Daniel S. Robinson (SBN 244245)
Wesley K Polischuk (SBN 254121)
Michael W. Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, CA 92660
(949) 720-1288; Fax (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com
molson@robinsonfirm.com

Attorneys for Plaintiff and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF LOS ANGELES

MARIA ORELLANA, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

PLANNED PARENTHOOD LOS ANGELES; and DOES 1 through 100, inclusive,

Defendants.

Case No. 21STCV44106

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff MARIA ORELLANA ("Plaintiff"), individually, and on behalf of the class defined below, brings this class action complaint against Planned Parenthood Los Angeles ("PPLA") and Does 1 through 100 ("Doe Defendants") (collectively, PPLA and Doe Defendants are referred to as "Defendants") and alleges as follows:

INTRODUCTION

1. On December 1, 2021, PPLA, one of the largest providers of comprehensive, reproductive health care services in Los Angeles County whose patients are especially concerned with the confidentiality of their sensitive medical treatment, announced a data breach whereby approximately 400,000 of its patients, including Plaintiff and putative Class members, had their personally identifiably information ("PII") and protected health information ("PHI") accessed by unauthorized parties due to Defendants' negligent data security (the "Data Breach"). Specifically, the PII and PHI accessed included Plaintiff's and Class members' names and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

2. In reports regarding the Data Breach, PPLA announced that unauthorized parties accessed its network between October 9 and October 17, 2021, installed malicious software, and exfiltrated files, which contained Plaintiff's and Class members' PII and PHI. During this time, the unauthorized parties utilized a specific type of malware called ransomware, which is a malicious computer code that hackers deploy to block an organization's access to its own computer network to extort a ransom.

3. Despite discovering the Data Breach on October 17, 2021 (more than one week after the unauthorized parties first accessed PPLA's systems), PPLA failed to determine that the stolen files included its patients' PII and PHI until November 4, 2021, and it did not provide notice to its patients until November 30, 2021 or December 1, 2021, more than one month after the Data Breach (Exhibit 1).

4. This is not the first time that a Planned Parenthood branch has been the subject of a data breach. In 2020, the Metropolitan Washington branch revealed that patient and donor information — including dates of birth, medical data and Social Security and financial information — was

breached.

5. While nearly 400,000 patients sought out and/or paid for comprehensive, reproductive health care services from PPLA, thieves were hard at work, stealing and using their hard-to-change Social Security numbers and highly sensitive PII/PHI without the victims' knowledge. PPLA's lax security practices that allowed this intrusion to occur have worsened Plaintiff's and other Class members' lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at an increased risk of fraudulent charges; (b) complicating diagnosis, prognosis, and treatment for their medical conditions by placing them at an increased risk of having inaccurate medical information in their files; and/or (c) increasing the risk of other potential personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

6. Prior to the Data Breach, PPLA acknowledged in the Privacy Policy that it is "committed to protecting the privacy of your identifiable health information" and that it would only use Plaintiff's and Class members' PII/PHI for certain limited purposes, such as providing patients with products, services, or information you request and for processing any transactions they have authorized. Although the Privacy Policy states it "does not apply to information [patients] may share with Planned Parenthood in connection with [the patients'] receipt of healthcare services online or via in-person visits at facilities operated by Planned Parenthood Affiliates. Such information is protected by state and federal law."[1]

7. PPLA not only led its patients to believe that it would protect their PII and PHI involved in the Data Breach, PPLA failed to live up to its own promises as well as its duties and obligations required by law and industry standards.

8. Contrary to its promises to help patients improve the quality of their lives, PPLA's conduct has instead been a direct cause of the ongoing harm to Plaintiffs and other Class members whose suffering has been magnified by the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future.

9. Specifically, Defendants failed to maintain reasonable and/or adequate security measures to protect Plaintiff's and other Class members' PII/PHI from unauthorized access and

[1] Planned Parenthood Privacy Policy, https://www.plannedparenthood.org/privacy-policy (last accessed on Dec. 2, 2021).

disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack even though Defendants knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from its network pertaining to approximately 400,000 PPLA patients.

10. Armed with PII/PHI, hackers can sell the PII/PHI to other thieves or misuse themselves to commit a variety of crimes that harm Plaintiff and Class members. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; give false information to police during an arrest; or engage in medical fraud that can result in financial harm or a harmful misdiagnosis to Plaintiff and Class members.

11. As a result of Defendants' willful failure to prevent the Data Breach, Plaintiff and Class members are more susceptible to identity theft, fraud, and other harm, and have experienced, will continue to experience, and face an increased risk of financial harms.

PARTIES

12. Plaintiff MARIA ORELLANA is a resident and citizen of Long Beach, California. Plaintiff was a patient of PPLA, having received services from, and being a patient of, PPLA in Los Angeles County, California. Upon information and belief, Plaintiff's PII/PHI was involved in the data breach, and as a result of Defendants' actions, Plaintiff has been injured, has suffered financial losses, and is subject to a substantial risk for further identity theft due to Defendants' Data Breach. Plaintiff believed, at the time of receiving services from PPLA, that it would maintain the privacy and security of her PII/PHI. Plaintiff further believes she paid a premium to PPLA for its data security. Plaintiff would not have used PPLA had she known that it would expose, or allow to be exposed, her PII/PHI, making it available to unauthorized parties.

13. Defendant PPLA is a California corporation with its principal place of business at 400 W. 30th Street, Los Angeles, California 90007.

14. The true names and/or capacities, whether individual, corporate, partnership, associate

or otherwise, of the Defendants herein designated as Does 1 to 100 are unknown to Plaintiff at this time who, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as Does is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiffs as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

15. Plaintiff is informed and believe and thereon alleges that at all times mentioned herein, Does were agents, servants, employees, partners, distributors or joint ventures of each other and that in doing the acts herein alleged, were acting within the course and scope of said agency, employment, partnership, or joint venture. Each and every Defendant aforesaid was acting as a principal and was negligent or grossly negligent in the selection, hiring and training of each and every other Defendant or ratified the conduct of every other Defendant as an agent, servant, employee or joint venture.

JURISDICTION AND VENUE

16. This Court has jurisdiction over the entire action by virtue of the fact that this is a civil action wherein the matter in controversy, exclusive of interest and costs, exceeds the jurisdictional minimum of the Court.

17. Venue is proper in this Court under Code of Civil Procedure section 395 because PPLA is headquartered and conducts substantial business within Los Angeles County. In addition, a substantial part of the conduct, omissions, and misrepresentations giving rise to the violations of law alleged herein occurred in Los Angeles County. The acts and omissions complained of in this action took place in the State of California.

FACTUAL ALLEGATIONS

A. The Data Breach

18. Beginning around October 9, 2021, unauthorized parties accessed the PPLA network that contained Plaintiff's and Class members' PII and PHI. Plaintiff and Class members are patients who paid and provided their PII and PHI to PPLA in exchange for comprehensive, reproductive health care services.

19. For more than a week, unauthorized parties maintained uninterrupted access to the PPLA system containing the PII and PHI of nearly 400,000 PPLA patients. Between October 9, 2021, and October 17, 2021, unauthorized parties viewed Plaintiff's and Class members' PII and PHI, and installed malicious software and exfiltrated files which contained Plaintiff's and Class members' PII and PHI. Specifically, the unauthorized parties utilized a specific type of malware called ransomware, which is a malicious computer code that hackers deploy to block an organization's access to its own computer network to extort a ransom.

20. Although PPLA knew that files had been stolen on or around October 17, 2021, PPLA did not learn until November 4, 2021, that the stolen files included its patients' PII and PHI, such as their name and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

21. As a result, unauthorized parties accessed, viewed, and acquired Plaintiff's and Class members' PII and PHI that Defendants released to them for nearly two months without Plaintiff's and Class members' knowledge or authorization.

22. PPLA has made numerous promises to Plaintiff and Class members that it will maintain the security and privacy of their personal information. For instance, in the Privacy Policy found on its website, PPLA promises its patients that it is "committed to protecting the privacy of your identifiable health information."[2]

23. In the Privacy Policy, PPLA further details that it will only use Plaintiff's and Class members' PII/PHI for certain limited purposes:

- providing [patients] with products, services, or information you request;
- processing any transactions [patients] have authorized;
- following up on services or information we provided to [patients];
- contacting you about fundraising campaigns or advocacy efforts;
- delivering advertisements targeted to [patients'] interests;
- conducting research;

[2] *See id*.

- promoting Planned Parenthood's services;
- processing an employment, internship, or volunteer application;
- providing [patients] with information about the Online Services or required notices;
- allowing us to improve the Online Services and the services we provide;
- generating and analyzing statistics about [patients'] use of the Online Services; and
- detecting, preventing, and responding to fraud, intellectual property infringement, violations of our Terms of Use, violations of law, or other misuse of the Online Services.

24. The Privacy Policy also provides that it will only disclose Plaintiff's and Class members' PII and PHI, to the following:

- to our affiliates;
- to service providers who work on our behalf;
- to other organizations that work with us for the provision of co-branded communications about Planned Parenthood and those organizations' products or services;
- to other organizations with whom Planned Parenthood participates in exchanges of supporter or donor information (e.g., donor list rental) and the service providers that facilitate such exchanges;
- as required by law;
- when required to protect our rights or [patients'] safety or the safety of others, or to detect, prevent, or respond to misuse of the Online Services; and
- to the extent reasonably necessary to proceed with the negotiation or completion of a merger, acquisition, or sale of all or a portion of our assets.

25. The Privacy Policy on the PPLA webpage does state that it "does not apply to information you may share with Planned Parenthood in connection with your receipt of healthcare services online or via in-person visits at facilities operated by Planned Parenthood Affiliates." In the Privacy Policy, PPLA also acknowledges that Plaintiff and Class members' PII and PHI "is protected

by state and federal law."

26. PPLA also has a HIPAA Privacy Policy that describes how health information about its patients may be used or disclosed. In that HIPAA Privacy Policy, PPLA provides the following pledge regarding its patients' health information:

> We understand that health information about you and your health care is personal. We are committed to protecting health information about you. We will create a record of the care and services you receive from us. We do so to provide you with quality care and to comply with any legal or regulatory requirements.[3]

27. The HIPAA Privacy Policy further acknowledges the following:

> Our pledge regarding your health information is backed-up by federal and state law. The privacy and security provisions of the federal Health Insurance Portability and Accountability Act ("HIPAA") require us to:
>
> - Make sure that health information that identifies you is kept private;
> - Make available this notice of our legal duties and privacy practices with respect to health information about you; and
> - Follow the terms of the notice that is currently in effect.

28. The HIPAA Privacy Policy also provides that PPLA will only use and disclose health information about its patients for certain limited purposes, such as for treatment, payment, health care operations, appointment reminders, and individuals involved in its patients' care or payment for the care.

29. The HIPAA Privacy Policy also explains the following additional protections that apply according to California law:

> In California, there are certain circumstances in which minors are given special protections from disclosure of their medical information. If you are a minor, you must provide us with written authorization to disclose information in certain circumstances. For example, we may not provide your medical information to your parents or guardians without your signed written authorization in most circumstances in which the care involves pregnancy, contraception, abortion, contagious or sexually

[3] [3] Planned Parenthood Los Angeles HIPAA Privacy Policy, https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa (last accessed on Dec. 2, 2021).

transmitted diseases, AIDS/HIV, mental health care, and drug and alcohol abuse treatment.

30. The HIPAA Privacy Policy also states that the following uses and disclosures of health information by PPLA will be made only with its patient's written permission:

- Uses and disclosures of protected health information for marketing purposes;
- Uses and disclosures that constitute the sale of your protected health information;
- Other uses and disclosures of health information not covered by this Notice or the laws that apply to us.

31. The HIPAA Privacy Policy also acknowledges that PPLA is "required by federal and state law to notify you following a breach with respect to your unsecured protected health information." Although PPLA provided Plaintiff and Class members with notice of the Data Breach, it failed to do so in a timely manner in violation of California law.

32. By failing to protect Plaintiff's and Class members' PII and PHI, and by allowing the Data Breach to occur, PPLA broke these privacy promises.

B. Personally Identifiable Information/Protected Health Information

33. PII/PHI is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

34. PII/PHI is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

35. PII/PHI does not include only data that can be used to directly identify or contact an individual (*e.g.*, name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number, payment card numbers).

36. PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security

number combined." The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."

37. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

38. Given the nature of the Data Breach, it is foreseeable that the compromised PII/PHI will be used to access Plaintiff's and the Class members' financial accounts, thereby providing access to additional PII/PHI or personal and sensitive information. Therefore, the compromised PII/PHI in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[4] For example, different PII/PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.

39. Further, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[5]

---

[4] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [as of June 24, 2017].

[5] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

40. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions.

41. The PII/PHI that Defendants exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in victims' names, obtaining protected health information, and/or committing medical fraud.

42. Unfortunately for Plaintiff and Class members, a person whose PII/PHI has been compromised may not fully experience the effects of the breach for years to come:

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

43. Accordingly, Plaintiff and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII/PHI is used without his or her permission to commit fraud or other crimes.[7]

44. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[8]

C. HIPAA Provides Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

45. As a healthcare provider, Defendants are subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part

[6] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <http://www.gao.gov/assets/270/262904.html.> [as of June 24, 2017].
[7] Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf> [as of June 24, 2017].
[8] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of June 24, 2017].

164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "Privacy and Security Rules").

46. The Privacy and Security Rules establish a national set of standards for the protection of "individually identifiable health information" that is held or transmitted by a health care provider, which HIPAA refers to as "protected health information."

47. Pursuant to HIPAA, Defendants must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

48. HIPAA imposes general security standards that Defendants must follow, including:

a. Ensuring the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);

b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);

c. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and

d. Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

49. From a technical standpoint, HIPAA requires Defendants to, among other things:

a. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, 45 C.F.R. § 164.312(a);

b. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and

c. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

50. The HIPAA Security Rule requires Defendants to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. 45 CFR 164.316(a). These policies and procedures must be maintained in written form. 45 CFR 164.316(b)(1)(i).

51. The HIPAA Security Rule requires covered entities to maintain a written record of any action, activity, or assessment required to be documented by the HIPAA Security Rule. 45 CFR 164.316(b)(1)(ii).

52. The HIPAA Security Rule requires covered entities to review documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. 45 CFR 164.316(b)(1)(iii).

53. Under the HIPAA Privacy Rule, Defendants may not use or disclose PHI or confidential medical information except as expressly permitted. 45 CFR 164.502(a).

D. The HITECH Act Provides Additional Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

54. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111–5), promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information.

55. The HITECH Act provides lucrative financial incentives, and the avoidance of penalties, to healthcare entities such as Defendants for demonstrating the meaningful use, interoperability, and security of electronic health information. Achieving meaningful use requires compliance with objectives, measures and certification and standards criteria. The Electronic Health Records ("EHR") Incentive Program requires compliance with the objective to protect electronic health information. A Core Measure to determine compliance with the objective is conducting or reviewing a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) (the HIPAA Security Rule) and implementing security updates as necessary and correcting identified security deficiencies as part of its risk management process.

56. Upon information and belief, Defendants implanted a rushed and substandard EHR

infrastructure in order to, in part, obtain millions of dollars in lucrative financial incentives, as well as the avoidance of penalties, despite knowing they were ill-equipped and unprepared to safely store and meaningfully use electronic health records and electronic health information in a secure manner consistent with regulations and industry standards.

E. Defendants are Subject To Other Federal and State Laws and Regulations That Provide Guidelines on the Practices It Should Have Implemented To Secure Patients' Protected Health Information

57. Section 5(a) of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prevents Defendants from using "unfair or deceptive acts or practices in or affecting commerce." The FTC has found that inadequate data privacy and cybersecurity practices can constitute unfair or deceptive practices that violate § 5.

58. The state of California generally prohibits healthcare providers from disclosing a patient's confidential medical information without prior authorization. The California Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code § 56.10(a)) states that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c)." *See also* Cal. Civ. Code §§ 1798.80, et seq.

59. In addition to their obligations under federal and state laws and regulations, Defendants owed a common law duty to Plaintiffs and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

60. Defendants further owed and breached its duty to Plaintiffs and the Class to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems (e.g. 45 CFR §§ 164.308(a), 164.306(d), 164.312, The Office for Civil Rights July 14, 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, etc.).

61. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII/PHI, and Defendants' failure to properly and timely notify Plaintiff and Class members, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

b. money and time lost as a result of fraudulent access to and use of their financial accounts;

c. loss of use of and access to their financial accounts and/or credit;

d. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of

fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the personal information in its possession.

62. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[9]

63. Further, criminals often trade stolen PII/PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII/PHI on the internet, thereby making such information publicly available.

CLASS ACTION ALLEGATIONS

64. Plaintiff brings this action on behalf of her minor child E.N., and on behalf of all persons similarly situated, pursuant to Code of Civil Procedure § 382. Plaintiff seeks to represent the following class ("Class"):

> All individuals who are California citizens whose PII and /or PHI was compromised as a result of the Data Breach.

65. Upon information and belief, the scope of this class definition, including its temporal scope, may be further refined after discovery of Defendants' and /or third-party records.

66. Excluded from the Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal

[9] True Identity Protection: Identity Theft Overview, ID Watchdog <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf> [as of Sept. 23, 2016].

representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

67. Plaintiff's claims are typical of the claims of the Class. Plaintiff is a member of a well-defined Class of similarly situated persons and the members of the Class were similarly affected by the conduct alleged of Defendants and incurred similar damage, as alleged in this complaint, as a result of the conduct of Defendants. Members of the Class are ascertainable from Plaintiff's description of the Class and /or Defendants' records and /or records of third parties accessible through discovery.

68. The representative Plaintiff will fairly and adequately represent the members of the Class and have no interests which are antagonistic to the claims of the Class. Plaintiff's interests in this action are antagonistic to the interests of Defendants, and Plaintiff will vigorously pursue the claims of the Class.

69. The representative Plaintiff has retained counsel who are competent and experienced in consumer, data breach, and invasion of privacy class action litigation, and have successfully represented plaintiffs in complex class actions. Plaintiff's counsel currently represent other plaintiffs in similar complex class action litigation involving wrongful disclosures and access of private information.

70. Common questions of law and fact impact the rights of each member of the Class and a common remedy by way of permissible damages and /or injunctive relief is sought for the Class.

71. There are substantial questions of law and fact common to all members of the Class which will predominate over any individual issues. These common questions of law and fact include, without limitation:

a. Whether Defendants disclosed the PII and PHI of Plaintiff and the Class, without authorization;

b. Whether such conduct constitutes a violation of California Civil Code section 56, *et seq.*;

c. Whether Defendants timely notified the patients whose information was wrongly disclosed;

d. Whether Defendants notice was deficient;

e. Whether Defendants' conduct was negligent;

f. Whether Defendants knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;

g. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII and PHI;

h. Whether Defendants violated California state consumer protection statutes; and

i. Whether Defendants were unjustly enriched by their conduct.

j. Whether Plaintiff and Class members are entitled to equitable relief including injunctive relief.

72. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiff and the Class are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

73. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because class members number in the tens of thousands and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed class members to prosecute their claims individually. Trial of Plaintiff and the Class members' claims are manageable. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

74. The persons in the Class are so numerous that the joinder of all such persons individually in this case is impracticable, and the disposition of their claims in this case and as part of a single class action lawsuit, rather than hundreds or thousands of individual lawsuits, will benefit the

parties and greatly reduce the aggregate judicial resources that would be spent if this matter were handled as hundreds or thousands of separate lawsuits.

75. Plaintiff knows of no difficulty that will be encountered in the management of this litigation, which would preclude its maintenance of a class action.

FIRST CAUSE OF ACTION

(Violations of California Confidentiality of Med. Information Act, Cal. Civ. Code § 56, *et seq.*)

76. Plaintiff and the Class re-alleges and incorporate by reference the allegations contained in the preceding paragraphs of this complaint, as though fully set forth herein.

77. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every 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." *Id*.

78. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

79. PPLA is a healthcare provider who is subject to the requirements and mandates of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.* ("CMIA").

80. Plaintiff and Class members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

81. The PHI of Plaintiff and Class members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

82. Defendants violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the PHI of Plaintiff and Class members, and failing to protect and preserve the integrity of the PHI of Plaintiff and Class members.

83. Plaintiff and Class members did not authorize Defendants' disclosure and release of their PHI that occurred in the Data Breach.

84. As a result of the Data Breach, the PHI of Plaintiff and Class members were compromised when it was acquired and accessed by unauthorized parties.

85. Defendants violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and Class members' PHI; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and Class members' PHI; (3) failing to use reasonable authentication procedures to track PHI in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff's and Class members' PHI was kept, all in violation of the CMIA.

86. Defendants' failure to implement adequate data security measures to protect the PHI of Plaintiff and Class members was a substantial factor in allowing unauthorized parties to access Defendants' computer systems and acquire the PHI of Plaintiff and Class members.

87. As a direct and proximate result of Defendants' violation of the CMIA, Defendants allowed the PHI of Plaintiff and Class members to (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and /or profit from their PHI, thereby breaching the confidentiality of their PHI. Plaintiff and Class members have accordingly sustained and will continue to sustain actual damages as set forth above.

88. Plaintiff, individually and on behalf of Class members, seeks actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

89. As a direct and proximate result of Defendants' violations of the CMIA, Plaintiff and Class members have been injured within the meaning of the CMIA and are entitled to damages of $1,000 each pursuant to Cal. Civ. Code § 56.36(b)(1).

90. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Civil Code § 56.35 and California Code of Civil Procedure § 1021.5.

SECOND CAUSE OF ACTION

(Negligence)

91. Plaintiff and the Class re-allege and incorporate by reference the allegations contained in the preceding paragraphs of this complaint, as though fully set forth herein.

92. Plaintiff and Class members were required to provide Defendants with their PII and PHI. Defendants collected and stored this information including their name and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

93. Defendants had a duty to Plaintiff and Class members to safeguard and protect their PII and PHI.

94. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII and PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

95. Defendants have full knowledge about the sensitivity of Plaintiff and Class members' PII and PHI, as well as the type of harm that would occur if such PII and PHI were wrongfully disclosed.

96. Defendants have a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII and PHI data.

97. Defendants breached their duty of care by failing to secure and safeguard the PII and PHI of Plaintiff and Class members. Defendants negligently stored and /or maintained its data security systems, and published that information on the Internet.

98. Further, Defendants by and through their above negligent actions and /or inactions, breached their duties to Plaintiff and Class members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII and PHI within their possession, custody and control.

99. Defendants further breached their duty to Plaintiff and Class members by failing to comply with the California Confidentiality of Medical Information Act, Consumers Legal Remedies

Act, the Customer Record's Act, and other state laws designed to protect Plaintiff and Class members from the type of harm they here have suffered. Such a breach by Defendants constitutes negligence per se.

100. Plaintiff and the other Class members have suffered harm as a result of Defendants' negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

101. It was reasonably foreseeable – in that Defendants knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII and PHI, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

102. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Class members, their PII and PHI would not have been compromised.

103. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class members' PII and PHI, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

104. Plaintiff and Class members are entitled to injunctive relief as well as actual and punitive damages.

THIRD CAUSE OF ACTION

(Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, et seq.)

105. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

106. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, et seq. This cause of action does not seek monetary

damages at this time but is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendants with notice required by California Civil Code § 1782.

107. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

108. Plaintiff, Class members, and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

109. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendants was likely to deceive consumers.

110. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

111. Defendants violated this provision by representing that they took appropriate measures to protect Plaintiff's and the Class members' PII and PHI. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

112. As a result, Plaintiff and Class members were induced to enter into a relationship with Defendants and provide their PII and PHI.

113. As a result of engaging in such conduct, Defendants have violated Civil Code § 1770.

114. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

115. Plaintiff and Class members suffered injuries caused by Defendants' misrepresentations, because they provided their PII and PHI believing that Defendants would adequately protect this information.

116. Plaintiff and Class members may be irreparably harmed and /or denied an effective and complete remedy if such an order is not granted.

117. The unfair and deceptive acts and practices of Defendants, as described above, present

a serious threat to Plaintiff and members of the Class.

///

///

FOURTH CAUSE OF ACTION

(Violation of Unfair Competition Law, California Business and Professional Code Section 17200, et seq.)

118. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

119. Plaintiff brings this claim on behalf of herself and the Class.

120. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

121. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff and Class members' PII and PHI, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

122. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII and PHI of consumers has been compromised for all to see, use, or otherwise exploit.

123. Defendants' practices were unlawful and in violation of Civil Code § 1798 et seq. because Defendants failed to take reasonable measures to protect Plaintiff's and the Class members' PII and PHI.

124. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII and PHI they provide to Defendants will remain private and secure, when in fact it was not private and secure.

125. Plaintiff and the Class members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions including, inter alia, the unauthorized release and disclosure of their PII and

PHI.

126. Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class members' PII and PHI also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 et seq., in that Defendants' conduct was substantially injurious to Plaintiff and Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

127. But for Defendants' misrepresentations and omissions, Plaintiff and Class members would not have provided their PII and PHI to Defendants or would have insisted that their PII and PHI be more securely protected.

128. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class members' PII and PHI, they have been injured: (1) the loss of the opportunity to control how their PII and PHI is used; (2) the diminution in the value and /or use of their PII and PHI entrusted to Defendants; (3) the compromise, publication, and /or theft of their PII and PHI ; and (4) costs associated with monitoring their PII and PHI, amongst other things.

129. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII and PHI. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

FIFTH CAUSE OF ACTION

(Violation of California Customer Records Act, California Civil Code § 1798.80 et seq.)

130. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

131. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures

and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

132. Defendants own, maintain, and license personal information, within the meaning of section 1798.81.5, about Plaintiff and the Class.

133. Defendants violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiff and Class members' personal information.

134. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

135. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, Plaintiff and the Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

136. Plaintiff and the Class members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

SIXTH CAUSE OF ACTION

(Breach of Contract)

137. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

138. Plaintiff and Class members entered into a contract with Defendants for the provision of title insurance or other closing services.

139. The terms of Defendants' privacy policy are part of the contract.

140. Plaintiff and Class members performed substantially all that was required of them under their contract with Defendants, or they were excused from doing so.

141. Defendants failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class member's information and documents.

142. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received title insurance or other

closing services that were less valuable than described in their contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

143. Also, as a result of Defendants' breach of contract, Plaintiff and Class members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

144. Accordingly, Plaintiff and Class members have been injured by Defendants' breach of contract and are entitled to damages and /or restitution in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION

(Unjust Enrichment)

145. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

146. Defendants received a benefit from Plaintiff and the Class in the form of payments for title insurance or other closing services.

147. The benefits received by Defendants were at Plaintiff's and the Class's expense.

148. The circumstances here are such that it would be unjust for Defendants to retain the portion of Plaintiff's and the Class's payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class members' personal information and documents.

149. Plaintiff and the Class seek disgorgement of Defendants' ill-gotten gains.

EIGHTH CAUSE OF ACTION

(Invasion of Privacy)

150. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

151. Plaintiff brings this claim on behalf of herself and the Class.

152. Plaintiff and Class members have a legally protected privacy interest in their PII and PHI that Defendants required them to provide and allow them to store.

153. Plaintiff and Class members reasonably expected that their PII and PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

154. Defendants unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII and PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII and PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII and PHI to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

155. In failing to adequately secure Plaintiff's and Class members' PII and PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

156. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under state law, including the California Constitution, Article I, Section I. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII and PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment as follows:

1. For an Order certifying the proposed Class pursuant to California Civil Code Section 382, requiring notice thereto to be paid by Defendants and appointing Plaintiff and her counsel to represent the Class;
2. For appropriate injunctive relief and/or declaratory relief, including, but not limited to, an order requiring Defendants to immediately secure and fully encrypt all confidential information, to store any computer passwords in a location separate from the computers, to cease negligently storing, hand ling, and securing its patients' confidential information, to notify patients whose medical information is wrongly disclosed in an expedient and timely manner and to provide identity theft monitoring for an additional five years;

3. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

4. For compensatory and general damages according to proof on certain causes of action;

5. For damages on certain causes of action, including $1,000 per Class Member pursuant to Cal. Civ. Code §§ 56.35 and 56.36(b) and all other available statutory damages;

6. For reimbursement, restitution and disgorgement on certain causes of action;

7. For both pre and post-judgment interest at the maximum allowable rate on any amounts awarded;

8. For costs of the proceedings herein;

9. For reasonable attorneys' fees as allowed by statute; and

10. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Dated: December 3, 2021

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson
Daniel S. Robinson
Wesley K Polischuk
Michael W. Olson

Attorneys for Plaintiff and the Proposed Class

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: December 3, 2021

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson
Daniel S. Robinson
Wesley K Polischuk
Michael W. Olson

Attorneys for Plaintiff and the Proposed Class

EXHIBIT 1

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

Planned Parenthood®
Care. No matter what.
Planned Parenthood Los Angeles

November 30, 2021

H1202-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample:

At Planned Parenthood Los Angeles ("PPLA"), we take our commitment to privacy very seriously, and we work hard to protect our patients' information. We are writing to inform you of an incident involving some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened
On October 17, 2021, we identified suspicious activity on our computer network. We immediately took our systems offline, notified law enforcement, and a third-party cybersecurity firm was engaged to assist in our investigation. The investigation determined that an unauthorized person gained access to our network between October 9, 2021 and October 17, 2021, and exfiltrated some files from our systems during that time.

What Information Was Involved
As soon as we determined what files were involved, we began a review to determine what they contained. On November 4, 2021, we identified files that contained your name and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

What You Can Do
At this time, we have no evidence that any information involved in this incident has been used for fraudulent purposes. However, in an abundance of caution, we wanted to notify you of this incident and assure you that we take this very seriously. It is always a good idea to review statements you receive from your health insurer and health care providers. If you see charges for services you did not receive, please call the insurer or provider immediately.

What We Are Doing
We have and will continue to take steps to enhance our existing security measures and to help protect the information in our care, including increasing our network monitoring, engaging an external cybersecurity firm, and hiring additional cybersecurity resources and talent to our team.

For More Information
We deeply regret that this incident occurred and for any concern this may cause you. If you have questions about this incident, please call (866) 665-2966, Monday through Friday from 6 a.m. to 8 p.m. Pacific Time, and Saturday and Sunday from 8 a.m. to 5 p.m. Pacific Time. Callers should provide Engagement Number **B021848** to the operator.

Sincerely,

Kevin Oliver
Compliance Officer

0000001

H1202-L01

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

Planned Parenthood®
Care. No matter what.
Planned Parenthood Los Angeles

30 de noviembre de 2021

SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Estimado Sample:

En Planned Parenthood de Los Angeles ("PPLA"), tomamos muy en serio nuestro compromiso con la privacidad y trabajamos arduamente para proteger la información de nuestros pacientes. Hoy le escribimos para informarle de un incidente relacionado con parte de su información. Esta carta explica el incidente, las medidas que hemos tomado y algunos pasos que puede considerar tomar como respuesta.

Qué sucedió
El 17 de octubre de 2021, identificamos actividad sospechosa en nuestra red informática. Inmediatamente desconectamos nuestros sistemas, notificamos a la policía y contratamos a una empresa independiente de ciberseguridad para ayudar con nuestra investigación. La investigación determinó que una persona no autorizada obtuvo acceso a nuestra red entre el 9 de octubre de 2021 y el 17 de octubre de 2021, y exfiltró algunos archivos de nuestros sistemas durante ese tiempo.

Qué información estuvo involucrada
Tan pronto como determinamos qué archivos estaban involucrados, comenzamos una revisión para determinar qué contenían. El 4 de noviembre de 2021, identificamos archivos que contenían el nombre de usted y uno o más de los siguientes: dirección, información del seguro, fecha de nacimiento e información clínica, como diagnóstico, procedimiento o información de recetas de medicamentos.

Lo que usted puede hacer
En este momento, no tenemos ninguna evidencia de que la información involucrada en este incidente haya sido utilizada con fines fraudulentos. Sin embargo, como una medida extrema de precaución, quisimos notificarle de este incidente y asegurarle que lo estamos tomando muy en serio. Una buena idea es la de siempre revisar las declaraciones que recibe de su aseguradora de salud y de sus proveedores de atención médica. Si ve cargos por servicios que usted no recibió, llame inmediatamente a la aseguradora o al proveedor.

Lo que estamos haciendo
Estamos tomando los pasos necesarios para mejorar nuestras medidas de seguridad y para ayudar a proteger la información que se encuentra bajo nuestro cuidado, incluido el aumento de nuestro monitoreo de red, la participación de una empresa de ciberseguridad externa y la contratación de recursos y talento de ciberseguridad adicionales para nuestro equipo.

Para más información
Lamentamos profundamente que este incidente haya ocurrido y cualquier preocupación que esto pueda ocasionarle. Si tiene preguntas sobre este incidente, llame al (866) 665-2966, de lunes a viernes, entre las 6:00 a.m. y las 8:00 p.m. y de sabado a domingo entre las 8:00 a.m. y las 5:00 p.m., horario del Pacífico. Al llamar deberá proporcionar su número de participación **B021848** al operador.

Atentamente,

Kevin Oliver
Oficial de Cumplimiento