

1 M. ANDERSON BERRY (*pro hac vice* forthcoming)
2 GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)

3 **CLAYEO C. ARNOLD,**
4 **A PROFESSIONAL LAW CORP.**

5 865 Howe Avenue
6 Sacramento, CA 95825
7 Telephone: (916) 239-4778
8 Facsimile: (916) 924-1829
9 aberry@justice4you.com
10 gharoutunian@justice4you.com

11 BETSY C. MANIFOLD (*pro hac vice* forthcoming)
12 RACHELE R. BYRD (*pro hac vice* forthcoming)
13 OANA CONSTANTIN (*pro hac vice* forthcoming)

14 **WOLF HALDENSTEIN ADLER**
15 **FREEMAN & HERZ LLP**

16 750 B Street, Suite 1820
17 San Diego, CA 92101
18 Telephone: (619) 239-4599
19 Facsimile: (619) 234-4599
20 manifold@whafh.com
21 byrd@whafh.com
22 constantin@whafh.com

23 *Attorneys for Plaintiff and the Proposed Class*

24 **IN THE UNITED STATES DISTRICT COURT**
25 **FOR THE DISTRICT OF ARIZONA**

26 DAVID BAROCAS, individually and on
27 behalf of all others similarly situated,

28 Plaintiff,

v.

TTEC SERVICES CORPORATION,

Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff David Barocas (“Plaintiff”), in his individual capacity and on behalf of all others
2 similarly situated, brings this Class Action Complaint against TTEC Services Corporation
3 (“Defendant” or “TTEC”) and alleges, upon personal knowledge as to his own actions and his
4 counsels’ investigations, and upon information and belief as to all other matters, as follows:

5 **I. INTRODUCTION**

6 1. Plaintiff brings this class action against Defendant for its failure to properly secure
7 and safeguard Personally Identifiable Information (“PII”) of its customers and employees,
8 including, without limitation, their names, dates of birth, Healthcare ID number, medical record
9 information, including clinical information such as diagnosis, and/or Social Security numbers.

10 2. Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate
11 notice to Plaintiff and similarly situated current and former employees and customers (“Class
12 Members”) that their PII had been lost and precisely what type of information was unencrypted
13 and is now in the possession of unknown third parties.

14 3. Defendant is a customer experience and technology company that operates
15 nationwide, offering its services to business clients. Defendant’s employees and customers entrust
16 it with an extensive amount of their PII. Defendant retains this information—even after the
17 employment and customer relationships end.

18 4. On or around September of 2021, Defendant learned “there was unauthorized
19 activity in [TTEC’s] network between March 31, 2021 and September 12, 2021.”¹ A hacker gained
20 access to directories where PII was stored and obtained files stored on some of TTEC’s servers
21 (the “Data Breach”). TTEC completed a review of those files and other files on the servers on
22 November 24, 2021, and determined that one or more of the files contained customers’ and
23 employees’ names and Social Security numbers.²

24 5. In December, three months later, Defendant issued notice letters to those whose PII
25

26 ¹ See **Exhibit A** attached hereto (letter from TTEC to Plaintiff Barocas dated December 8,
27 2021).

28 ² See **Exhibit A**; <https://oag.ca.gov/system/files/Health%20Net%20-%20TTEC%20Notification%20Letter.pdf> (last visited Feb. 8, 2022); <https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-9135d8726541.shtml> (with link to “Copy of notice to affected Maine residents: TTEC-ME App & Sample.pdf” last visited Feb. 8, 2022).

1 may have been impacted.

2 6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and
3 Class Members, Defendant assumed legal and equitable duties to those individuals to protect and
4 safeguard that information from unauthorized access and intrusion. Defendant admits that the
5 unencrypted PII that the attacker viewed and took included individuals' names, date of birth,
6 Healthcare ID number, medical record information, including clinical information such as
7 diagnosis, and/or Social Security numbers.³

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

12 8. This PII was compromised due to Defendant's negligent and/or careless acts and
13 omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to
14 Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited
15 three months to report it to the states' Attorneys General and affected individuals. Defendant has
16 not informed Plaintiff or Class Members what the specific vulnerabilities and root causes of the
17 breach were.

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

22 10. Plaintiff brings this action on behalf of all persons whose PII was compromised as
23 a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members;
24 (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices;
25 and (iii) effectively secure hardware containing protected PII using reasonable and effective
26

27 ³ *Id.* It is clear that the information exposed as a result of the Data Breach was unencrypted.
28 California law, for example, requires companies to notify California residents "whose
unencrypted personal information was, or is reasonably believed to have been, acquired by an
unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code §
1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data
Breach on Dec. 22, 2021, evidencing that the exposed data was unencrypted. *See also Exhibit A.*

1 security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to
2 negligence and violates federal and state statutes.

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

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

21 **II. PARTIES**

22 13. Plaintiff David Barocas is a resident and citizen of Phoenix, Arizona. Plaintiff
23 Barocas is acting on his own behalf and on behalf of others similarly situated. Defendant obtained
24 and continues to maintain Plaintiff Barocas' PII and has a legal duty and obligation to protect that
25 PII from unauthorized access and disclosure. Plaintiff Barocas would not have entrusted his PII to
26 Defendant, his former employer, had he known that it would fail to maintain adequate data
27 security. Plaintiff Barocas' PII was compromised and disclosed as a result of the Data Breach.

1 14. Defendant TTEC is a Colorado corporation with its headquarters in Englewood,
2 Colorado. Defendant is a customer experience and technology company based in Colorado that
3 does business nationwide.⁴ Defendant has employed thousands of people, and maintains a
4 workforce of 4,450 employees to operate its business.⁵ TTEC is a subsidiary of TTEC Holdings,
5 Inc., a publicly traded company and “one of the largest, global CX (customer experience)
6 technology and services innovators for end-to-end, digital CX solutions[,]” whose “62,000+
7 employees operate on six continents and bring technology and humanity together to deliver happy
8 customers and differentiated business results.”⁶

9 15. All of Plaintiff’s claims stated herein are asserted against Defendant and any of its
10 owners, predecessors, successors, subsidiaries, agents and/or assigns.

11 III. JURISDICTION AND VENUE

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

17 17. This Court has personal jurisdiction over Defendant because it is authorized to and
18 regularly conducts business in Arizona.

19 18. Venue is proper in this District under 28 U.S.C. §1391(b)(2) because a substantial
20 part of the events or omissions giving rise to Plaintiff’s claims occurred in this District.

21 IV. FACTUAL ALLEGATIONS

22 *Background*

23 19. Plaintiff and Class Members, as Defendant’s employees and customers, were
24 required to provide Defendant with sensitive and confidential information, including their names,
25 date of birth, Healthcare ID number, medical record information, including clinical information
26

27 ⁴ See <https://www.ttec.com/about-us> (last visited Feb. 8, 2022).

28 ⁵ [https://www.dnb.com/business-directory/company-profiles.ttec_services_corporation.558b8d1089a5686b32f5b6ebd0856163.html#:~:text=Ttec%20Services%20Corporation%20has%204%2C450,million%20in%20sales%20\(USD\)](https://www.dnb.com/business-directory/company-profiles.ttec_services_corporation.558b8d1089a5686b32f5b6ebd0856163.html#:~:text=Ttec%20Services%20Corporation%20has%204%2C450,million%20in%20sales%20(USD)) (last visited Feb. 8, 2022).

⁶ See <https://www.ttec.com/about-us> (last visited Feb. 8, 2022).

1 including diagnosis, and/or Social Security numbers, and other PII, which is static, does not
2 change, and can be used to commit countless different types of financial crimes.

3 20. Plaintiff and Class Members, as current and former employees and as customers of
4 Defendant, relied on the sophistication of Defendant to keep their PII confidential and securely
5 maintained, to use this information for business purposes only, and to make only authorized
6 disclosures of this information. Plaintiff and Class Members demand security to safeguard their
7 PII.

8 21. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff
9 and Class Members from involuntary disclosure to third parties.

10 22. TTEC promises to “take steps to ensure your personal data will be given adequate
11 protection as required by relevant data protection laws and TTEC’s internal policies.”⁷

12 23. TTEC states that it:
13 complies with the EU-US Privacy Shield and Swiss-US Privacy Shield frameworks
14 as set forth by the US Department of Commerce regarding the collection, use, and
15 retention of personal information transferred from the European Union (“EU”), the
16 United Kingdom or Switzerland to the United States in reliance on Privacy Shield.
17 TTEC has certified to the U.S. Department of Commerce that it adheres to the
18 Privacy Shield Principles (“Principles”) with respect to all such information. If
19 there is any conflict between the Principals and the language in this privacy
20 statement, the Principles will govern.⁸

21 24. TTEC’s commitment to the Privacy Shield Principles includes to “[u]pon notice,
22 take reasonable and appropriate steps to stop and remediate unauthorized processing[.]”⁹

23 ***The Data Breach***

24 25. Beginning on or about December 8, 2021, Defendant sent Plaintiff and other current
25 and former employees and customers a *Notice of Data Breach*. Defendant informed the recipients
26 of the notice that:

27 We learned that there was unauthorized activity in our network between March 31,
28 2021 and September 12, 2021. During that time, an unauthorized actor obtained
files stored on some of our servers. We completed a careful review of those files
and other files on the servers on November 24, 2021 and determined that one or
more of the files contained your name and Social Security number.

⁷ See <https://www.ttec.com/privacy-policy> (last visited Feb. 8, 2022).

⁸ See *id.*

⁹ See <https://www.privacyshield.gov/Key-New-Requirements> (last visited Feb. 8, 2022).

1 Other letters stated:

2 ***What Information Was Involved***

3 Your information involved in this incident included your name and one or more of
4 the following types of information:

- 5 · Date of Birth
- 6 · Healthcare ID Number
- 7 · Clinical Information Including Diagnosis

8 26. On or about December 8, 2021, Defendant sent data breach notifications to various
9 state Attorneys General, including Vermont, Maine and Montana’s Attorney General.¹⁰

10 27. Defendant admitted in the letters to the Attorneys General that unauthorized
11 individuals accessed directories that contained PII and were capable of “accessing and acquiring”
12 the PII, including individuals’ names, date of birth, Healthcare ID number, medical record
13 information, including clinical information including diagnosis, and/or Social Security numbers.

14 28. In response to the Data Breach, Defendant claims that “[a]s soon as TTEC learned
15 about the cyber security incident we immediately began an investigation, and cyber security firms
16 that have assisted other organizations with similar matters were engaged. We also notified law
17 enforcement and have been supporting their investigation.” The details of the root cause of the
18 Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a
19 breach does not occur again have not been shared with regulators or Plaintiff and Class Members,
20 who retain a vested interest in ensuring that their PII remains protected.¹¹

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

25 30. Defendant did not use reasonable security procedures and practices appropriate to
26 the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing

26 ¹⁰ See [https://ago.vermont.gov/blog/2021/12/11/ttec-services-corporation-data-breach-](https://ago.vermont.gov/blog/2021/12/11/ttec-services-corporation-data-breach-notice-to-consumers/)
27 [notice-to-consumers/](https://ago.vermont.gov/blog/2021/12/11/ttec-services-corporation-data-breach-notice-to-consumers/) (last visited Feb. 8, 2022);
28 [https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-](https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-9135d8726541.shtml)
[9135d8726541.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-9135d8726541.shtml) (with link to “Copy of notice to affected Maine residents: TTEC-ME App &
Sample.pdf” last visited Feb. 8, 2022); [https://media.dojmt.gov/wp-content/uploads/Consumer-](https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-133.pdf)
[Notification-Letter-133.pdf](https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-133.pdf) (last visited Feb. 8, 2022).

¹¹ See *id.*

1 the exposure of PII for many current and former employees, such as encrypting the information or
2 deleting it when it is no longer needed.

3 31. As explained by the Federal Bureau of Investigation, “[p]revention is the most
4 effective defense against ransomware and it is critical to take precautions for protection.”¹²

5 32. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
6 and should have implemented, as recommended by the United States Government, the following
7 measures:

- 8 • Implement an awareness and training program. Because end users are targets,
9 employees and individuals should be aware of the threat of ransomware and how it is
10 delivered.
- 11 • Enable strong spam filters to prevent phishing emails from reaching the end users and
12 authenticate inbound email using technologies like Sender Policy Framework (SPF),
13 Domain Message Authentication Reporting and Conformance (DMARC), and
14 DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- 15 • Scan all incoming and outgoing emails to detect threats and filter executable files from
16 reaching end users.
- 17 • Configure firewalls to block access to known malicious IP addresses.
- 18 • Patch operating systems, software, and firmware on devices. Consider using a
19 centralized patch management system.
- 20 • Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 21 • Manage the use of privileged accounts based on the principle of least privilege: no
22 users should be assigned administrative access unless absolutely needed; and those
23 with a need for administrator accounts should only use them when necessary.
- 24 • Configure access controls—including file, directory, and network share permissions—
25 with least privilege in mind. If a user only needs to read specific files, the user should
26 not have write access to those files, directories, or shares.
- 27 • Disable macro scripts from office files transmitted via email. Consider using Office
28

¹² See *How to Protect Your Networks from RANSOMWARE*, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 8, 2022).

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

- 3 • Implement Software Restriction Policies (SRP) or other controls to prevent programs
4 from executing from common ransomware locations, such as temporary folders
5 supporting popular Internet browsers or compression/decompression programs,
6 including the AppData/LocalAppData folder.
- 7 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 8 • Use application whitelisting, which only allows systems to execute programs known
9 and permitted by security policy.
- 10 • Execute operating system environments or specific programs in a virtualized
11 environment.
- 12 • Categorize data based on organizational value and implement physical and logical
13 separation of networks and data for different organizational units.¹³

14 33. To prevent and detect cyber-attacks Defendant could and should have implemented,
15 as recommended by the United States Cybersecurity & Infrastructure Security Agency, the
16 following measures, which direct organizations to:

- 17 • **Update and patch your computer.** Ensure your applications and operating systems
18 (OSs) have been updated with the latest patches. Vulnerable applications and OSs are
19 the target of most ransomware attacks....
- 20 • **Use caution with links and when entering website addresses.** Be careful when
21 clicking directly on links in emails, even if the sender appears to be someone you
22 know. Attempt to independently verify website addresses (*e.g.*, contact your
23 organization's helpdesk, search the internet for the sender organization's website or
24 the topic mentioned in the email). Pay attention to the website addresses you click on,
25 as well as those you enter yourself. Malicious website addresses often appear almost
26 identical to legitimate sites, often using a slight variation in spelling or a different
27 domain (*e.g.*, .com instead of .net)
- 28 • **Open email attachments with caution.** Be wary of opening email attachments, even

¹³ See *id.* at 3-4.

1 from senders you think you know, particularly when attachments are compressed files
2 or ZIP files.

- 3 • **Keep your personal information safe.** Check a website’s security to ensure the
4 information you submit is encrypted before you provide it....
- 5 • **Verify email senders.** If you are unsure whether or not an email is legitimate, try to
6 verify the email’s legitimacy by contacting the sender directly. Do not click on any
7 links in the email. If possible, use a previous (legitimate) email to ensure the contact
8 information you have for the sender is authentic before you contact them.
- 9 • **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to
10 date on ransomware techniques. You can find information about known phishing
11 attacks on the Anti-Phishing Working Group website. You may also want to sign up
12 for CISA product notifications, which will alert you when a new Alert, Analysis
13 Report, Bulletin, Current Activity, or Tip has been published.
- 14 • **Use and maintain preventative software programs.** Install antivirus software,
15 firewalls, and email filters—and keep them updated—to reduce malicious network
16 traffic....¹⁴

17 34. To prevent and detect cyber-attacks or ransomware attacks Defendant could and
18 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
19 the following measures:

20 **Secure internet-facing assets**

- 21 - Apply latest security updates
- 22 - Use threat and vulnerability management
- 23 - Perform regular audit; remove privileged credentials;

24 **Thoroughly investigate and remediate alerts**

- 25 - Prioritize and treat commodity malware infections as potential full
26 compromise;

27 **Include IT Pros in security discussions**

28

¹⁴ See *Security Tip (ST19-001) Protecting Against Ransomware* (original release date Apr. 11, 2019), <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Feb. 8, 2022).

- 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].¹⁵

35. Given that Defendant was storing the PII of its current and former employees and customers, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

36. The occurrence of the Data Breach indicates that Defendant failed to implement adequately one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former employees, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

37. Defendant has historically acquired, collected, and stored the PII of Plaintiff and

¹⁵ See *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Feb. 8, 2022).

1 Class Members.

2 38. As a condition of maintaining employment with Defendant, Defendant requires that
3 its employees entrust it with highly confidential PII. Defendant also collects information about
4 employees and customers who use its services, website and business tools. According to
5 Defendant's privacy policy, the information it collects may include:

6 ... personal data from you, such as your name, postal address, telephone number,
7 e-mail address, credit card number or other payment account number ... personal
8 identity numbers, financial account information, racial or ethnic origin, political
9 opinions, religious, philosophical or other similar beliefs, membership of a trade
10 union or profession or trade association, physical or mental health, biometric or
11 genetic data, sexual life, or criminal record (including information about suspected
12 criminal activities). Sensitive personal data may be collected and used in the context
of your employment application and relationship with TTEC, to provide you with
services you request, or to perform analysis that we may use to improve our website
or services and may be shared with our service providers for these purposes. ...¹⁶

13 39. By obtaining, collecting, and storing the PII of Plaintiff and Class Members,
14 Defendant assumed legal and equitable duties and knew or should have known that it was
15 responsible for protecting the PII from disclosure.

16 40. Plaintiff and Class Members have taken reasonable steps to maintain the
17 confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained
18 securely, to use this information for business purposes only, and to make only authorized
19 disclosures of this information.

20 41. In the ordinary course of doing business with Defendant, customers are required to
21 provide Defendant with PII, such as, but not limited to, payment information. Defendant collects
22 this payment information when it sells products and services. The payment information likely
23 includes financial account numbers, expiration dates, and CVC security codes to process payment
24 cards. Further, in the ordinary course of business Defendant collects and stores PII from
25 prospective, current, and former employees including full name, address, date of birth, Social
26 Security number, and other identifying information as described in paragraph 36.

27
28

¹⁶ See <https://www.ttec.com/privacy-policy> (last visited Feb. 8, 2022).

1 ***Securing PII and Preventing Breaches***

2 42. Defendant could have prevented this Data Breach by properly securing and
3 encrypting the files and file servers containing the PII of Plaintiff and Class Members.
4 Alternatively, Defendant could have destroyed the data, especially data from former employees.

5 43. Defendant’s policies on its website include promises and legal obligations to
6 maintain and protect PII, demonstrating an understanding of the importance of securing PII. For
7 example, Defendant’s Privacy Statement provides in part that it “take[s] reasonable steps to
8 maintain the security of personal data collected via TTEC’s websites.”¹⁷

9 44. Defendant’s negligence in safeguarding the PII of Plaintiff and Class Members is
10 exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

11 45. Despite the prevalence of public announcements of data breach and data security
12 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class
13 Members from being compromised.

14 46. Defendant does not claim that it abides by the Payment Card Industry Data Security
15 Standard (“PCI DSS”), which is a set of standards designed to ensure that all companies that
16 accept, process, store, or transmit credit card information maintain a secure environment. PCI
17 DSS compliance is a requirement for all businesses that store, process, or transmit payment card
18 data.

19 47. The PCI DSS defines measures for ensuring data protection and consistent security
20 processes and procedures around online financial transactions. Businesses that fail to maintain PCI
21 DSS compliance are subject to steep fines and penalties.

22 48. As formulated by the PCI Security Standards Council, the mandates of PCI DSS
23 compliance include, in part: Developing and maintaining a security policy that covers all aspects
24 of the business, installing firewalls to protect data, and encrypting payment data that is transmitted
25 over public networks using anti-virus software and updating it regularly.

26 ***Value of Personally Identifiable Information***

27 49. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
28

¹⁷ See <https://www.ttec.com/privacy-policy> (last visited Feb. 8, 2022).

1 committed or attempted using the identifying information of another person without authority.”¹⁸
 2 The FTC describes “identifying information” as “any name or number that may be used, alone or
 3 in conjunction with any other information, to identify a specific person,” including, among other
 4 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s
 5 license or identification number, alien registration number, government passport number,
 6 employer or taxpayer identification number.”¹⁹

7 50. The PII of individuals remains of high value to criminals, as evidenced by the prices
 8 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
 9 credentials. For example, Personal Information can be sold at a price ranging from \$40 to \$200,
 10 and bank details have a price range of \$50 to \$200.²⁰ Experian reports that a stolen credit or debit
 11 card number can sell for \$5 to \$110 on the dark web.²¹ Criminals can also purchase access to entire
 12 company data breaches from \$900 to \$4,500.²²

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

17 A dishonest person who has your Social Security number can use it to get other
 18 personal information about you. Identity thieves can use your number and your
 19 good credit to apply for more credit in your name. Then, they use the credit cards
 20 and don’t pay the bills, it damages your credit. You may not find out that someone
 21 is using your number until you’re turned down for credit, or you begin to get calls
 22 from unknown creditors demanding payment for items you never bought. Someone
 23 illegally using your Social Security number and assuming your identity can cause
 24 a lot of problems.²³

23 ¹⁸ 17 C.F.R. § 248.201 (2013).

24 ¹⁹ *Id.*

25 ²⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, DIGITAL
 26 TRENDS, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Feb. 8, 2022).

27 ²¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN,
 28 Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 8, 2022).

²² *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 8, 2022).

²³ Social Security Administration, *Identity Theft and Your Social Security Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Feb. 8, 2022).

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

6 53. Even then, a new Social Security number may not be effective. According to Julie
7 Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link
8 the new number very quickly to the old number, so all of that old bad information is quickly
9 inherited into the new Social Security number.”²⁴

10 54. Based on the foregoing, the information compromised in the Data Breach is
11 significantly more valuable than the loss of, for example, credit card information in a retailer data
12 breach because, there, victims can cancel or close credit and debit card accounts. The information
13 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
14 change—Social Security number, name, date of birth, information about a clinical evaluation or
15 diagnosis, or even a Healthcare ID number.

16 55. This data demands a much higher price on the black market. Martin Walter, senior
17 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
18 personally identifiable information and Social Security numbers are worth more than 10x on the
19 black market.”²⁵

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

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

24 58. There may be a time lag between when harm occurs versus when it is discovered,
25

26 ²⁴ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*,
27 NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Feb. 8, 2022).

28 ²⁵ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit
Card Numbers*, IT WORLD, (Feb. 6, 2015),
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Feb. 8, 2022).

1 and also between when PII is stolen and when it is used. According to the U.S. Government
2 Accountability Office (“GAO”), which conducted a study regarding data breaches:

3 [L]aw enforcement officials told us that in some cases, stolen data may be held for
4 up to a year or more before being used to commit identity theft. Further, once stolen
5 data have been sold or posted on the Web, fraudulent use of that information may
6 continue for years. As a result, studies that attempt to measure the harm resulting
7 from data breaches cannot necessarily rule out all future harm.²⁶

8 59. At all relevant times, Defendant knew, or reasonably should have known, of the
9 importance of safeguarding the PII of Plaintiff and Class Members, including Social Security
10 numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant’s
11 data security system was breached, including, specifically, the significant costs that would be
12 imposed on Plaintiff and Class Members as a result of a breach.

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

16 61. Defendant was, or should have been, fully aware of the unique type and the
17 significant volume of data on Defendant’s servers, amounting to potentially thousands of
18 individuals’ detailed, PII and, thus, the significant number of individuals who would be harmed
19 by the exposure of the unencrypted data.

20 62. In the breach notification letter, Defendant made an offer of 12 months of identity
21 monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it
22 fails to provide for the fact that victims of data breaches and other unauthorized disclosures
23 commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely
24 fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff’s
25 and Class Members’ PII.

26 63. The injuries to Plaintiff and Class Members were directly and proximately caused
27 by Defendant’s failure to implement or maintain adequate data security measures for the PII of
28 Plaintiff and Class Members.

64. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class

²⁶ *Report to Congressional Requesters*, GAO, at 29 (June 2007),
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Feb. 8, 2022).

1 Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers,
2 fraudulent use of that information and damage to victims may continue for years.

3 ***Plaintiff David Barocas's Experience***

4 65. Plaintiff Barocas was required to provide his PII to Defendant in connection with
5 his employment, which started in or about September of 2017 and ended in or about October 2017.
6 Plaintiff Barocas was also employed with Defendant in February of 2018.

7 66. On or about December 8, 2021, Plaintiff Barocas received notice from Defendant
8 that his PII had been improperly accessed and/or obtained by unauthorized third parties. This
9 notice indicated that Plaintiff Barocas' PII, including name and Social Security number, was
10 compromised as a result of the Data Breach.

11 67. Plaintiff Barocas made reasonable efforts to mitigate the impact of the Data Breach,
12 including but not limited to: researching the Data Breach; reviewing credit reports and financial
13 account statements for any indications of actual or attempted identity theft or fraud; researching
14 and signing up for credit monitoring and identity theft protection services offered by Defendant;
15 and contacting creditors and credit bureaus. Plaintiff Barocas has spent at least five hours dealing
16 with the Data Breach, valuable time Plaintiff Barocas otherwise would have spent on other
17 activities, including but not limited to work and/or recreation.

18 68. As a result of the Data Breach, Plaintiff Barocas has suffered emotional distress due
19 to the release of his PII, which he believed would be protected from unauthorized access and
20 disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for
21 purposes of identity theft and fraud. Plaintiff Barocas is very concerned about identity theft and
22 fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

23 69. Plaintiff Barocas suffered actual injury from having his PII compromised as a result
24 of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his
25 PII, a form of property that Defendant obtained from Plaintiff Barocas; (b) violation of his privacy
26 rights; and (c) present, imminent and impending injury arising from the increased risk of identity
27 theft and fraud.

28 70. As a result of the Data Breach, Plaintiff Barocas anticipates spending considerable
time and money on an ongoing basis to try to mitigate and address harms caused by the Data

1 Breach. As a result of the Data Breach, Plaintiff Barocas is at a present risk and will continue to
2 be at increased risk of identity theft and fraud for years to come.

3 **V. CLASS ALLEGATIONS**

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

7 **All individuals residing in the United States whose PII was compromised in**
8 **the data breach first announced by Defendant on or about December 8, 2021**
9 **(the “Nationwide Class”).**

10 72. The Arizona Subclass is defined as follows:

11 **All individuals residing in Arizona whose PII was compromised in the data**
12 **breach first announced by Defendant on or about December 8, 2021 (the**
13 **“Arizona Subclass”).**

14 The Nationwide Class and Arizona Subclass are collectively referred to herein as the “Class.”

15 73. Excluded from the Class are the following individuals and/or entities: Defendant
16 and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which
17 Defendant has a controlling interest; all individuals who make a timely election to be excluded
18 from this proceeding using the correct protocol for opting out; and all judges assigned to hear any
19 aspect of this litigation, as well as their immediate family members.

20 74. Plaintiff reserves the right to modify or amend the definition of the proposed Class
21 before the Court determines whether certification is appropriate.

22 75. Numerosity, Fed. R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all
23 members is impracticable. The Class is apparently identifiable within Defendant’s records.

24 76. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact
25 common to the Class exist and predominate over any questions affecting only individual Class
26 Members. These include:

- 27 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and
28 Class Members;
- b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members
to unauthorized third parties;
- c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for

1 non-business purposes;

2 d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class
3 Members;

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

5 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and
6 Class Members that their PII had been compromised;

7 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class
8 Members that their PII had been compromised;

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

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

14 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
15 safeguard the PII of Plaintiff and Class Members;

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

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

20 m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
21 imminent and currently ongoing harm faced as a result of the Data Breach.

22 77. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other
23 Class Members because he had his PII compromised as a result of the Data Breach due to
24 Defendant's misfeasance.

25 78. Policies Generally Applicable to the Class: This class action is also appropriate for
26 certification because Defendant acted or refused to act on grounds generally applicable to the
27 Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
28 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

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

3 79. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent
4 and protect the interests of the Class Members in that he has no disabling conflicts of interest that
5 would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is
6 antagonistic or adverse to the Members of the Class and the infringement of the rights and the
7 damages he has suffered are typical of other Class Members. Plaintiff has retained counsel
8 experienced in complex class action litigation, and Plaintiff intends to prosecute this action
9 vigorously.

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

20 81. The nature of this action and the nature of laws available to Plaintiff and Class
21 Members make the use of the class action device a particularly efficient and appropriate procedure
22 to afford relief to Plaintiff and Class Members for the wrongs alleged for the following reasons:
23 (i) Defendant would necessarily gain an unconscionable advantage since it would be able to exploit
24 and overwhelm the limited resources of each individual Class Member with superior financial and
25 legal resources; (ii) the costs of individual suits could unreasonably consume the amounts that
26 would be recovered; (iii) proof of a common course of conduct to which Plaintiff was exposed is
27 representative of that experienced by the Class and will establish the right of each Class Member
28 to recover on the cause of action alleged; and (iv) individual actions would create a risk of
inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

7 84. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
8 properly secure the PII of Class Members, Defendant may continue to refuse to provide proper
9 notification to Class Members regarding the Data Breach, and Defendant may continue to act
10 unlawfully as set forth in this Complaint.

11 85. Further, Defendant has acted or refused to act on grounds generally applicable to
12 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the
13 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
14 Procedure.

15 86. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification
16 because such claims present only particular, common issues, the resolution of which would
17 advance the disposition of this matter and the parties' interests therein. Such particular issues
18 include, but are not limited to:

- 19 a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise
20 due care in collecting, storing, using, and safeguarding their PII;
- 21 b. Whether Defendant breached a legal duty to Plaintiff and Class Members to
22 exercise due care in collecting, storing, using, and safeguarding their PII;
- 23 c. Whether Defendant failed to comply with its own policies and applicable laws,
24 regulations, and industry standards relating to data security;
- 25 d. Whether an implied contract existed between Defendant on the one hand, and
26 Plaintiff and Class Members on the other, and the terms of that implied contract;
- 27 e. Whether Defendant breached the implied contract;
- 28 f. Whether Defendant adequately and accurately informed Plaintiff and Class
Members that their PII had been compromised;

- 1 g. Whether Defendant failed to implement and maintain reasonable security
2 procedures and practices appropriate to the nature and scope of the information
3 compromised in the Data Breach;
- 4 h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing
5 to safeguard the PII of Plaintiff and Class Members; and,
- 6 i. Whether Class Members are entitled to actual damages, statutory damages,
7 nominal damages, and/or injunctive relief as a result of Defendant's wrongful
8 conduct.

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

12 87. Plaintiff and the Class re-allege and incorporate by reference herein all of the
13 allegations contained in paragraphs 1 through 86.

14 88. As a condition of their employment with Defendant or by purchasing goods or
15 services from Defendant, Defendant's current and former employees and customers were obligated
16 to provide Defendant with PII, among other sensitive PII, their names, dates of birth, and Social
17 Security numbers.

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

21 90. Defendant has full knowledge of the sensitivity of the PII and the types of harm that
22 Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

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

27 92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
28 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 of Plaintiff and the Class in Defendant's

1 possession was adequately secured and protected.

2 93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
3 former employees' PII that Defendant was no longer required to retain pursuant to regulations.

4 94. Defendant also had a duty to have procedures in place to detect and prevent the
5 improper access and misuse of the PII of Plaintiff and the Class.

6 95. Defendant's duty to use reasonable security measures arose as a result of the special
7 relationship that existed between Defendant and Plaintiff and the Class. That special relationship
8 arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary
9 part of employment with the company or making purchases from Defendant.

10 96. Defendant was subject to an "independent duty," untethered to any contract
11 between Defendant and Plaintiff or the Class.

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

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

20 99. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the
21 Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and
22 opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included
23 its decisions to not comply with industry standards for the safekeeping of the PII of Plaintiff and
24 the Class, including basic encryption techniques freely available to Defendant.

25 100. Plaintiff and the Class had no ability to protect their PII that was in, and possibly
26 remains in, Defendant's possession.

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

102. Defendant had and continues to have a duty to adequately disclose that the PII of

1 Plaintiff and the Class within Defendant's possession might have been compromised, how it was
2 compromised, and precisely the types of data that were compromised and when. Such notice was
3 necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity
4 theft and the fraudulent use of their PII by third parties.

5 103. Defendant had a duty to employ proper procedures to prevent the unauthorized
6 dissemination of the PII of Plaintiff and the Class.

7 104. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost
8 and disclosed to unauthorized third persons as a result of the Data Breach.

9 105. Defendant, through its actions and/or omissions, unlawfully breached its duties to
10 Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in
11 protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within
12 Defendant's possession or control.

13 106. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the
14 Class in deviation of standard industry rules, regulations, and practices at the time of the Data
15 Breach.

16 107. Defendant failed to heed industry warnings and alerts to provide adequate
17 safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

18 108. Defendant, through its actions and/or omissions, unlawfully breached its duty to
19 Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent
20 dissemination of its current and former employees' PII.

21 109. Defendant, through its actions and/or omissions, unlawfully breached its duty to
22 adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data
23 Breach.

24 110. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
25 the Class, the PII of Plaintiff and the Class would not have been compromised.

26 111. There is a close causal connection between Defendant's failure to implement
27 security measures to protect the PII of Plaintiff and the Class and the present harm, or risk of
28 imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and
accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding

1 such PII by adopting, implementing, and maintaining appropriate security measures.

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

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

12 114. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

13 115. Plaintiff and the Class are within the class of persons that the FTC Act was intended
14 to protect.

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

19 117. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
20 Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual
21 identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise,
22 publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,
23 detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost
24 opportunity costs associated with effort expended and the loss of productivity addressing and
25 attempting to mitigate the actual present and future consequences of the Data Breach, including
26 but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax
27 fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the
28 continued risk to their PII, which remain in Defendant’s possession and is subject to further
unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

1 measures to protect the PII of Plaintiff and the Class; and (viii) costs in terms of time, effort, and
2 money that will be expended to prevent, detect, contest, and repair the impact of the PII
3 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

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

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

13 120. Plaintiff and Class Members are therefore entitled to damages, including restitution
14 and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

15 **COUNT II**
16 **BREACH OF IMPLIED CONTRACT**
17 **(On Behalf of Plaintiff and the Nationwide Class)**

18 121. Plaintiff and the Class re-allege and incorporate by reference herein all of the
19 allegations contained in paragraphs 1 through 86.

20 122. Defendant required Plaintiff and the Class to provide their PII, including names,
21 dates of birth, Social Security numbers and other PII, as a condition of their employment or
22 purchases.

23 123. As a condition of their employment with or purchases from Defendant, Plaintiff and
24 the Class provided their PII. In so doing, Plaintiff and the Class entered into implied contracts with
25 Defendant by which Defendant agreed to safeguard and protect such information, to keep such
26 information secure and confidential, and to timely and accurately notify Plaintiff and the Class if
27 their data had been breached and compromised or stolen.

28 124. Plaintiff and the Class fully performed their obligations under the implied contracts
with Defendant.

1 125. Defendant breached the implied contracts it made with Plaintiff and the Class by
2 failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to
3 them that their PII was compromised as a result of the Data Breach.

4 126. As a direct and proximate result of Defendant's above-described breach of implied
5 contract, Plaintiff and the Class have suffered (and will continue to suffer): ongoing, imminent,
6 and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and
7 economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and
8 economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the
9 compromised data on the dark web; expenses and/or time spent on credit monitoring and identity
10 theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;
11 expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work
12 time; and other economic and non-economic harm.

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

16 127. Plaintiff and the Class re-allege and incorporate by reference herein all of the
17 allegations contained in paragraphs 1 through 86.

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

20 129. Defendant owed a duty to its current and former customers and employees,
21 including Plaintiff and the Class, to keep their PII confidential.

22 130. Defendant failed to protect and released to unknown and unauthorized third parties
23 the PII of Plaintiff and the Class.

24 131. Defendant allowed unauthorized and unknown third parties access to and
25 examination of the PII of Plaintiff and the Class, by way of Defendant's failure to protect the PII.

26 132. The unauthorized release to, custody of, and examination by unauthorized third
27 parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

28 133. The intrusion was into a place or thing which was private and is entitled to be
private. Plaintiff and the Class disclosed their PII to Defendant as part of the current and former
employees' employment with Defendant and/or during a consumer transaction with Defendant,

1 but privately with an intention that the PII would be kept confidential and would be protected from
2 unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such
3 information would be kept private and would not be disclosed without their authorization.

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

7 135. Defendant acted with a knowing state of mind when it permitted the Data Breach
8 to occur because it was with actual knowledge that its information security practices were
9 inadequate and insufficient.

10 136. Because Defendant acted with this knowing state of mind, it had notice and knew
11 the inadequate and insufficient information security practices would cause injury and harm to
12 Plaintiff and the Class.

13 137. As a proximate result of the above acts and omissions of Defendant, the PII of
14 Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and
15 the Class to suffer damages.

16 138. Unless and until enjoined, and restrained by order of this Court, Defendant's
17 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in
18 that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons
19 for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a
20 judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

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

24 139. Plaintiff and the Class re-allege and incorporate by reference herein all of the
25 allegations contained in paragraphs 1 through 86.

26 140. At all times during Plaintiff's and the Class's interactions with Defendant,
27 Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's
28 PII that Plaintiff and the Class provided to Defendant.

1 141. As alleged herein and above, Defendant's relationship with Plaintiff and the Class
2 was governed by terms and expectations that Plaintiff's and the Class's PII would be collected,
3 stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

4 142. Plaintiff and the Class provided their PII to Defendant with the explicit and implicit
5 understandings that Defendant would protect and not permit the PII to be disseminated to any
6 unauthorized third parties.

7 143. Plaintiff and the Class also provided Plaintiff's and the Class's PII to Defendant
8 with the explicit and implicit understanding that Defendant would take precautions to protect that
9 PII from unauthorized disclosure.

10 144. Defendant voluntarily received in confidence Plaintiff's and the Class's PII with
11 the understanding that PII would not be disclosed or disseminated to the public or any unauthorized
12 third parties.

13 145. Due to Defendant's failure to prevent and avoid the Data Breach from occurring,
14 Plaintiff's and the Class's PII was disclosed and misappropriated to unauthorized third parties
15 beyond Plaintiff's and the Class's confidence, and without their express permission.

16 146. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff
17 and the Class have suffered damages.

18 147. But for Defendant's disclosure of Plaintiff's and the Class's PII in violation of the
19 parties' understanding of confidence, their PII would not have been compromised, stolen, viewed,
20 accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal
21 cause of the theft of Plaintiff's and the Class's PII as well as the resulting damages.

22 148. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable
23 result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII. Defendant knew
24 or should have known its methods of accepting and securing Plaintiff's and the Class's PII was
25 inadequate as it relates to, at the very least, securing servers and other equipment containing
26 Plaintiff's and the Class's PII.

27 149. As a direct and proximate result of Defendant's breach of its confidence with
28 Plaintiff and the Class, 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 how their PII is used; (iii) the

1 compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the
2 prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their
3 PII; (v) lost opportunity costs associated with effort expended and the loss of productivity
4 addressing and attempting to mitigate the actual present and future consequences of the Data
5 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and
6 recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit
7 reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject
8 to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
9 adequate measures to protect the PII of current and former customers and employees; and (viii)
10 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
11 contest, and repair the impact of the PII compromised as a result of the Data Breach for the
12 remainder of the lives of Plaintiff and the Class.

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

17 **COUNT V**
18 **UNJUST ENRICHMENT**
19 **(On Behalf of Plaintiff and the Nationwide Class)**

20 151. Plaintiff and the Class re-allege and incorporate by reference herein all of the
21 allegations contained in paragraphs 1 through 86.

22 152. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability
23 to retain and use that information for its own benefit. Defendant understood this benefit.

24 153. Defendant also understood and appreciated that Plaintiff's and Class Members' PII
25 was private and confidential, and its value depended upon Defendant maintaining the privacy and
26 confidentiality of that PII.

27 154. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the
28 form of their employment and by purchasing goods from Defendant, and in connection thereto, by
providing their PII to Defendant with the understanding that Defendant would pay for the
administrative costs of reasonable data privacy and security practices and procedures. Specifically,

1 they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members
2 should have received adequate protection and data security for such PII held by Defendant.

3 155. Defendant knew Plaintiff and Class members conferred a benefit which Defendant
4 accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class
5 Members for business purposes.

6 156. Defendant failed to provide reasonable security, safeguards, and protections to the
7 PII of Plaintiff and Class Members.

8 157. Under the principles of equity and good conscience, Defendant should not be
9 permitted to retain money belonging to Plaintiff and Class members, because Defendant failed to
10 implement appropriate data management and security measures mandated by industry standards.

11 158. Defendant wrongfully accepted and retained these benefits to the detriment of
12 Plaintiff and Class Members.

13 159. Defendant's enrichment at the expense of Plaintiff and Class Members is and was
14 unjust.

15 160. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the
16 Class Members are entitled to restitution and disgorgement of all profits, benefits, and other
17 compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

18
19 **COUNT VI**
20 **VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT**
21 **A.R.S. REV. STAT. § 44-1522 *et seq.***
22 **(On Behalf of Plaintiff and the Arizona Subclass)**

23 161. Plaintiff and the Arizona Class re-alleges and incorporates by reference herein all
24 of the allegations contained in paragraphs 1 through 86.

25 162. Plaintiff and the Arizona Class Members were employed by Defendant and were
26 engaged in transactions and conduct to procure merchandise or services in connection with
27 Defendant.

28 163. Defendant engaged in transactions and conduct to procure merchandise or services
on behalf of Plaintiff and Class Members as defined by Arizona Revised Statutes ("A.R.S.") § 44-
1521(5).

1 164. Defendant engaged in trade and commerce through its acts and omissions and its
2 course of business, including marketing, offering to sell, and selling sporting goods throughout the
3 United States.

4 165. Defendant violated A.R.S. section 44-1522, *et seq.* by engaging in deceptive, unfair,
5 and unlawful trade acts or practices that were committed in Arizona, while conducting trade or
6 commerce in Arizona. Defendant's violations include, but are not limited to:

- 7 a. A failure to safeguard customer PII through data security practices and computer
8 systems;
- 9 b. A failure to disclose that their computer systems and data security practices were
10 inadequate to protect PII;
- 11 c. A failure to notify Plaintiff and Class Members in a timely manner of the data
12 breach;
- 13 d. A failure to stop accepting and storing PII after the Defendant knew or should
14 have known that the vulnerabilities were exploited in a data breach;
- 15 e. A failure to remediate the vulnerabilities that allowed the Data Breach to happen.
- 16 f. A misrepresentation and/or omission regarding its commitment to give adequate
17 protection to PII; and
- 18 g. A failure to take reasonable and appropriate steps to stop and remediate
19 unauthorized processing.

20 166. These unfair acts and practices violate the duties imposed by, but not limited to, the
21 FTCA and A.R.S. section 44-1522(A).

22 167. As a direct result of these violations, Plaintiff and Class Members suffered damages.
23 These damages include, but are not limited to:

- 24 a. Lost time spent constantly checking their credit for unauthorized activity, which
25 is necessary to do to protect themselves from the consequences of having their
26 PII available on the dark web because of the Data Breach; and
- 27 b. Other economic damage that may not be detected for years to come.

1 168. Plaintiff and Class Members are entitled to damages as well as injunctive relief
2 because of Defendant's knowing violation of Arizona Consumer Fraud Act. These include, but are
3 not limited to, ordering that Defendant:

- 4 a. Utilize third-party security professionals to regularly test for security
5 vulnerabilities;
- 6 b. Utilize third-party security professionals and internal personnel to perform
7 automated security monitoring;
- 8 c. Train security personnel on how to audit and test any new or modified security
9 protocols;
- 10 d. Protect data by securing it separately from other portions of the network;
- 11 e. Delete PII that is no longer necessary to provide services;
- 12 f. Conduct regular database security checks;
- 13 g. Provide regular training to internal security personnel on how to identify and
14 contain a breach and what to do when a breach occurs; and
- 15 h. Educate class members about the threats they face now that their PII is available
16 to unauthorized third parties and steps that patients can take to protect
17 themselves.

18 169. Plaintiff brings this action on behalf of himself and Arizona Class Members for the
19 relief requested above. This action will also protect the public from Defendant's unfair methods
20 of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

21 170. The deceptive practices and acts by Defendant were immoral, unethical, oppressive,
22 and unscrupulous. The acts caused substantial injury to Plaintiff and Arizona Class Members that
23 they could not reasonably avoid and the injuries suffered outweigh any benefit to patient-
24 consumers or to competition.

25 171. Defendant knew or should have known that the computer systems and data security
26 protocols were inadequate to store sensitive PII, which put the data at an increased risk of theft or
27 breach.

28 172. Defendant's unfair practices and deceptive acts were negligent, knowing and
willful, and/or wanton and reckless.

1 173. Plaintiff and Arizona Class Members seek relief under the Arizona Consumer Fraud
2 Act (A.R.S. § 44-1522(A)). The relief includes, but is not limited to, damages, restitution,
3 injunction relief, and/or attorney fees and costs, and any other just and proper relief.

4 **PRAYER FOR RELIEF**

5 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, request judgment
6 against Defendant and that the Court grant the following:

- 7 A. For an Order certifying the Class, as defined herein, and appointing Plaintiff and
8 his Counsel to represent each such Class;
- 9 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
10 complained of herein pertaining to the misuse and/or disclosure of the PII of
11 Plaintiff and Class Members, and from refusing to issue prompt, complete, any
12 accurate disclosures to Plaintiff and Class Members;
- 13 C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive
14 and other equitable relief as is necessary to protect the interests of Plaintiff and
15 Class Members, including but not limited to an order:
- 16 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
17 described herein;
- 18 ii. requiring Defendant to protect, including through encryption, all data collected
19 through the course of its business in accordance with all applicable regulations,
20 industry standards, and federal, state or local laws;
- 21 iii. requiring Defendant to delete, destroy, and purge the personal identifying
22 information of Plaintiff and Class Members unless Defendant can provide to
23 the Court reasonable justification for the retention and use of such information
24 when weighed against the privacy interests of Plaintiff and Class Members;
- 25 iv. requiring Defendant to implement and maintain a comprehensive Information
26 Security Program designed to protect the confidentiality and integrity of the PII
27 of Plaintiff and Class Members;
- 28 v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members
on a cloud-based database;

- 1 vi. requiring Defendant to engage independent third-party security
2 auditors/penetration testers as well as internal security personnel to conduct
3 testing, including simulated attacks, penetration tests, and audits on
4 Defendant's systems on a periodic basis, and ordering Defendant to promptly
5 correct any problems or issues detected by such third-party security auditors;
- 6 vii. requiring Defendant to engage independent third-party security auditors and
7 internal personnel to run automated security monitoring;
- 8 viii. requiring Defendant to audit, test, and train its security personnel regarding any
9 new or modified procedures;
- 10 ix. requiring Defendant to segment data by, among other things, creating firewalls
11 and access controls so that if one area of Defendant's network is compromised,
12 hackers cannot gain access to other portions of Defendant's systems;
- 13 x. requiring Defendant to conduct regular database scanning and securing checks;
- 14 xi. requiring Defendant to establish an information security training program that
15 includes at least annual information security training for all employees, with
16 additional training to be provided as appropriate based upon the employees'
17 respective responsibilities with handling personal identifying information, as
18 well as protecting the personal identifying information of Plaintiff and Class
19 Members;
- 20 xii. requiring Defendant to routinely and continually conduct internal training and
21 education, and on an annual basis to inform internal security personnel how to
22 identify and contain a breach when it occurs and what to do in response to a
23 breach;
- 24 xiii. requiring Defendant to implement a system of tests to assess its respective
25 employees' knowledge of the education programs discussed in the preceding
26 subparagraphs, as well as randomly and periodically testing employees'
27 compliance with Defendant's policies, programs, and systems for protecting
28 personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as

1 necessary a threat management program designed to appropriately monitor
2 Defendant's information networks for threats, both internal and external, and
3 assess whether monitoring tools are appropriately configured, tested, and
4 updated;

5 xv. requiring Defendant to meaningfully educate all Class Members about the
6 threats that they face as a result of the loss of their confidential PII to third
7 parties, as well as the steps affected individuals must take to protect themselves;

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

15 D. For an award of damages, including actual, statutory, nominal, and consequential
16 damages, as allowed by law in an amount to be determined;

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

18 F. For prejudgment interest on all amounts awarded; and

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

20 **DEMAND FOR JURY TRIAL**

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

22
23 Dated: February 8, 2022

Respectfully Submitted,

24 **WOLF HALDENSTEIN ADLER**
25 **FREEMAN & HERZ LLP**

26 By: /s/ Betsy C. Manifold
27 **BETSY C. MANIFOLD**

28 **BETSY C. MANIFOLD** (*pro hac vice* forthcoming)
RACHELE R. BYRD (*pro hac vice* forthcoming)
OANA CONSTANTIN (*pro hac vice* forthcoming)
750 B Street, Suite 1820
San Diego, CA 92101

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Telephone: (619) 239-4599
Facsimile: (619) 234-4599
manifold@whafh.com
byrd@whafh.com
constantin@whafh.com

M. ANDERSON BERRY (*pro hac vice*
forthcoming)
GREGORY HAROUTUNIAN (*pro hac vice*
forthcoming)

**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**

865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

*Attorneys for Plaintiff and
the Proposed Class*

28009v6

**UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA**

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): David Barocas

Defendant(s): TTEC Services Corporation

County of Residence: Maricopa

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Defendant's Atty(s):

**Betsy C. Manifold
Wolf Haldenstein Adler Freeman & Herz LLP
750 B Street, Suite 1820
San Diego, California 92101
619-239-4599**

II. Basis of Jurisdiction: 4. Diversity (complete item III)

III. Citizenship of Principal Parties (Diversity Cases Only)

Plaintiff: - **1 Citizen of This State**
Defendant: - **5 Non AZ corp and Principal place of Business outside AZ**

IV. Origin : 1. Original Proceeding

V. Nature of Suit: 360 Other Personal Injury

VI. Cause of Action: A.R.S. REV. STAT. § 44-1522 et seq.

VII. Requested in Complaint

Class Action: **Yes**
Dollar Demand:
Jury Demand: **Yes**

VIII. This case is not related to another case.

Signature: /s/ Betsy C. Manifold

Date: 2/8/2022

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [TTEC Services Corp. Facing Another Class Action Over 2021 Data Breach](#)
