they remain at "risk for further theft or errors in [their] healthcare records that could jeopardize medical treatments and diagnosis."[40]

---

[35] *Study: Medical Identity Theft Is Costly for Victims*, *supra* note 16.

[36] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE LLC 1 (Feb. 2015), https://bit.ly/38vGnNh.

[37] *Id.*

[38] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 13, 2010), https://bit.ly/3Fy49mO.

[39] *Id.*

[40] *Id.*

79. As a result of the Data Breach, Plaintiffs and Class members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

80. As a long-standing member of the healthcare community, TIC knew or should have known the importance of safeguarding patient Personal Information entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, TIC failed to take adequate cyber-security measures to prevent the ransomware attack from happening.

81. As known to Plaintiffs, other than the inadequate one-year credit monitoring, TIC has not provided any compensation to fund participants victimized in the Data Breach or offered to provide any assistance or compensation for the costs and burdens, current and future, associated with the identity theft and fraud resulting from the Data Breach.

82. Even if TIC did reimburse Plaintiffs and members of the Class for the harms they have suffered, it is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[41]

83. As a result of TIC's failure to prevent the Data Breach, Plaintiffs and Class members have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

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

b. The diminution in value of their Personal Information;

[41] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf.

c. The compromise, publication and/or theft of their Personal Information;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Personal Information;

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

i. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

84. Plaintiffs have already incurred harms as a result of the Data Breach.

***i. Plaintiff Drew***

85. Plaintiff Drew has always taken reasonable measures to safeguard his Personal Information.

86. Plaintiff Drew received a Notice Letter from TIC notifying him that the cybercriminals obtained his Personal Information, including his name, address, Social Security number, date of birth, and protected health information. *Pls.' Ex. A* at 1. Upon information and belief, the cybercriminals responsible for the Data Breach—the Conti ransomware group—posted the Personal Information they purloined on the Dark Web.

87. In or around late spring/summer of 2022, an unknown actor purchased an auto part and had it shipped to Plaintiff Drew's address. Soon thereafter, an unknown actor attempted to

purchase a $1,000.00 Best Buy gift card using Plaintiff Drew's compromised Personal Information.

88. Additionally, Plaintiff Drew has experienced an increase in spam texts and phone calls following the Data Breach. The spam concerns his compromised Personal Information.

89. To Plaintiff Drew's knowledge, he has never been the victim of any other data breach.

90. In addition to the out-of-pocket expenses Plaintiff Drew has incurred relating to the reasonable mitigation efforts that he has employed, Plaintiff Drew has also expended time and effort in order to mitigate the increased risk of harm he is likely to suffer on account of the Data Breach.

***ii. Plaintiff Fater***

91. Plaintiff Fater has always taken reasonable measures to safeguard his Personal Information.

92. Plaintiff Fater received a Notice Letter from TIC notifying him that the cybercriminals obtained his Personal Information, including his name, address, Social Security number, date of birth, and protected health information. *Pls.' Ex. A* at 1. Upon information and belief, the cybercriminals responsible for the Data Breach—the Conti ransomware group—posted the Personal Information they purloined on the Dark Web.

93. To Plaintiff Fater's knowledge, he has never been the victim of any other data breach.

94. In addition to the out-of-pocket expenses Plaintiff Fater has incurred relating to the reasonable mitigation efforts that he has employed, Plaintiff Fater has also expended time and

effort in order to mitigate the increased risk of harm he is likely to suffer on account of the Data Breach.

## CLASS ACTION ALLEGATIONS

95. Plaintiffs bring this action on behalf of themselves and as a class action on behalf of the following proposed class ("the Class"):

> All Indiana citizens whose personally identifying information or personal health information was compromised in TIC's Data Breach.

96. Excluded from the Class are the officers, directors, and legal representatives of TIC and the judges and court personnel in this case and any members of their immediate families.

97. This action is properly maintainable as a class action under Indiana Rules of Trial Procedure 23(A) and (B)(3).

98. Numerosity. TIC reports that the Data Breach compromised the Personal Information of 187,341 individuals. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

99. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether TIC failed to adopt the practices and procedures necessary to adequately safeguard the information compromised in the Data Breach;

b. Whether TIC timely, adequately, and accurately informed Class Members that their Personal Information had been compromised;

c. Whether and to what extent TIC breached its express contract with Plaintiffs and the Class;

d. Whether TIC breached its implied contract with Plaintiffs and the Class;

e. Whether TIC was unjustly enriched;

f. Whether TIC acted negligently;

g. Whether Class members are entitled to damages as a result of TIC's wrongful conduct;

h. Whether Plaintiffs and the Class are entitled to restitution as a result of TIC's wrongful conduct; and

i. Whether Plaintiffs and the Class are entitled to injunctive relief.

100. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' Personal Information, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiffs, like all Class members, were injured by TIC's uniform conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

101. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiffs suffered are typical of other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in complex consumer class action litigation, including data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

102. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in

individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

103. The litigation of the claims brought herein is manageable. TIC'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.

104. Adequate notice can be given to Class members directly using information maintained in TIC's records.

105. Predominance. Pursuant to Rule 23(B)(3), the issues in this action 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 the questions identified above.

106. This proposed class action does not present any unique management difficulties.

**FIRST CAUSE OF ACTION**
**Breach of Express Contract**
**(On Behalf of the Class)**

107. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

108. Plaintiffs and Class members entered into written agreements with TIC regarding the administration of their plan benefits that TIC was to provide to Plaintiffs and Class members. This agreement included, *inter alia*, TIC's privacy policies and procedures.

109. Plaintiffs and Class members were required to provide their Personal Information, including names, addresses, Social Security numbers, dates of birth, protected health information, and other personal information to TIC as a condition of participating in the benefit funds TIC

administered. Plaintiffs and Class members also paid TIC monies as consideration for these agreements, either directly or through an insurance carrier.

110. TIC therefore offered Plaintiffs and the Class a unilateral contract, which Plaintiffs and the Class members accepted by providing the necessary Personal Information and proceeding with participating in the benefit funds.

111. Plaintiffs' and the Class members' decision to obtain benefit fund administration services from TIC while under no obligation to do so constituted both consideration for and acceptance of TIC's offer.

112. Implicit in the agreement between TIC and the Class was the obligation that both parties to the agreement would maintain information confidentially and securely.

113. Additionally, TIC expressly promised to protect the Personal Information entrusted to it and to make disclosures only if permitted by law, permitted by TIC's privacy policies and procedures, or if made with the patient's express authorization.

114. TIC also promised to disclose the Personal Information entrusted to it to authorized individuals only.

115. Implicit in performing these contractual duties is an obligation for TIC to reasonably safeguard its systems and data against cyberattack, including ransomware attacks and data breaches like the Data Breach in this instance which can cause and have caused harm and injury to Plaintiffs and the Class members.

116. Additionally, TIC's privacy policies and procedures contained additional covenants restricting its disclosure of Personal Information.

117. Plaintiffs and the Class members fully performed as required under the agreement. TIC did not.

118. TIC violated the terms of the agreement by allowing unauthorized access to Plaintiffs and the other Class members' Personal Information for unauthorized purposes without first obtaining Plaintiffs' or the other Class members' consent and without encrypting or otherwise protecting the Personal Information in a form which could not reasonably be used to identify, target, extract, or publish the Personal Information.

119. TIC further violated the terms of the agreement by allowing cybercriminals to encrypt and extract Class members' Personal Information and to publish the stolen Personal Information on the dark web.

120. TIC materially breached the agreement when it exposed Plaintiffs and the Class members' Personal Information during the Data Breach, thereby depriving Plaintiffs and Class members of the full benefit of their bargain.

121. Plaintiffs and Class members would not have produced their Personal Information to TIC if they knew that TIC would not adequately safeguard it as promised and would allow cybercriminals to extract it and publish it on the dark web.

122. TIC breached its agreement with Plaintiffs and Class members by failing to reasonably safeguard its systems and data from the Data Breach.

123. TIC violated the terms of the contract by failing to take appropriate measures to protect Plaintiffs and the other Class members' Personal Information in accordance with its promises and representations.

124. TIC violated the agreement by failing to comply with applicable laws regarding the access, correction, and/or deletion of Personal Information, and notification to affected persons.

125. Plaintiffs and Class members have been injured as a result of TIC's breach of contract and are therefore entitled to damages.

126. As a result of TIC's unlawful misconduct and breach of its contract with Plaintiffs and the Class members, Plaintiffs and the Class members have suffered additional pecuniary loss and injury-in-fact, including without limitation the improper disclosure of their Personal Information, lost benefit of their bargain, lost value of their Personal Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach, which injury-in-fact and damages are ongoing, imminent, and immediate.

**SECOND CAUSE OF ACTION**
**Breach of Implied Contract**
**(On Behalf of the Class)**

127. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

128. Plaintiffs and Class members were required to provide their Personal Information —including names, addresses, Social Security numbers, dates of birth, protected health information, and other personal information—to TIC as a condition of its benefit fund administration.

129. Implicit in the agreement between TIC and its fund participants was the obligation that both parties would maintain the Personal Information confidentially and securely.

130. TIC had an implied duty of good faith to ensure that the Personal Information of Plaintiffs and Class members in its possession was only used only as authorized, such as to perform legitimate benefit fund administration services.

131. TIC had an implied duty to reasonably safeguard and protect the Personal Information of Plaintiffs and Class members from unauthorized disclosure or use.

132. Additionally, TIC implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential.

133. Plaintiffs and Class members fully performed their obligations under the implied contract with TIC. TIC did not. Plaintiffs and Class members would not have provided their confidential Personal Information to TIC in the absence of their implied contracts with TIC and would have instead retained the opportunity to control their Personal Information for uses other than TIC's administration of benefit funds.

134. TIC breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs and Class members' Personal Information, which was compromised as a result of the Data Breach.

135. TIC's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class members to provide their Personal Information in exchange for medical treatment and benefits.

136. As a direct and proximate result of TIC's breach of its implied contracts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in TIC's possession and is subject to further unauthorized disclosures so long as TIC fails to undertake appropriate and adequate measures to protect the Personal

Information of current and former fund participants that is in its 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 Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

**THIRD CAUSE OF ACTION**
**Unjust Enrichment**
**(On Behalf of the Class)**

137. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

138. This claim is pleaded solely in the alternative to Plaintiffs' express and implied contract claims.

139. Plaintiffs and Class members conferred a monetary benefit upon TIC in the form of monies paid for benefit fund administration.

140. TIC appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members.

141. TIC also benefited from the receipt of Plaintiffs and Class members' Personal Information, as this was used to facilitate the administration of the benefit funds.

142. As a result of TIC's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

143. Under principals of equity and good conscience, TIC should not be permitted to retain the money belonging to Plaintiffs and Class members because TIC failed to implement (or adequately implement) the data privacy and security practices and procedures for which Plaintiffs

and Class members paid, and which were otherwise mandated by federal, state, and local laws and by industry standards.

144. TIC should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds it received as a result of its conduct and the Data Breach alleged herein.

**FOURTH CAUSE OF ACTION**
**Negligence**
**(On Behalf of Plaintiffs and the Class)**

145. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

146. Upon agreeing that TIC would administer the benefit funds Class members were participants in, fund participants were obligated to provide TIC with certain Personal Information, including their name, address, Social Security number, date of birth, and protected health information. TIC had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiffs and Class members could and would suffer if their Personal Information were wrongfully disclosed.

147. TIC 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 TIC's policies regarding the storage, utilization, and distribution of fund participants' Personal Information to ensure that Plaintiffs and Class members' information was adequately secured and protected.

148. Personal Information is highly valuable, and TIC knew or should have known the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiffs and the Class as well as the importance of exercising reasonable care in handling it.

149. The risk that unauthorized persons would try to gain access and misuse to the

Personal Information stored on TIC's systems was foreseeable.

150. TIC had a duty of care to Plaintiffs and members of the Class because it was foreseeable that TIC's failure to adequately safeguard their Personal Information in accordance with state-of-the-art industry standards for data security would result in the compromise of that Personal Information —just like the Data Breach that ultimately came to pass. TIC acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' Personal Information by disclosing and allowing access to Personal Information to unknown third parties and by failing to properly supervise both the way the Personal Information was stored, used, and exchanged, and those in its employ who were responsible for data security.

151. TIC owed Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. TIC also owed Plaintiffs and Class members a duty to timely and accurately disclose to them the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

152. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. TIC knew or should have known of the inherent risks in collecting and storing Personal Information and the critical importance of providing adequate security for that Personal Information. TIC also knew or should have known that it had inadequate employee training and education and information security protocols in place to secure the Personal Information of Plaintiffs and the Class.

153. TIC's conduct created a foreseeable risk of harm to Plaintiffs and Class members.

154. TIC's misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Breach as set forth herein. TIC's misconduct also included its decision not to comply with industry standards for the safekeeping and use of the Personal Information of Plaintiffs and Class members.

155. Plaintiffs and Class members had no ability to protect their Personal Information that was in TIC's possession. Only TIC was able to protect against the harm Plaintiffs and Class members suffered as a result of the Data Breach.

156. TIC had and continues to have a duty to adequately notify Plaintiffs and Class members that their Personal Information was compromised, how it was compromised, and other details of the Data Breach. Such notice is necessary to allow Plaintiffs and the Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their Personal Information by unauthorized third parties.

157. TIC has failed to timely or adequately notify Plaintiffs and the Class of the Data Breach, as the Notice Letter did not contain sufficient information detailing the incident, including, but not limited to, key information regarding the nature of the hacking incident and how the unauthorized third party obtained access to Plaintiffs and Class members' Personal Information. TIC's failure to provide appropriate notice of the Data Breach to Plaintiffs and Class members actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries in fact.

158. TIC had a duty to have appropriate procedures in place to prevent the unauthorized dissemination of the Personal Information of Plaintiffs and Class members.

159. TIC has acknowledged that the privacy and security of Plaintiffs and Class members' Personal Information was compromised as a result of the Data Breach.

160. TIC, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to exercise reasonable care in protecting and safeguarding their Personal Information.

161. TIC deviated from standard industry rules, regulations, and practices at the time of the Data Breach by improperly and inadequately safeguarding the Plaintiffs' and Class members' Personal Information.

162. TIC, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to store and access fund participants' Personal Information and to detect and prevent unauthorized access to fund participants' Personal Information.

163. TIC, through its actions and/or omissions, unlawfully breached its duty to timely and adequately disclose to Plaintiffs and Class members the existence and scope of the Data Breach.

164. But for TIC's wrongful and negligent breach of these duties, Plaintiffs and Class members' Personal Information would not have been compromised.

165. There is a close causal connection between TIC's failure to implement security measures to protect the Personal Information entrusted to it and the risk of imminent harm suffered by Plaintiffs and the Class.

166. As a result of TIC's negligence, Plaintiffs and the Class members have suffered and will continue to suffer damages and injury including, but not limited to, the costs associated with identity theft and fraud, the increased risk of future identity theft and fraud, the costs associated therewith, and lost time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

**FIFTH CAUSE OF ACTION**
**Negligence *Per Se***
**(On Behalf of Plaintiffs and the Class)**

167. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

168. Pursuant to the FTC Act, 15 U.S.C. § 45, TIC has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' Personal Information.

169. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of TIC's duty to protect Plaintiffs and Class members' sensitive Personal Information. 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 TIC, of failing to use reasonable measures to protect customers or, in this case, fund participants and employees' Personal Information.

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

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

172. TIC had a duty to Plaintiffs and the Class to implement and maintain reasonable security procedures and practices to safeguard their Personal Information.

173. TIC breached its duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Personal Information.

174. TIC's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

175. Pursuant to HIPAA (42 U.S.C. § 1302d, *et seq*.), TIC had a duty to implement reasonable safeguards to protect Plaintiffs and Class members' PHI.

176. Pursuant to HIPAA, TIC had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

177. Plaintiffs and Class members are within the class of persons that the HIPAA was intended to protect.

178. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against covered entities, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class members.

179. TIC breached its duties to Plaintiffs and the Class under HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard

Plaintiffs and Class members' PHI.

180. TIC's failure to comply with applicable laws and regulations constitutes negligence *per se*.

181. But for TIC's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

182. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of TIC's breach of its duties. TIC knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and the Class to suffer the foreseeable harms associated with the exposure of their Personal Information.

183. Had Plaintiffs and members of the Class known that TIC did not adequately protect the Personal Information entrusted to it, Plaintiffs and members of the Class would not have entrusted TIC with their Personal Information.

184. As a direct and proximate result of TIC's negligence *per se*, Plaintiffs and members of the Class have suffered harm, including, but not limited to, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiffs and members of the Class paid for that they would not have sought had they known of TIC's careless approach to cyber security; lost control over the use of their Personal Information; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

**SIXTH COUNT**
**INVASION OF PRIVACY**
**(On Behalf of Plaintiffs and the Class)**

185. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

186. Indiana recognizes the Restatement (Second) of Torts formulation of invasion of privacy, consisting of the distinct injuries: (1) intrusion upon seclusion; (2) appropriation of likeness; (3) public disclosure of private facts; and (4) false light publicity. Herein, Plaintiffs proceed upon the third injury.

187. Plaintiffs' and Class members' Private Information is private in nature.

188. TIC disclosed Plaintiffs' and Class members' Private Information to the public via the Data Breach, when the Conti ransomware group publicized it on the Dark Web and elsewhere.

189. The disclosure of Plaintiffs' and Class members' Private Information, including Social Security numbers and protected health information would be highly offensive to a reasonable person.

190. The Personal Information is not of legitimate public concern.

191. As a direct and proximate result of TIC's actions alleged above, Plaintiffs and Class members have suffered damages.

**PRAYER FOR RELIEF**

WHEREFORE Plaintiffs, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class counsel;

B. A mandatory injunction directing TIC to adequately safeguard the Personal Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

C. A mandatory injunction requiring that TIC provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Personal Information to unauthorized persons;

D. An award of damages, in an amount to be determined;

E. An award of attorneys' fees and costs;

F. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and

G. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: January 5, 2023

Respectfully submitted,

*s/ Lynn A. Toops*

Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
T: (317) 636-6481
F: (317) 636-2593
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

Samuel J. Strauss*
Raina C. Borrelli*
Alex Phillips*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkeStrauss.com

J. Gerard Stranch, IV*

Peter J. Jannace
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Ave. Ste. 200
Nashville, TN
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*to seek admission *pro hac vice*

*Counsel for the Plaintiffs and the Proposed Class*

# ClassAction.org



---