SUM-100

SUMMONS
(CITACION JUDICIAL)

FOR COURT USE ONLY
(SOLO PARA USO DE LA CORTE)

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):
THE GAY AND LESBIAN COMMUNITY SERVICES CENTER OF ORANGE COUNTY, a California corporation; and DOES 1-50, Inclusive,

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):
DANIEL MARTINEZ, an individual, on behalf of Plaintiff, and on behalf of all persons similarly situated,

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (*www.lawhelpcalifornia.org*), the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of $10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.
¡AVISO! *Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.*

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, (www.lawhelpcalifornia.org), en el Centro de Ayuda de las Cortes de California, (www.sucorte.ca.gov) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de $10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:
(El nombre y dirección de la corte es): Orange County Superior Court

Civil Complex Center - 751 West Santa Ana Blvd., Santa Ana, CA 92701

CASE NUMBER:
(Número del Caso): 30-2026-01577422-CU-MT-CXC

Judge Layne H. Melzer

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Shani O. Zakay, Esq.; Zakay Law Group, APLC - 3110 Camino Del Rio S, Suite 308, San Diego, CA 92108; T:(619) 255-9047

DATE: 06/11/2026 *(Fecha)* DAVID H. YAMASAKI, Clerk of the Court Clerk, by *(Secretario)* S. Juarez S. Juarez, Deputy *(Adjunto)*

(For proof of service of this summons, use Proof of Service of Summons *(form POS-010).)*
(Para prueba de entrega de esta citatión use el formulario Proof of Service of Summons, *(POS-010)).*

NOTICE TO THE PERSON SERVED: You are served
1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of *(specify):*
3. ☐ on behalf of *(specify):*
   under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
   ☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
   ☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
   ☐ other *(specify):*
4. ☐ by personal delivery on *(date)*:

Form Adopted for Mandatory Use
Judicial Council of California
SUM-100 [Rev. July 1, 2009]

SUMMONS

Code of Civil Procedure §§ 412.20, 465
www.courts.ca.gov

ZAKAY LAW GROUP, APLC
Shani O. Zakay (State Bar #277924)
shani@zakaylaw.com
Jackland K. Hom (State Bar #327243)
jackland@zakaylaw.com
Eden Zakay (State Bar #339536)
eden@zakaylaw.com
3110 Camino Del Rio S, Suite 308
San Diego, CA 92108
Telephone: (619) 255-9047

Attorneys for PLAINTIFF

Assigned for All purposes:
Judge Layne H. Melzer
Dep. CX102

SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF ORANGE

DANIEL MARTINEZ, an individual, on behalf of Plaintiff, and on behalf of all persons similarly situated,

Plaintiff,

v.

THE GAY AND LESBIAN COMMUNITY SERVICES CENTER OF ORANGE COUNTY, a California corporation; and DOES 1-50, Inclusive,

Defendants.

Case No: 30-2026-01577422-CU-MT-CXC

CLASS ACTION COMPLAINT FOR:

1) NEGLIGENCE
2) NEGLIGENCE *PER SE*
3) BREACH OF IMPLIED CONTRACT
4) BREACH OF FIDUCIARY DUTY
5) BREACH OF CONFIDENCE
6) INVASION OF PRIVACY
7) UNJUST ENRICHMENT
8) VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et sq.*
9) VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE §§ 1798.80
10) VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE §§ 1798.150, *et. seq.*
11) VIOLATIONS OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CA. CIV. CODE §§ 56, et seq.

DEMAND FOR A JURY TRIAL

DANIEL MARTINEZ ("Plaintiff" or "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against THE GAY AND LESBIAN COMMUNITY SERVICES CENTER OF ORANGE COUNTY ("Defendant") for its failure to properly safeguard patients' personal information and protected health information stored within Defendant's information network. Plaintiff makes these allegations based on their personal knowledge with respect to their own experiences and actions, and on information and belief as to all other matters, derived from the investigation conducted by and through their counsel.

INTRODUCTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Defendant, which collected and stored certain personally identifying information ('PII') and protected health information ('PHI')" (collectively, the "Private Information") of Plaintiff and the class members.

2. Defendant provides counseling, advocacy, outreach, and health services for members of the LGBTQ community in Orange County. Headquartered in Santa Ana, California, Defendant serves thousands of patients seeking counseling, advocacy, outreach, and health services, and maintains detailed patient files and medical records as part of its operations. In the course of providing these services, Defendant collects and stores extensive personal and medical information from patients—including full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information. Defendant's size, scope, and the sensitive nature of the information it maintains make it a significant repository of confidential personal and medical data for California residents who entrust it with their care.

3. To effectively provide counseling, advocacy, outreach, and health services to thousands of patients, Defendant collects and stores vast amounts of sensitive Private Information. This information includes patients' full name, date of birth, Social Security number, diagnosis

information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information used for billing and care coordination. Defendant owes a duty of care to the individuals whose data it obtains and maintains. This duty arises because it is reasonably foreseeable that the exposure of such Private Information to unauthorized individuals—particularly cybercriminals seeking to exploit or sell the data—would cause substantial harm to affected persons. Such harm includes, but is not limited to, invasion of privacy, identity theft, fraudulent financial activity, exposure to phishing and scams, loss of time and resources spent securing one's identity and medical information, and the ongoing anxiety and loss of peace of mind resulting from knowing that one's most sensitive personal and medical data is no longer secure.

4. In light of the severe consequences of compromised Private Information, individuals reasonably expect that their data will be properly safeguarded. That trust is violated when entities like Defendant fail to implement adequate safeguards, thereby exposing themselves and the individuals whose data they hold to the risk of cyberattacks.

5. The U.S. Department of Health and Human Services ("HHS") has repeatedly warned organizations that store sensitive personal or health information about the growing threat of ransomware and other cyberattacks. In a joint advisory, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), the Federal Bureau of Investigation ("FBI"), and HHS specifically cautioned that cybercriminal groups are actively targeting entities that maintain such information.[1]

6. Despite being on notice that it was storing sensitive Private Information—data that is both valuable and highly sought after by cybercriminals—Defendant failed to implement and maintain basic security measures that could have prevented the unauthorized access and protected Plaintiff's and Class Members' information.

[1] See, e.g., Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation & U.S. Department of Health and Human Services, Joint Advisory: *Protecting Against Interlock Ransomware* (July 22, 2025), https://www.cisa.gov/news-events/alerts/2025/07/22/joint-advisory-issued-protecting-against-interlock-ransomware; Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation & U.S. Department of Health and Human Services, Joint Cybersecurity Advisory: *Ransomware Activity Targeting the Healthcare and Public Health Sector*, https://www.cisa.gov/stopransomware/ransomware-activity-targeting-healthcare-and-public-health-sector.

7. On or about June 5, 2026, Defendant disclosed that it had detected suspicious activity within its computer network. Following further investigation, Defendant determined that an unauthorized actor had infiltrated its systems and accessed, and potentially exfiltrated, files containing the personal and medical information of Plaintiff and Class Members.

8. On or about June 5, 2026, over six month after the data breach began, Defendant issued a written "Notice of Data Breach" to affected individuals. In that notice, Defendant disclosed that an unauthorized actor had accessed its computer systems between approximately December 25, 2025 and December 26, 2025, and had obtained certain data from its internal network. The notice further confirmed that Defendant had been aware of the suspicious activity for some time before notifying affected individuals.

9. For approximately 162 days, unauthorized actors maintained access to Defendant's network and obtained sensitive information that federal and state law require businesses to safeguard. This information included, but was not limited to, full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information.

10. Plaintiff and Class Members have already suffered harm as a result of the Data Breach and continue to face a substantial and ongoing risk of future misuse of their Private Information. The exposure of such data leaves them perpetually susceptible to fraud, identity theft, and other malicious activity. Critically, Social Security numbers, and government-issued identification numbers are permanent identifiers that cannot be readily replaced or changed, ensuring that the risk to affected individuals will persist indefinitely.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity measures necessary to protect Private Information. Specifically, Defendant violated its duty to safeguard such information and disregarded the rights of Plaintiff and Class Members by: (a) failing to adopt and maintain reasonable administrative, technical, and

physical safeguards to secure its databases and information technology systems; (b) concealing or omitting the material fact that it lacked sufficient systems and procedures to protect Private Information from unauthorized access; (c) failing to take available measures to detect, prevent, and contain the Data Breach; (d) failing to properly monitor its networks and systems, thereby delaying detection and response; and (e) failing to provide Plaintiff and Class Members with timely and accurate notice of the Data Breach.

12. As a result of Defendant's inadequate security measures, negligence, and other data protection failures, Class Members face an ongoing and substantial risk of harm. They remain exposed to potential misuse of their information, including the fraudulent opening of financial accounts, unauthorized loans, false applications for government benefits, the filing of fraudulent tax returns, and the submission of false medical or insurance claims in their names.

13. Plaintiff and Class Members maintain a strong and ongoing interest in ensuring that their Private Information, which remains in Defendant's possession, is adequately protected from further unauthorized access or disclosure. They also seek to remedy the harms and risks they have suffered and continue to face as a result of the Data Breach.

14. Plaintiff, individually and on behalf of all others similarly situated, seeks to recover damages, equitable relief—including injunctive measures to prevent a recurrence of the Data Breach and its resulting harm—restitution, disgorgement, reasonable attorneys' fees and costs, and all other relief the Court deems just and appropriate.

THE PARTIES

15. Plaintiff is, and at all relevant times was, a resident of California. Plaintiff relied on Defendant's representations and the reasonable expectation that Defendant would employ appropriate safeguards to protect sensitive data. Plaintiff provided Defendant with his Private Information, including but not limited to her name, full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification

number, financial account information, biometric identifiers, financial account information, and payment card information in connection with Defendant's services.

16. Defendant retained Plaintiff's Private Information through at least December 25, 2025 when the Data Breach occurred.

17. In or about June 5, 2026, Plaintiff received written notice from Defendant informing Plaintiff that Plaintiff's Private Information had been compromised in the Data Breach. Since that time, Plaintiff has spent significant time monitoring his accounts, reviewing financial statements, and taking precautionary measures to protect herself from identity theft. These efforts have caused a significant disruption to his daily life and represent a tangible loss of time and productivity. Plaintiff expects to continue undertaking these protective steps indefinitely due to the enduring risk of misuse of his information.

18. Plaintiff reasonably believed that Defendant would maintain the confidentiality and security of his Private Information and would not have entrusted it to Defendant had he known it would be inadequately protected. As a direct result of the Data Breach, Plaintiff has suffered harm, including emotional distress, anxiety, loss of time, and an ongoing and heightened risk of identity theft and fraud.

19. provides counseling, advocacy, outreach, and health services for members of the LGBTQ community in Orange County. In the course of its operations, Defendant collects, maintains, and stores highly sensitive personal and medical information from thousands of patients. Defendant is registered in the State of California and maintains its principal place of business at 1605 N SPURGEON STREET, SANTA ANA, CA 92701.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to California Code of Civil Procedure § 410.10. This matter qualifies as an unlimited civil and complex class action, as the aggregate amount in controversy for Plaintiff and the Class exceeds $25,000, exclusive of interest and costs.

21. This Court has jurisdiction over Defendant because it conducts substantial business within, and maintains its principal place of business in, Orange County, California.

22. Venue is proper in this Court pursuant to Business and Professions Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5, because Defendant maintains its principal place of business, and is headquartered, within this Court's jurisdiction and a substantial portion of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this County.

THE CONDUCT

23. Data breaches have become a widespread and persistent problem across the United States. Cybercriminals increasingly target organizations that store large volumes of personal data, seeking to profit by selling or otherwise exploiting the stolen information.

24. When an individual's personal information is compromised, that person faces significant and lasting risks—regardless of how sensitive the data may appear. The exposure of personally identifiable information ("PII") can result in identity theft, fraudulent financial activity, damaged credit, loss of access to medical care or insurance, and other serious personal and economic consequences.

25. According to the U.S. Department of Justice, Bureau of Justice Statistics, nearly one-third of identity theft victims whose personal data was used fraudulently reported spending a month or more resolving related problems, and in many cases, the process took more than a year to complete.[2]

26. The U.S. Government Accountability Office ("GAO") has similarly found that data thieves often retain stolen information for months—or even years—before using it, making it impossible for victims to know when or how their information will next be misused. The GAO also emphasized that while credit monitoring services may alert individuals to signs of fraud, such services do not prevent identity theft or misuse of personal information once it has been compromised.

27. When companies fail to implement and maintain industry-standard data security practices, cyberattacks can go undetected for extended periods of time. The longer an intrusion remains undiscovered, the greater the resulting harm to consumers, who lose valuable time and the

[2] According to the **U.S. Department of Justice, Bureau of Justice Statistics**, nearly one-third of identity theft victims whose personal information was fraudulently used reported spending a month or more attempting to resolve the resulting issues, and for many, the process of recovery extended beyond a year.

ability to mitigate the damage. In some cases, the effects of such breaches are permanent and irreparable.

28. Stolen PII has substantial economic value and is actively traded on black markets, including the dark web. Depending on the type and completeness of the information, a full identity profile can command hundreds or even thousands of dollars. The legitimate data brokerage industry, which profits from the aggregation and sale of personal information, has itself been estimated to exceed $250 billion in value—illustrating just how lucrative consumer data has become.

29. [Information containing medical or insurance details is particularly valuable because, unlike credit or debit card numbers that can be quickly replaced, health-related data is largely immutable. For this reason, entities that collect or store such information, including Defendant, are frequent targets of cybercriminals seeking long-term value in stolen datasets.

30. Independent research supports this heightened risk. A 2021 report by the data technology company Invisibly found that personal medical records are among the most valuable forms of data on the illicit market, noting that health care files often contain a comprehensive set of identifiers and background information. While a single Social Security number might sell for less than one dollar, a complete medical record can fetch an average of **$**250—underscoring the significant incentive for cybercriminals to target entities that manage such information.[3]

31. On the dark web, cybercriminals sell stolen personal information to identity thieves who use it to exploit victims—engaging in extortion, harassment, identity takeover, and fraudulent financial activity such as opening credit accounts or conducting unauthorized transactions in the victims' names.

32. Personally identifiable information ("PII") carries significant and measurable value—both to legitimate businesses that rely on it for commercial purposes and to criminals who traffic in stolen data. Increasingly, cybercriminals also target the personal information of minors, recognizing that children's data often remains unmonitored for years and can be exploited for fraudulent purposes without immediate detection.

[3] *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY (Jul. 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

33. Medical and health-related information is particularly prized by identity thieves. As a result, the healthcare and insurance sectors experience disproportionately high rates of data theft compared to other industries. According to the **HIPAA Journal**, healthcare data breaches have risen steadily over the past decade, with recent years setting record highs for the number of reported incidents.[4]

34. A study conducted by **Experian** found that the average cost of medical identity theft is approximately **$20,000** per victim, with many individuals forced to pay out-of-pocket expenses for fraudulent medical services to restore their benefits. These breaches not only devastate individuals and families but also impose far-reaching economic consequences.

35. Given the sensitivity of the information they hold, entities that maintain patient or consumer records must employ rigorous, industry-standard safeguards to prevent unauthorized access. The **Ponemon Institute**, a leading authority on data privacy, has repeatedly warned that organizations storing protected health information ("PHI") are among the top targets for cyberattacks. Defendant has long been on notice that such data carries exceptional risk and value, yet failed to implement the enhanced security measures necessary to protect it.

36. A January 2023 report by the Ponemon Institute, conducted in partnership with Censinet, found that more than half of healthcare organizations surveyed had experienced at least one ransomware attack in the previous two years. The study further reported that ransomware incidents disrupted patient care in a majority of cases and resulted in complications to medical procedures for approximately **45 percent** of respondents. These findings reflect a growing trend of cyberattacks that jeopardize both the privacy of patient data and the safety of individuals receiving medical treatment.[5]

37. Victims of the Data Breach now face an ongoing and indefinite threat of harm. Once Private Information is exposed, it can be compiled, aggregated, and resold indefinitely, allowing criminals to build detailed profiles that may be used for identity theft, fraud, blackmail, harassment,

---

[4] HIPAA Journal, *Healthcare Data Breach Statistics* (updated 2024), available at https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[5] *See* Ponemon Institute, ***The Impact of Ransomware on Patient Safety and Care: 2023 Update*** *(Jan. 2023), available at* https://www.censinet.com/blog/new-ponemon-report-shows-ransomware-continues-to-impact-patient-safety-per-survey-of-hospital-it-security-leaders/.

phishing scams, and other malicious activity. The psychological toll of living with the knowledge that one's most personal information is permanently compromised is itself a substantial and continuing injury.

38. Data breaches of this nature often expose particularly sensitive information, including the medical histories, health conditions, psychological evaluations, and even the home or school locations of affected children. The **Federal Bureau of Investigation (FBI)** has warned that the widespread collection and potential compromise of student data poses significant privacy and safety risks. According to the FBI, the misuse of such information could enable social engineering, bullying, stalking, or identity theft directed at minors. Beyond these immediate threats, children whose information is exposed may spend their lives knowing that deeply personal details about them could resurface at any time.

39. Given the escalating risks and frequency of cyberattacks, it is essential that entities like Defendant proactively monitor their systems for intrusions, regularly update and patch their software, and implement robust security protocols—including strong encryption, intrusion detection, and network segmentation—to safeguard against further breaches and mitigate ongoing threats.

40. Defendant provides counseling, advocacy, outreach, and health services for members of the LGBTQ community in Orange County and, as part of its operations, collects and processes the personal and medical information of thousands of patients across the state.

41. Defendant routinely receives and stores extensive personally identifiable information ("PII") from consumers, including, among other things, full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information in connection with its rendering of services.

42. The Federal Trade Commission ("FTC") has repeatedly emphasized the importance of implementing and maintaining reasonable data security practices for all businesses that collect

or store personal information. According to the FTC, data protection should be an integral part of every organization's operations and decision-making processes.

43. In its 2016 publication *Protecting Personal Information: A Guide for Business*, the FTC outlined specific cybersecurity principles and best practices for safeguarding consumer data. The guidance advises that businesses should: (a) secure the personal information they collect and store; (b) properly dispose of data that is no longer needed; (c) encrypt sensitive information both in transit and at rest; (d) identify and address network vulnerabilities; and (e) implement policies and procedures to promptly correct any security weaknesses.[6]

44. The FTC also recommends that companies: (a) minimize the retention of private information to what is strictly necessary; (b) restrict access to sensitive data to authorized personnel only; (c) require the use of strong, complex passwords and authentication mechanisms; (d) utilize industry-tested and regularly updated security technologies; (e) monitor systems for suspicious or unauthorized activity; and (f) ensure that third-party vendors and service providers maintain comparable levels of security.

45. The FTC has brought numerous enforcement actions against companies that failed to protect customer information, treating the failure to adopt and maintain reasonable data security measures as an unfair practice in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

46. Plaintiff and Class Members entrusted their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant—and any third parties acting on its behalf—would fulfill their obligations to maintain the confidentiality of that information and protect it from unauthorized access, disclosure, or misuse.

47. Defendant knew or should have known that unprotected or exposed PII and PHI in the possession of companies like itself is highly valuable and frequently targeted by cybercriminals seeking to unlawfully profit from unauthorized access and misuse of such data. When

[6] U.S. Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business-0

compromised, this information—often deeply personal and sensitive—can have devastating consequences for affected individuals.

48. As a business entrusted with sensitive personal information, Defendant knew or should have known the critical importance of protecting the Private Information provided by Plaintiff and Class Members, as well as the foreseeable harm that would result if its data security systems were compromised. This includes the substantial financial and personal costs that victims incur following a data breach. Despite this knowledge, Defendant failed to implement adequate cybersecurity measures to prevent the Data Breach.

49. As a condition of providing counseling, advocacy, outreach, and health services, Defendant requires individuals to provide highly sensitive Private Information, including full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information.

50. By requesting, collecting, utilizing, and deriving benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to protect that information and knew or should have known that it was responsible for maintaining its security and preventing unauthorized access, disclosure, or misuse.

51. Plaintiff and Class Members took reasonable measures to preserve the confidentiality of their information and relied on Defendant to do the same—specifically, to maintain adequate data security, to use their Private Information solely for legitimate business purposes, and to prevent any unauthorized access, exposure, or disclosure.

52. Defendant failed to meet the data protection standards established under federal law and guidance from the Federal Trade Commission ("FTC") and other regulatory authorities.

53. Defendant was at all times fully aware of its duty to safeguard Plaintiff's and Class Members' Private Information, given its role as a trusted medical providers responsible for handling sensitive patient PII and PHI data. Defendant also knew, or should have known, that failing to

adequately protect this information would expose affected individuals to serious and foreseeable harm.

54. Defendant failed to adopt even the most basic and cost-effective cybersecurity safeguards that could have significantly strengthened its data protection posture. Indeed, Defendant allowed nefarious actors to breach its systems for an ongoing period of eight months. Such basic measures include, but are not limited to: (a) properly encrypting personally identifiable information (PII); (b) training employees on data security best practices and the handling of sensitive information; and (c) ensuring that software systems and network devices were correctly configured and regularly updated to prevent unauthorized access.

55. Despite the widespread availability of information and guidance on cybersecurity threats and the well-established best practices for mitigating them, Defendant failed to take appropriate action. These best practices were readily known—or should have been known—to Defendant, which had ample opportunity and resources to implement them. Defendant's disregard for recognized industry and regulatory standards directly resulted in the Data Breach and the unlawful exposure of Private Information.

56. As a direct and foreseeable consequence of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered, will continue to suffer, and remain at heightened risk of suffering the following harms:

a. The compromise, exposure, theft, and/or unauthorized use of their Private Information;

b. Out-of-pocket expenses incurred to prevent, detect, and recover from identity theft or fraud, as well as to remediate the effects of the breach;

c. Lost opportunity costs and lost wages resulting from time spent addressing and mitigating both the immediate and long-term consequences of the Data Breach, including researching methods to protect against, detect, and recover from identity theft and fraud;

d. The embarrassment, humiliation, and emotional distress associated with the public exposure of deeply personal and sensitive medical and cosmetic information.

e. The ongoing risk that their Private Information, which remains in Defendant's possession, may be further accessed, misused, or disclosed as long as Defendant fails to implement adequate data protection measures; and

f. The continued expenditure of time, money, and effort required to monitor accounts, guard against future misuse, and repair the damage caused by the Data Breach.

57. Beyond seeking redress for the economic harm suffered, Plaintiff and Class Members have a compelling and ongoing interest in ensuring that their Private Information is properly safeguarded, remains secure, and is not subjected to any further unauthorized access, misuse, or disclosure.

58. It is well established that prompt notification following a data breach is essential to minimizing harm. The sooner financial institutions, credit card issuers, wireless carriers, or other service providers are alerted to potential fraud, the faster they can act to limit damage. Early notice not only reduces the scope of harm but can also lessen victims' liability and increase the likelihood that law enforcement will identify and apprehend the perpetrators.

59. Timely disclosure also enables affected individuals to take immediate protective measures—such as monitoring financial statements, changing passwords, freezing credit reports, and reporting suspicious activity. When consumers are not promptly informed of a breach, they lose the critical opportunity to safeguard themselves and prevent further misuse of their information.

60. Despite the exposure of their Private Information, Plaintiff and Class Members were not timely notified of the Data Breach, depriving them of the ability to promptly mitigate the potential harm caused by Defendant's security failure. As a result of Defendant's delay in detecting and disclosing the breach, Plaintiff and Class Members face an increased and prolonged risk of identity theft, fraud, and other misuse of their personal data.

61. Plaintiff brings this class action pursuant to California Code of Civil Procedure § 382 on behalf of all California residents whose Private Information was maintained, stored, or otherwise possessed by Defendant and was compromised, accessed, or disclosed in connection with the Data Breach.

62. Excluded from the Class are Defendant, its officers, directors, and employees, as well as their immediate families, legal representatives, heirs, successors, assigns, any entity in which Defendant has a controlling interest, and any judge assigned to this case and their immediate family members. Plaintiff reserves the right to amend or refine the Class definition as necessary.

63. The Class is so numerous that joinder of all members is impracticable, with potentially thousands of affected individuals whose identities can be determined from Defendant's records.

64. Common questions of law and fact predominate over individual issues, including whether Defendant failed to implement reasonable data security measures, whether such failure resulted in the unauthorized access and disclosure of Private Information, whether Defendant acted negligently or unlawfully in collecting, maintaining, or securing that information, whether Defendant delayed in providing notice of the Data Breach, and whether Plaintiff and Class Members are entitled to damages, equitable relief, or other remedies under California law, including the Unfair Competition Law (Bus. & Prof. Code § 17200 et seq.), the Customer Records Act (Civ. Code § 1798.80 et seq.), and the Consumer Privacy Act (Civ. Code § 1798.100 et seq.).

65. Plaintiff's claims are typical of those of the Class, as each suffered similar harm from Defendant's conduct.

66. Plaintiff will fairly and adequately represent the interests of the Class and is represented by experienced Class Counsel with a history of successfully litigating complex class actions.

67. A class action is the superior method for adjudicating this dispute because individual suits would be inefficient, burdensome, and risk inconsistent outcomes, whereas class treatment promotes judicial economy and ensures uniform resolution of all claims.

/ / /

FIRST CAUSE OF ACTION

Negligence

(Alleged by PLAINTIFF and the CLASS against DEFENDANT)

68. Plaintiff realleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

69. Defendant's negligent acts and omissions created a foreseeable and unreasonable risk of harm to Plaintiff and Class Members. Defendant's negligence included, but was not limited to, its failure to take reasonable steps and utilize available safeguards that would have prevented the Data Breach. Defendant further acted negligently by disregarding well-established industry standards, federal regulations, and the data security best practices promulgated by the Federal Trade Commission ("FTC"), including those under Section 5 of the FTC Act (15 U.S.C. § 45), which require the implementation of reasonable security measures to protect consumers' personal information.

70. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in collecting, storing, and securing their Private Information to prevent it from being compromised, misused, or disclosed to unauthorized parties. This duty included the obligation to design, implement, and regularly test security systems sufficient to protect the Private Information in its possession, to train personnel on proper data security protocols, and to establish procedures to detect and prevent unauthorized access or disclosure.

71. Plaintiff and Class Members were required to provide Defendant with their Private Information as a condition of receiving property management and related administrative services. In doing so, they reasonably entrusted Defendant with their information under the expectation that it would be adequately safeguarded. Defendant, by contrast, had both the means and the duty to protect against the foreseeable harms resulting from a data breach, while Plaintiff and Class Members had no control over Defendant's data security practices or systems. Defendant knew or should have known of the sensitivity of the information it held and the significant harm that would result from its exposure.

72. Plaintiff and Class Members were the foreseeable victims of Defendant's negligent and deficient data security practices. Defendant knew or should have known of the risks inherent in maintaining large repositories of highly valuable personal information, of the increasing prevalence of cyberattacks, and of the need to employ robust data protection systems. Nevertheless, Defendant failed to adopt adequate training, monitoring, and technological safeguards to protect the Private Information in its possession.

73. Through its acts and omissions, Defendant breached its duty of care by failing to employ reasonable and appropriate data security measures; failing to comply with applicable laws, regulations, and industry standards; and failing to timely detect, contain, and disclose the Data Breach. The resulting exposure of Plaintiff's and Class Members' Private Information is precisely the type of harm privacy and consumer protection laws are intended to prevent, and Plaintiff and Class Members are the individuals those laws were designed to protect.

74. Defendant's failure to adhere to Section 5 of the FTC Act—which prohibits unfair practices in commerce, including failing to implement reasonable data security measures—constitutes negligence per se. The FTC has made clear through numerous publications, enforcement actions, and consent decrees that businesses must take reasonable steps to protect consumer information from unauthorized access. Defendant's disregard for these established standards, despite its possession of highly sensitive data and awareness of the foreseeable risks, was unreasonable and unlawful.

75. But for Defendant's wrongful acts and omissions, Plaintiff's and Class Members' Private Information would not have been compromised. There exists a direct and proximate causal link between Defendant's failure to maintain reasonable security controls and the injuries sustained by Plaintiff and Class Members as a result of the Data Breach.

76. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and continue to suffer damages, including but not limited to: the time and effort spent mitigating the effects of the breach; expenses associated with credit monitoring and account protection; anxiety, emotional distress, and loss of privacy; and, in some cases, identity theft and related financial losses. Plaintiff and Class Members also face the continuing risk that

their Private Information—still retained by Defendant—may be subject to further unauthorized access or misuse unless and until Defendant implements adequate security measures.

SECOND CAUSE OF ACTION

Negligence Per Se

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

77. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

78. 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 companies such as EP for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

79. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

80. Defendant's violation of Section 5 of the FTC Act in failing to adhere to industry standards regarding data security constitutes negligence *per se*. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

81. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

82. Defendant also has a duty under the California Constitution which contains a Right to Privacy clause, Article 1, Section 1, which states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending . . . privacy."[7]

83. Defendant's failure to implement reasonable measures to secure consumers' PII violates the California Constitution and the FTC Act, and thus constitutes negligence per se.

[7] Calif. Const. Art. 1, § 1.

84. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Breach of Implied Contract

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

86. Defendant provides counseling, advocacy, outreach, and health services to members of the LGBTQ community. In the course of providing these services, Defendant collected and maintained the Private Information of Plaintiff and Class Members, including full name, date of birth, Social Security number, diagnosis information, prescription information, medical history and treatment information, medical record number, health insurance information, driver's license number, government identification number, state identification number, passport number, taxpayer identification number, financial account information, biometric identifiers, financial account information, and payment card information, and other personally identifiable and protected health data.

87. In connection with this relationship, Plaintiff and Class Members entered into implied contracts with Defendant. By providing their Private Information as part of Defendant's medical services, Plaintiff and Class Members reasonably expected, and Defendant implicitly agreed, to safeguard that information and to use it solely for legitimate business purposes.

88. Under these implied contracts, Defendant agreed to: (1) implement and maintain reasonable administrative, technical, and physical safeguards to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; (2) comply with applicable federal and state laws and regulations governing data protection; and (3) adhere to industry standards and best practices concerning information security.

89. The protection of Private Information was a material term of these implied contracts. Plaintiff and Class Members would not have provided their Private Information to Defendant—or

allowed Defendant to retain and use it—had they known that Defendant would fail to maintain adequate safeguards to protect it from unauthorized access, disclosure, or misuse.

90. Plaintiff and Class Members fully performed their obligations under the implied contracts by providing accurate and necessary Private Information to Defendant in reliance on Defendant's duty to protect that information and maintain its confidentiality.

91. Defendant breached its obligations under the implied contracts with Plaintiff and Class Members by failing to implement and maintain reasonable data security measures to protect their Private Information from unauthorized access, use, and disclosure. Defendant's failure to employ adequate safeguards, despite its knowledge of the foreseeable risks of a data breach, constitutes a material breach of its contractual obligations.

92. The damages suffered by Plaintiff and Class Members were the direct and proximate result of Defendant's breach of these implied agreements.

93. As a result of Defendant's breach, Plaintiff and Class Members have suffered, and will continue to suffer, harm, including but not limited to: (i) the actual and threatened misuse of their Private Information, including identity theft and fraud; (ii) a substantially increased and ongoing risk of identity theft, necessitating time and money spent on credit monitoring, account protection, and other preventive measures; (iii) the unauthorized disclosure and loss of confidentiality of their Private Information; (iv) the deprivation of the value inherent in their Private Information, which carries recognized commercial and market value; (v) the loss of the benefit of their bargain, as they provided their Private Information in reliance on Defendant's promise to safeguard it; and (vi) time and financial losses associated with mitigating and addressing the effects of the Data Breach, including efforts to prevent further misuse of their data.

FOURTH CAUSE OF ACTION

Beach of Fiduciary Duty

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

95. A relationship of trust and confidence existed between Plaintiff and Class Members, on the one hand, and Defendant, on the other. Plaintiff and Class Members entrusted Defendant with their Private Information, relying on Defendant to exercise the highest degree of care, integrity, and loyalty in safeguarding that information from unauthorized access, disclosure, or misuse. Defendant knowingly accepted that trust and assumed a fiduciary duty to protect and preserve the confidentiality and security of the data in its possession.

96. Defendant breached its fiduciary duties by failing to act with the utmost good faith, fairness, and honesty, and by failing to exercise the level of care and loyalty required of a party entrusted with sensitive personal information. Defendant's conduct—including its failure to implement reasonable data security measures, failure to properly monitor and maintain its systems, and failure to timely notify affected individuals of the Data Breach—constitutes a breach of its fiduciary obligations.

97. Defendant's breach of fiduciary duty was a direct and proximate cause of the injuries sustained by Plaintiff and Class Members. But for Defendant's wrongful acts and omissions, Plaintiff's and Class Members' Private Information would not have been compromised, and the resulting damages would not have occurred.

98. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members have suffered and continue to suffer harm, including economic loss, loss of privacy, emotional distress, and an increased risk of identity theft. Plaintiff and Class Members seek actual, consequential, and nominal damages, as well as injunctive and equitable relief to prevent further unauthorized access, misuse, or disclosure of their Private Information.

FIFTH CAUSE OF ACTION

Breach of Confidence

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

100. At all relevant times, Defendant was fully aware of the confidential and sensitive nature of the Private Information entrusted to it by Plaintiff and Class Members. Defendant's

relationship with Plaintiff and Class Members was governed by the express and implied understanding that their Private Information would be collected, stored, and maintained in strict confidence, and would not be disclosed or made accessible to unauthorized third parties.

101. Plaintiff and Class Members provided their Private Information to Defendant with the explicit and implicit understanding that Defendant would safeguard it using reasonable, industry-standard security measures and would take all appropriate precautions to prevent unauthorized access, use, or disclosure. Defendant voluntarily received this Private Information in confidence and understood that maintaining its confidentiality was a condition of its relationship with Plaintiff and Class Members.

102. However, as a direct result of Defendant's failure to maintain adequate data security measures, the Data Breach occurred, causing Plaintiff's and Class Members' Private Information to be accessed, misappropriated, and disclosed to unauthorized third parties—beyond the scope of the confidence reposed in Defendant and without their consent. But for Defendant's failure to maintain the confidentiality of this information, the Private Information of Plaintiff and Class Members would not have been compromised, viewed, or used by unauthorized individuals.

103. The injuries and harm sustained by Plaintiff and Class Members were the reasonably foreseeable result of Defendant's failure to exercise due care in securing the Private Information in its possession. Defendant knew or should have known that its data collection, storage, transmission, and security practices were inadequate to protect against the type of cyber intrusion that occurred.

104. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class Members have suffered and will continue to suffer injuries, including but not limited to: (i) exposure to an increased risk of identity theft and fraud; (ii) loss of control over the use and dissemination of their Private Information; (iii) the compromise, publication, and theft of their confidential data; (iv) out-of-pocket expenses related to the prevention, detection, and remediation of identity theft and fraud; (v) ongoing risk that their Private Information, which remains in Defendant's possession, may be subject to further unauthorized access or misuse; and (vi) future financial and temporal costs associated with protecting, monitoring, and repairing the continued effects of the Data Breach for years to come.

105. As a direct and proximate result of Defendant's unauthorized disclosure and mishandling of their Private Information, Plaintiff and Class Members have suffered—and will continue to suffer—additional forms of injury, including emotional distress, anxiety, loss of privacy, and diminished value of their personal data.

SIXTH CAUSE OF ACTION

Invasion of Privacy

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

106. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

107. Plaintiff and Class Members had a reasonable and legally protected expectation of privacy in their Private Information, which Defendant was obligated to maintain in strict confidence and protect from unauthorized access, disclosure, or misuse. Defendant owed a duty to safeguard the privacy and security of this information and to prevent its unauthorized release to third parties.

108. Defendant breached this duty by failing to employ adequate data protection measures and by allowing the Private Information of Plaintiff and Class Members to be accessed and obtained by unknown and unauthorized third parties. Through its failure to secure the Private Information in its custody—despite the foreseeable risk of cyber intrusion—Defendant unlawfully invaded the privacy of Plaintiff and Class Members by: (i) intruding upon their private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to implement reasonable safeguards to prevent unauthorized disclosure; and (iii) enabling the release and dissemination of their Private Information without consent.

109. Defendant knew, or acted in reckless disregard of the fact, that its inadequate data security practices would expose the Private Information of Plaintiff and Class Members to unauthorized access, and that such conduct would be considered highly offensive and objectionable to a reasonable person. Defendant further knew, or should have known, that entities handling sensitive personal and financial data—such as that collected and stored by Defendant—are prime targets for cyberattacks, and that its failure to employ reasonable, industry-standard safeguards rendered it especially vulnerable to such breaches.

110. As a direct and proximate result of Defendant's wrongful conduct and the resulting unauthorized disclosure of their Private Information, Plaintiff's and Class Members' reasonable expectations of privacy were violated, causing them harm including emotional distress, anxiety, loss of privacy, and an ongoing risk of identity theft.

111. Plaintiff seeks injunctive and equitable relief on behalf of the Class to require Defendant to implement adequate security practices and to prevent further unauthorized disclosures, as well as restitution and any other relief available at law or in equity. Unless enjoined and restrained by this Court, Defendant's unlawful conduct will continue to cause irreparable injury to Plaintiff and Class Members, for which monetary damages alone are inadequate.

SEVENTH CAUSE OF ACTION

Unjust Enrichment

(Alleged by PLAINTIFF and the CALIFORNIA CLASS against DEFENDANTS)

112. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein. This cause of action is pleaded in the alternative to Plaintiff's contract-based claims.

113. Plaintiff and Class Members conferred a monetary and tangible benefit upon Defendant by providing and entrusting Defendant with their **valuable Private Information.** Upon information and belief, Defendant funds its operational and data security programs, in whole or in part, from the payments and fees collected through its counseling, advocacy, outreach, and health services. Plaintiff and Class Members—whose information was collected and stored as part of Defendant's business operations—were the intended beneficiaries of Defendant's obligation to maintain reasonable and adequate data security protections. Accordingly, a portion of the monies paid to Defendant, directly or indirectly, was intended to fund such security measures.

114. In exchange for these payments and the provision of their Private Information, Plaintiff and Class Members were entitled to the implementation of reasonable safeguards to ensure the protection and confidentiality of that data. Defendant, however, failed to provide such protections, thereby depriving Plaintiff and Class Members of the benefit of their bargain and retaining the benefit conferred upon it under inequitable and unjust circumstances.

115. Defendant accepted and retained the benefits derived from Plaintiff and Class Members while simultaneously failing to secure their Private Information and concealing its inadequate data protection practices. Defendant's retention and use of this benefit, while exposing the information to unauthorized access and misuse, was unjust and inequitable.

116. Because Defendant failed to safeguard Plaintiff's and Class Members' Private Information, it did not provide full or fair value in exchange for the benefits it received. Moreover, Defendant's acquisition and continued possession of that data was inequitable, as it failed to disclose its deficient security systems and the foreseeable risk of a data breach.

117. Plaintiff and Class Members lack an adequate remedy at law because monetary damages alone cannot rectify the continuing harm caused by Defendant's failure to adequately protect their Private Information. Under principles of equity and good conscience, Defendant should not be permitted to retain either the benefits conferred upon it or the improperly secured data of Plaintiff and Class Members.

118. Defendant should be compelled to disgorge, into a common fund or constructive trust for the benefit of Plaintiff and the Class, all monies or benefits it unjustly retained, and to implement adequate data security measures to protect the Private Information that remains in its possession.

EIGHTH CAUSE OF ACTION

Violation of the California Unfair Competition Law

(Cal. Bus. & Prof Code § 17200, *et seq.*)

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

119. Plaintiff realleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

120. Defendant violated California Business and Professions Code § 17200, et seq. (the "Unfair Competition Law" or "UCL") by engaging in unlawful and unfair business acts and practices that constitute "unfair competition" within the meaning of the statute.

121. Defendant's unlawful and unfair conduct includes, but is not limited to: (a) implementing inadequate and substandard data security practices and procedures as described

herein; (b) soliciting and collecting Plaintiff's and Class Members' Private Information despite knowing its systems lacked adequate safeguards; and (c) maintaining and storing such information in an unsecure electronic environment in violation of California Civil Code § 1798.81.5, which requires businesses to implement reasonable security measures to protect personal information.

122. Additionally, Defendant engaged in unlawful business acts and practices by failing to timely and accurately disclose the Data Breach, as required by California Civil Code § 1798.82.

123. As a direct and proximate result of Defendant's unlawful and unfair practices, Plaintiff and Class Members suffered injury in fact and lost money or property, including but not limited to: (i) the loss of their legally protected interest in the confidentiality and privacy of their Private Information; (ii) the deprivation of the benefit of their bargain; and (iii) other financial and non-economic damages described herein.

124. Defendant knew or should have known that its computer systems and data protection practices were insufficient to safeguard Plaintiff's and Class Members' Private Information, and that a data breach was a foreseeable and highly probable consequence of such deficiencies. Defendant's conduct was negligent, willful, reckless, and undertaken with conscious disregard for the rights and privacy of Plaintiff and Class Members.

125. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, et seq., including restitution of money or property acquired through Defendant's unlawful and unfair business practices, restitutionary disgorgement of all ill-gotten gains, declaratory and injunctive relief to prevent the continuation of such practices, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and such other equitable relief as the Court deems just and proper.

NINTH CAUSE OF ACTION

Violation of the California Customer Records Act ("CCRA")

(Cal. Civ. Code §§ 1798.80, et seq.)

(Alleged by PLAINTIFF and the CLASS against DEFENDANTS)

126. Plaintiff realleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

127. California Civil Code § 1798.82 (the California Customer Records Act, or CCRA) requires any person or business that conducts business in California and owns or licenses computerized data that includes personal information to disclose any breach of the security of that system to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Such disclosure must be made "in the most expedient time possible and without unreasonable delay."

128. Under Cal. Civ. Code § 1798.82(b), any person or business maintaining computerized data that includes personal information owned by another must immediately notify the owner or licensee following discovery of a security breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

129. The CCRA further mandates that any required breach notification must be written in plain language and include, at minimum: (a) the name and contact information of the reporting business; (b) a list of the types of personal information reasonably believed to have been compromised; (c) the date, estimated date, or date range of the breach; (d) whether notification was delayed due to a law enforcement investigation; (e) a general description of the incident; and (f) contact information for the major credit reporting agencies if Social Security numbers or driver's license numbers were involved.

130. The Data Breach described herein constituted a "breach of the security system" under Cal. Civ. Code § 1798.82. Defendant unreasonably delayed notifying Plaintiff and Class Members that their Private Information had been compromised, despite knowing or having reason to know of the breach. Defendant failed to disclose the breach "in the most expedient time possible and without unreasonable delay," as required by law, thereby depriving Plaintiff and Class Members of the opportunity to take timely protective measures such as credit monitoring, fraud alerts, or credit freezes.

131. Upon information and belief, no law enforcement agency instructed Defendant that prompt disclosure would impede a criminal investigation. Defendant's delay was therefore unjustified and motivated, at least in part, by its own business interests and desire to avoid reputational and financial harm.

132. As a direct and proximate result of Defendant's violations of Cal. Civ. Code § 1798.82, Plaintiff and Class Members were denied timely notice of the Data Breach, suffered unnecessary and preventable harm, and incurred additional damages distinct from those caused by the breach itself—including increased exposure to identity theft and the loss of opportunity to mitigate further harm.

133. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including compensatory damages, statutory damages where applicable, injunctive and equitable relief, and any other relief the Court deems just and proper.

TENTH CAUSE OF ACTION

Violations of the California Consumer Privacy Act

(Cal. Civ. Code §§ 1798.150, *et seq.)*

(Alleged by PLAINTIFF and the CLASS against all Defendants)

134. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

135. Defendant is a for-profit business operating for the financial benefit of its owners and qualifies as a "business" under Cal. Civ. Code § 1798.140(d)(1) because it (a) has annual gross revenues exceeding $25 million, (b) collects, receives, or otherwise processes the personal information of more than 100,000 California residents, and/or (c) derives substantial revenue from the use or disclosure of consumers' personal information. Defendant collects and maintains consumers' personally identifiable information ("PII") as defined by Cal. Civ. Code § 1798.140.

136. Defendant violated Cal. Civ. Code § 1798.150 by failing to prevent the unauthorized access, exfiltration, theft, and disclosure of Plaintiff's and Class Members' nonencrypted PII. These failures resulted from Defendant's violations of its statutory duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it possessed.

137. Defendant owed a duty to Plaintiff and Class Members to employ reasonable data security measures to safeguard their PII. As alleged herein, Defendant breached that duty by failing to implement adequate technical, administrative, and physical safeguards. As a direct and

proximate result of Defendant's conduct, Plaintiff's and Class Members' PII—including names, addresses, and Social Security numbers—was exposed to unauthorized access and misuse.

138. Plaintiff and Class Members seek statutory penalties, damages, and injunctive and equitable relief requiring Defendant to implement and maintain reasonable security procedures and practices sufficient to protect employees' and consumers' PII from future compromise. Such relief is necessary and appropriate because Defendant continues to retain current and former employees' PII, including that of Plaintiff and Class Members, and has demonstrated a pattern of failing to adequately protect this sensitive information.

ELEVENTH CAUSE OF ACTION

Violations of California Confidentiality of Med. Information Act,

(Civil Code § 56, et seq.*.*)

(Alleged by PLAINTIFF and the CLASS against all Defendants)

139. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

140. California's Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56 et seq., requires any health care provider or contractor who creates, maintains, stores, or disposes of medical information to do so in a manner that preserves its confidentiality. Under § 56.101(a), "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

141. The CMIA further mandates that any electronic health record system or electronic medical record system "protect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

142. Defendant, as a business that collects, stores, and maintains residents' and employees' medical and health-related information in the course of providing management services, qualifies as a "provider of health care" and/or "contractor" within the meaning of the

California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §§ 56.05, 56.06, and 56.13.

143. As such, Defendant was obligated to safeguard and preserve the confidentiality of all medical and health-related information in its possession, and to refrain from disclosing or permitting unauthorized access to such information without the individual's authorization, in compliance with Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

144. Defendant further had a statutory duty to create, maintain, and store medical information securely, and to prevent its unauthorized disclosure, use, or access, as required by the CMIA and related regulations.

145. Under Cal. Civ. Code §§ 56.06 and 56.101(b)(1)(A), Defendant was required to protect and preserve the confidentiality of all electronic medical information of Plaintiff and the Class in its possession, and to implement appropriate administrative, technical, and physical safeguards to prevent its unauthorized release or disclosure. The CMIA further requires entities covered by the Act to take preventive actions to protect confidential medical records against unauthorized access or disclosure. Cal. Civ. Code § 56.36(b)(2)(E).

146. Pursuant to § 56.10(a) of the CMIA, a provider of health care or contractor "shall not disclose medical information regarding a patient … without first obtaining an authorization." Plaintiff and the Class are "patients" under § 56.05(k), as individuals whose medical information was collected and maintained by Defendant and pertains to their receipt of health-related services. The information compromised in the Data Breach constitutes "medical information" within the meaning of § 56.05(j).

147. Defendant violated § 56.36(b) by negligently maintaining, preserving, and storing the medical information of Plaintiff and the Class in a manner that failed to protect and preserve its confidentiality and integrity. Plaintiff and the Class did not authorize the disclosure of their medical information, and Defendant's inadequate data-security measures allowed unauthorized third parties to access, view, and exfiltrate their information.

148. The unauthorized actors who perpetrated the Data Breach obtained and viewed the medical information of Plaintiff and the Class, which is now available for potential misuse, sale, or other unlawful exploitation. Defendant's failure to implement reasonable administrative, technical, and physical safeguards—including timely intrusion detection, data-loss prevention, and authentication measures—constitutes a violation of the CMIA and directly enabled the unauthorized access and acquisition of protected health information.

149. As a direct and proximate result of Defendant's violations, Plaintiff's and Class members' medical information was released from its secure environment and disclosed to unauthorized third parties who accessed, viewed, and acquired it for improper purposes. Defendant's misuse and affirmative disclosure of medical information violated Cal. Civ. Code §§ 56.10, 56.11, 56.13, 56.26, and 56.101.

150. Accordingly, Plaintiff and the Class seek actual and statutory damages of $1,000 per person pursuant to Cal. Civ. Code § 56.36(b)(1), as well as injunctive and equitable relief, and recovery of reasonable attorneys' fees and costs under Cal. Civ. Code § 56.35 and Cal. Code Civ. Proc. § 1021.5.

/ / /

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment against Defendant as follows:

1. On behalf of the CALIFORNIA CLASS:
2. That the Court certify this case as a class action pursuant to California Code of Civil Procedure § 382, appoint Plaintiff as the representative of the Class, and designate her attorneys as Class Counsel;
3. That the Court grant injunctive and other equitable relief necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:
    a. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
    b. Requiring Defendant to safeguard, including through encryption, all personal and medical data collected or maintained in the course of its business in compliance with applicable federal, state, and industry standards;
    c. Requiring Defendant to delete, destroy, or permanently de-identify all Private Information belonging to Plaintiff and Class members, unless Defendant can demonstrate a lawful and necessary basis for its continued retention;
    d. Requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality, integrity, and availability of personal data;
    e. Prohibiting Defendant from maintaining Class members' Private Information on insecure or unencrypted systems or cloud environments;
    vi. Requiring Defendant to engage independent, third-party cybersecurity auditors and penetration testers to conduct periodic assessments of Defendant's systems, report findings, and oversee remediation of any identified vulnerabilities;
    f. Requiring Defendant to implement continuous network monitoring, automated intrusion detection, and system auditing to promptly identify and address potential breaches;
    g. Requiring Defendant to establish and maintain an information security training

program that includes at least annual cybersecurity training for all employees, with additional role-based training for those handling sensitive data;

h. Requiring Defendant to routinely test employees' understanding and compliance with data security policies and breach response procedures;

i. Requiring Defendant to develop and maintain an effective threat management and incident response plan capable of identifying, containing, and remediating cybersecurity incidents in real time;

j. Requiring Defendant to provide ongoing credit monitoring, identity theft protection, and fraud resolution services to all Class members; and

k. Requiring Defendant to issue timely and transparent notifications to affected individuals in the event of any future data breaches or unauthorized disclosures;

4. Awarding compensatory, statutory, and nominal damages to Plaintiff and the Class in an amount to be determined at trial;

5. Awarding equitable relief, including restitution and disgorgement of all revenues and profits unjustly retained as a result of Defendant's wrongful conduct;

6. Awarding reasonable attorneys' fees, costs, and litigation expenses as permitted by law;

7. Granting such other and further relief as the Court may deem just, equitable, and proper under the circumstances.

DATED: June 10, 2026

ZAKAY LAW GROUP, APLC

By: _____
Shani O. Zakay, Esq.
Attorney for PLAINTIFF

/ / /

DEMAND FOR A JURY TRIAL

PLAINTIFF demands a jury trial on issues triable to a jury.

DATED: June 10, 2026

ZAKAY LAW GROUP, APLC

By: _____
Shani O. Zakay, Esq.
Attorney for PLAINTIFF