

1 Scott Edward Cole, Esq. (S.B. #160744)  
2 Laura Grace Van Note, Esq. (S.B. #310160)  
3 Elizabeth Ruth Klos, Esq. (S.B. #346781)

**COLE & VAN NOTE**

4 555 12<sup>th</sup> Street, Suite 1725  
5 Oakland, California 94607  
6 Telephone: (510) 891-9800  
7 Facsimile: (510) 891-7030  
8 Email: sec@colevannote.com  
9 Email: lvn@colevannote.com  
10 Email: erk@colevannote.com  
11 Web: www.colevannote.com

12 Timothy K. Talbot, Esq. (S.B. #173456)  
13 Joseph R. Lucia Esq. (S.B. #278318)  
14 **RAINS LUCIA STERN ST. PHALLE & SILVER, P.C.**

15 2300 Contra Costa Boulevard, Suite 500  
16 Pleasant Hill, California 94523  
17 Telephone: (925) 609-1699  
18 Facsimile: (925) 609-1690  
19 Email: TTalbot@RLSLawyers.com  
20 Email: JLucia@RLSLawyers.com  
21 Web: www.rlslawyers.com

22 Attorneys for Representative Plaintiff  
23 and the Plaintiff Class

24 **IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA**

25 **IN AND FOR THE COUNTY OF ALAMEDA**

26 HADA GONZALEZ individually, and on  
27 behalf of all others similarly situated,

28 Plaintiff,

vs.

CITY OF OAKLAND and DOES 1  
through 100, inclusive,

Defendants.

**Case No. 23CV031786**

**CLASS ACTION**

**COMPLAINT FOR DAMAGES,  
INJUNCTIVE AND EQUITABLE RELIEF  
FOR:**

1. **INFORMATION PRACTICES ACT OF 1977 (CIV. CODE, § 1798);**
2. **NEGLIGENCE;**
3. **BREACH OF IMPLIED CONTRACT**

**[JURY TRIAL DEMANDED]**

**ELECTRONICALLY FILED**

Superior Court of California,  
County of Alameda

**04/25/2023 at 09:30:44 AM**

By: Lynn Wiley,  
Deputy Clerk

Representative Plaintiff alleges as follows:

### INTRODUCTION

1. Representative Plaintiff Hada Gonzalez (“Gonzalez”) (“Representative Plaintiff”) brings this class action against Defendant City of Oakland and Does 1 through 100 (“Defendant” or “Oakland”) for its failure to properly secure and safeguard Representative Plaintiff’s and Class Members’ personally identifiable information stored within Defendant’s information network, including without limitation, full names, addresses, driver’s license numbers, medical information, city record information and Social Security numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as “protected health information” or “PHI”<sup>1</sup> and “personally identifiable information” or “PII”).<sup>2</sup>

2. With this action, Representative Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and the countless other similarly situated persons in the massive and preventable cyberattack that occurred on or about February 8, 2023, by which cybercriminals infiltrated Defendant’s inadequately protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected (the “Data Breach”).

3. Representative Plaintiff further seeks to hold Defendant responsible for not ensuring the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule (45 CFR, Parts 160 and

---

<sup>1</sup> Personal health information (“PHI”) is a category of information that refers to an individual’s medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

<sup>2</sup> Personally identifiable information (“PII”) generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver’s license numbers, financial account numbers, etc.).

1 164(A) and (E)), the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), California  
2 privacy laws (e.g., Pen. Code, § 832.7(a); Cal. Const. art. I § 1) and other relevant standards.

3 4. While Defendant claims to have known about the Data Breach as early as February  
4 8, 2023, it did not immediately report the security incident to Representative Plaintiff or Class  
5 Members. Despite the Data Breach's clear disruption to Defendant's services (wherein Defendant  
6 disconnected many city services, such as license issuing and phone services), Defendant did not  
7 immediately alert Representative Plaintiff or Class Members that their information was  
8 endangered by the breach.<sup>3</sup> Rather, Representative Plaintiff and Class Members were left in the  
9 dark about the Data Breach's effect on their information—or that the Data Breach impacted their  
10 information at all—until Representative Plaintiff received an email from Defendant informing  
11 Representative Plaintiff of it. Representative Plaintiff did not receive such notice until  
12 Representative Plaintiff received an email from Defendant dated March 4, 2023.

13 5. Defendant acquired, collected and stored Representative Plaintiff's and Class  
14 Members' PHI/PII in connection with its provision of city services and/or Representative  
15 Plaintiff's and Class Members' employment therewith. Therefore, at all relevant times, Defendant  
16 knew or should have known that it was storing Representative Plaintiff's and Class Members'  
17 PHI/PII as it requested or otherwise collected this information in the course of its operations.

18 6. HIPAA establishes national minimum standards for the protection of individuals'  
19 medical records and other personal health information. HIPAA generally applies to health plans,  
20 health care clearinghouses and those health care providers that conduct certain health care  
21 transactions electronically. HIPAA sets minimum standards for Defendant's maintenance of  
22 Representative Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires  
23 appropriate safeguards be maintained by healthcare providers such as Defendant to protect the  
24 privacy of personal health information and sets limits and conditions on the uses and disclosures  
25 that may be made of such information without patient authorization. HIPAA also establishes a  
26

27 <sup>3</sup> “*Ransomware Gangs Leaks Data Stolen from City of Oakland*,”  
28 <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-city-of-oakland/> (Last accessed April 16, 2023).

1 series of rights over Representative Plaintiff's and Class Members' PHI/PII, including rights to  
2 examine and obtain copies of their health records and to request corrections thereto.

3 7. Additionally, the HIPAA Security Rule establishes national standards to protect  
4 individuals' electronic personal health information that is created, received, used or maintained by  
5 a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and  
6 technical safeguards to ensure the confidentiality, integrity and security of electronic protected  
7 health information.

8 8. By obtaining, collecting, using and deriving a benefit from Representative  
9 Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those  
10 individuals. These duties arise from HIPAA and other state and federal statutes and regulations as  
11 well as common law principles. Representative Plaintiff does not bring claims in this action for  
12 direct violations of HIPAA, but charges Defendant with various legal violations merely predicated  
13 upon the duties set forth in HIPAA.

14 9. Defendant disregarded the rights of Representative Plaintiff and Class Members by  
15 intentionally, willfully, recklessly or negligently failing to take and implement adequate and  
16 reasonable measures to ensure that Representative Plaintiff's and Class Members' PHI/PII was  
17 safeguarded, failing to take available steps to prevent an unauthorized disclosure of data and failing  
18 to follow applicable, required and appropriate protocols, policies and procedures regarding the  
19 encryption of data, even for internal use. As a result, Representative Plaintiff's and Class  
20 Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third  
21 party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding  
22 Representative Plaintiff and Class Members in the future. What's worse, this third party has  
23 already begun spreading sensitive information obtained through the Data Breach on the “dark  
24 web,” an unindexed area of the internet where cybercriminals buy and sell private information.  
25 Representative Plaintiff and Class Members have a continuing interest in ensuring their  
26 information is and remains safe and are entitled to injunctive and other equitable relief.

**JURISDICTION AND VENUE**

10. This Court has jurisdiction over Representative Plaintiff's and Class Members' claims for damages and injunctive relief pursuant to, *inter alia*, Civ. Code, § 56, *et seq.*, § 1798, *et seq.*, among other California state statutes.

11. Venue as to Defendant is proper in this Judicial District pursuant to Civ. Proc. Code, § 395(a) and/or § 394(a). Defendant provided the aforementioned services within this County to numerous Class Members and transacts business, has agents and is otherwise within this Court's jurisdiction for purposes of service of process. The unlawful acts alleged herein have had a direct effect on Representative Plaintiff and those similarly situated within the State of California and within this County.

**PLAINTIFF**

12. Gonzalez is an adult individual and, at all relevant times herein, a resident of the State of California. Gonzalez is a victim of the Data Breach.

13. Prior to the Data Breach, Gonzalez provided information to Defendant in connection with Representative Plaintiff's receipt of city services or employment therefrom. As a result, Gonzalez's information was among the data accessed by an unauthorized third party in the Data Breach.

14. At all times herein relevant, Gonzalez is and was a member of the Class.

15. As required to receive services/employment from Defendant, Gonzalez provided Defendant with highly sensitive personal and financial information.

16. Gonzalez's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Gonzalez's PHI/PII. Representative Plaintiff's PHI/PII was within Defendant's possession and control at the time of the Data Breach.

17. Gonzalez received an email from Defendant explaining that Representative Plaintiff's PHI/PII was involved in the Data Breach (the "Notice"). The Notice explained that Defendant investigated a network intrusion and malware attack that resulted in an unauthorized person accessing or taking certain information from Defendant's network.

1           18.     Gonzalez submitted a claim for damages to Defendant via certified mail on March  
2           9, 2023 and substantially complied with all requirements for presenting a claim under Gov't Code,  
3           § 910. A true and correct copy of Gonzalez's claim is attached as **Exhibit 1**.

4           19.     As of filing, Gonzalez has not received any response from Defendant and  
5           Defendant's time to respond has elapsed.

6           20.     As a result of the data breach, Representative Plaintiff spent time dealing with the  
7           consequences of the Data Breach, which included and continues to include time spent verifying  
8           the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft  
9           insurance options, self-monitoring Representative Plaintiff's accounts and seeking legal counsel  
10          regarding Representative Plaintiff's options for remedying and/or mitigating the effects of the Data  
11          Breach. This time has been lost forever and cannot be recaptured.

12          21.     Representative Plaintiff suffered actual injury in the form of damages to and  
13          diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that  
14          Representative Plaintiff entrusted to Defendant for the purpose of obtaining city services and/or  
15          employment, which was compromised in and as a result of the Data Breach.

16          22.     Representative Plaintiff suffered lost time, annoyance, interference and  
17          inconvenience as a result of the Data Breach and has anxiety and increased concern for the loss of  
18          Representative Plaintiff's privacy, as well as anxiety over the impact of cybercriminals accessing  
19          and using Representative Plaintiff's PHI/PII. This anxiety is acute given that the third-party  
20          cybercriminals used the Data Breach to exfiltrate agency internal reports, citation records and other  
21          potentially embarrassing or inciteful information that has already been made available to the public  
22          via the dark web.

23          23.     Representative Plaintiff has suffered imminent and impending injury arising from  
24          the substantially increased risk of fraud, identity theft and misuse resulting from Representative  
25          Plaintiff's PHI/PII in combination with Representative Plaintiff's name being placed in the hands  
26          of unauthorized third parties/criminals.

**DEFENDANT**

25. Defendant is the largest city and the county seat of Alameda County, California, with its headquarters at 1 Frank H. Ogawa Plaza, Oakland, California 94612.

26. Respondent is a “local public entity” for purposes of Gov’t Code, § 905.

27. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

## CLASS ACTION ALLEGATIONS

28. Representative Plaintiff brings this action individually and on behalf of all persons similarly situated and proximately damaged by Defendant's conduct including but not necessarily limited to the following Plaintiff Class:

“All individuals within the State of California whose PHI/PII was stored by Defendant and was exposed to unauthorized third parties as a result of the data breach occurring on or around February 8, 2023.”

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

30. Representative Plaintiff reserves its right to request additional subclasses be added, as necessary, based on the types of PHI/PII that were compromised and/or the nature of certain Class Members' relationship(s) to the Defendant. At present, Class Members include, *inter alia*, Defendant's current and former California employees, vendors and clients.

31. Representative Plaintiff reserves the right to amend the above definition in subsequent pleadings and/or motions for class certification.

32. This action has been brought and may properly be maintained as a class action under Civ. Proc. Code, § 382 because there is a well-defined community of interest in the litigation and the Proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiff and Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

- 1) Whether Defendant engaged in the wrongful conduct alleged herein;
- 2) Whether Defendant had a legal duty to Representative Plaintiff and Class Members to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;
- 3) Whether Defendant knew or should have known of the susceptibility of Defendant's data security systems to a data breach;
- 4) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 5) Whether Defendant's failure to implement adequate data security measures, including the sharing of Representative Plaintiff's and Class Members' PHI/PII allowed the Data Breach to occur and/or worsened its effects;



- 6) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
  - 7) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;
  - 8) How and when Defendant actually learned of the Data Breach;
  - 9) Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay and whether this caused damages to Representative Plaintiff and Class Members;
  - 10) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of Representative Plaintiff's and Class Members' PHI/PII;
  - 11) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
  - 12) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach and/or damages flowing therefrom;
  - 13) Whether Defendant's actions alleged herein constitute gross negligence and whether the negligence/recklessness of any one or more individual(s) can be imputed to Defendant;
  - 14) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct and, if so, what is necessary to redress the imminent and currently ongoing harm faced by Representative Plaintiff, Class Members and the general public;
  - 15) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;
  - 16) Whether Defendant continues to breach duties to Representative Plaintiff and Class Members.
- c. Typicality: The Representative Plaintiff's claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and each Class Member had their sensitive PHI/PII

1 compromised in the same way by the same conduct of Defendant.  
2 Representative Plaintiff and all Class Members face the identical  
3 threats resulting from the breach of their PHI/PII without the  
protection of encryption and adequate monitoring of user behavior  
and activity necessary to identify those threats.

4 d. Adequacy of Representation: Representative Plaintiff is an adequate  
5 representative of the Plaintiff Class in that Representative Plaintiff  
6 has the same interest in the litigation of this case as the remaining  
7 Class Members, is committed to vigorous prosecution of this case  
8 and has retained competent counsel who are experienced in  
conducting litigation of this nature. Representative Plaintiff is not  
9 subject to any individual defenses unique from those conceivably  
applicable to other Class Members or the Class in its entirety.  
Representative Plaintiff anticipates no management difficulties in  
this litigation. Representative Plaintiff and Representative  
Plaintiff's counsel will fairly and adequately protect the interests of  
all Class Members.

10 e. Superiority of Class Action: The damages suffered by individual  
11 Class Members are significant but may be small relative to the  
12 enormous expense of individual litigation by each member. This  
13 makes or may make it impractical for members of the Plaintiff Class  
14 to seek redress individually for the wrongful conduct alleged herein.  
15 Even if Class Members could afford such individual litigation, the  
16 court system could not. Should separate actions be brought or be  
17 required to be brought, by each individual member of the Plaintiff  
18 Class, the resulting multiplicity of lawsuits would cause undue  
19 hardship and expense for the Court and the litigants. The  
20 prosecution of separate actions would also create a risk of  
inconsistent rulings which might be dispositive of the interests of  
other Class Members who are not parties to the adjudications and/or  
may substantially impede their ability to adequately protect their  
interests. Individualized litigation increases the delay and expense  
to all parties, and to the court system, presented by the complex legal  
and factual issues of the case. By contrast, the class action device  
presents far fewer management difficulties and provides benefits of  
single adjudication, economy of scale and comprehensive  
supervision by a single court.

21 33. This class action is also appropriate for certification because Defendant has acted  
22 or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's  
23 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members  
24 and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's  
25 policies and practices challenged herein apply to and affect Class Members uniformly and  
26 Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct  
27  
28

1 with respect to the Class in its entirety, not on facts or law applicable only to the Representative  
2 Plaintiff.

3 34. Unless a Class-wide injunction is issued, Defendant may continue in its failure to  
4 properly secure Class Members' PHI/PII, and Defendant may continue to act unlawfully as set  
5 forth in this Complaint.

### 7 COMMON FACTUAL ALLEGATIONS

#### 8 The Cyberattack

9 35. According to Defendant's Notice, Defendant's investigation into unusual activity  
10 on its network concluded that an unauthorized third party had access to data stored on Defendant's  
11 information systems which stored Class Members' PHI/PII.

12 36. In the course of the Data Breach, one or more unauthorized third parties accessed  
13 and/or took Class Members' sensitive data including but not limited to full names, addresses,  
14 driver's license numbers and Social Security numbers. Representative Plaintiff was among the  
15 individuals whose data was accessed in the Data Breach.

16 37. Representative Plaintiff was provided the information detailed above upon  
17 Representative Plaintiff's receipt of an email from Defendant sent March 9, 2023. Representative  
18 Plaintiff was not aware Representative Plaintiff's information had been accessed in the Data  
19 Breach until receiving that letter.

20 38. However, since receipt of the Notice, the third-party cybercriminals have made it  
21 clear that this is not all the information that was accessed. Though the Notice indicated that only  
22 Class Members' full names, addresses, driver's license numbers and Social Security numbers had  
23 been accessed, portions of the stolen data posted on the dark web show that other information was  
24 exfiltrated and viewed. This information includes internal reports made by city agencies (including  
25 peace officer reports), employee healthcare records and whistleblower's identities.<sup>4</sup> Despite there  
26

27 <sup>4</sup> "Oakland Ransomware Hackers Dumped Gigabytes of Sensitive City Files on the Web,"  
28 <https://oaklandside.org/2023/03/06/oakland-ransomware-hackers-leak-sensitive-city-files-data/>  
(last accessed April 16, 2023); "Oakland Confirms Massive Second Data Leak,"

1 being, to date, two public leaks of new information accessed in the Data Breach, Representative  
2 Plaintiff was not provided timely updated notices detailing the full breadth of the information  
3 exposed.<sup>5</sup>

4  
5 **Defendant's Failed Response to the Breach**

6 39. Not until over a month after it claims to have discovered the Data Breach did  
7 Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was  
8 potentially compromised as a result of the Data Breach. The Notice provided basic details of the  
9 Data Breach and Defendant's recommended next steps, such as reviewing account statements and  
10 credit reports for "any unauthorized activity over the next 12 to 24 months."

11 40. Upon information and belief, the unauthorized third-party cybercriminals gained  
12 access to Representative Plaintiff's and Class Members' PHI/PII with the intent of engaging in  
13 misuse, including marketing and selling Representative Plaintiff's and Class Members' PHI/PII  
14 and distributing it broadly across the dark web for destructive purposes.

15 41. Defendant had and continues to have obligations created by HIPAA, reasonable  
16 industry standards, common law, state statutory law and its own assurances and representations to  
17 keep Representative Plaintiff's and Class Members' PHI/PII confidential and to protect such  
18 PHI/PII from unauthorized access.

19 42. Representative Plaintiff and Class Members were required to provide their PHI/PII  
20 to Defendant with the reasonable expectation and mutual understanding that Defendant would  
21 comply with its obligations to keep such information confidential and secure from unauthorized  
22 access.

23 43. Despite this, Representative Plaintiff and the Class Members remain, even today,  
24 in the dark regarding what particular data was stolen, the particular malware used and what steps  
25 are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiff and Class

26  
27 

---

<https://therecord.media/oakland-confirms-massive-second-data-leak> (last accessed April 16,  
28 2023).

<sup>5</sup> *Id.*

Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

44. Representative Plaintiff's and Class Members' PHI/PII has already ended up for sale on the dark web. To effectuate the sale, the third-party cybercriminals who exfiltrated the information initially published a compressed version of the information on the dark web for public viewing.<sup>6</sup> This first leak comprised of select internal reports, including hundreds of records related to peace officers (which, in the current political climate, are deeply interesting and enticing for vast swaths of the public).<sup>7</sup> After receiving no response from the City, the third-party cybercriminals published a second, larger portion of the data, which included more extensive internal reports and city employee medical information.<sup>8</sup> Over 3,000 individuals have viewed these files containing Class Members' PHI/PII.<sup>9</sup> The third-party cybercriminals responsible for the leak may sell or leak more Class Member information. Defendant has taken little or no action to suppress or contain this information. As a result, unauthorized individuals can now easily access Representative Plaintiff's and Class Members' PHI/PII.

#### **Defendant Collected/Stored Class Members' PHI/PII**

45. Defendant acquired, collected and stored and assured reasonable security over Representative Plaintiff's and Class Members' PHI/PII.

<sup>6</sup> "Ransomware Gang Leaks Data Stolen from City of Oakland," <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-city-of-oakland/> (last accessed April 16, 2023).

<sup>7</sup> "Hackers Release Data of Thousands of City Workers—Including Senior Officials," <https://www.sfchronicle.com/eastbay/article/oakland-ransomware-attack-employees-17822693.php> (last accessed April 16, 2023).

<sup>8</sup> "Hackers Leaked a Second, Larger Set of Files on the Dark Web," <https://oaklandside.org/2023/04/05/ransomware-attack-hackers-oakland-second-data-leak-confidential-city-files/> (last accessed April 16, 2023).

<sup>9</sup> "Oakland Ransomware Attack: Leaked Data has More than 3.1k Views on the Dark Web," <https://abc7news.com/oakland-ransomware-attack-dark-web-play-randomware/12965273/> (last accessed April 16, 2023).

1           46. As a condition of its relationships with Representative Plaintiff and Class Members,  
2 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly  
3 sensitive and confidential PHI/PII.

4           47. By obtaining, collecting and storing Representative Plaintiff's and Class Members'  
5 PHI/PII, Defendant assumed legal and equitable duties over it and knew or should have known  
6 that it was thereafter responsible for protecting Representative Plaintiff's and Class Members'  
7 PHI/PII from unauthorized disclosure.

8           48. Representative Plaintiff and Class Members have taken reasonable steps to  
9 maintain their PHI/PII's confidentiality. Representative Plaintiff and Class Members relied on  
10 Defendant to keep their PHI/PII confidential and securely maintained, to use this information for  
11 business purposes only and to make only authorized disclosures of this information.

12           49. Defendant could have prevented the Data Breach by properly securing and  
13 encrypting and/or more securely encrypting its servers generally, as well as Representative  
14 Plaintiff's and Class Members' PHI/PII.

15           50. Defendant's negligence in safeguarding Representative Plaintiff's and Class  
16 Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and  
17 securing sensitive data, as evidenced by the trending data breach attacks in recent years.

18           51. Organizations and industries which store PHI/PII have experienced a large number  
19 of high-profile cyberattacks even in just the one-year period preceding this Complaint's filing.  
20 Generally, cyberattacks have become increasingly common.

21           52. Moreover, municipalities such as Defendant have become more prominent  
22 cyberattack targets in recent years.<sup>10</sup> In 2020, 44 percent of cyberattacks targeted municipalities.<sup>11</sup>  
23 Municipalities are especially enticing targets due to both the wealth of information stored on city  
24 systems and because of their relatively lax cybersecurity standards. As municipalities are often on

25  
26 <sup>10</sup> "Cyber Attacks on Municipalities are on the Rise—Sending Shockwaves Through  
27 Communities," [https://www.linkedin.com/pulse/cyber-attacks-municipalities-rise-sending-through-brett-gallant/?trk=pulse-article\\_more-articles\\_related-content-card/](https://www.linkedin.com/pulse/cyber-attacks-municipalities-rise-sending-through-brett-gallant/?trk=pulse-article_more-articles_related-content-card/) (last accessed April 16, 2023).

28 <sup>11</sup> "Are Municipal Cyber Attacks Threatening Citizens' Privacy?" <https://www.packetlabs.net/posts/municipal-cyber-attacks/> (last accessed April 16, 2023).

1 limited budgets, they often choose to forgo more robust cybersecurity protocols.<sup>12</sup> This makes  
2 municipalities an easy, lucrative mark for cybercriminals.

3 53. In 2021, Defendant received an audit report stating in pertinent part:

4 “We noted a weakness within the City’s information security program. Specifically,  
5 the City does not have updated policies and procedures along with continuous risk  
6 assessment and testing programs in place to actively mitigate threats to the City’s  
7 IT infrastructure for ransom ware attacks, cyber attacks, and other unauthorized  
8 data breaches. [...] As such, the City is exposed to threats from ransomware attacks,  
9 cyber attacks, and other threats.”<sup>13</sup>

10 54. Due to the high-profile nature of these breaches, and other breaches of their kind,  
11 as well as a direct warning from its Finance Department, Defendant was and/or certainly should  
12 have been on notice and aware of such attacks occurring and, therefore, should have assumed and  
13 adequately performed the duty of preparing for such an imminent attack.

14 55. Yet, despite the prevalence of public announcements of data breach and data  
15 security compromises, as well as specific reports about its own security practices, Defendant failed  
16 to take appropriate steps to protect Representative Plaintiff’s and Class Members’ PHI/PII from  
17 being compromised.

18 **Defendant Had an Obligation to Protect the Stolen Information**

19 56. Defendant’s failure to adequately secure Representative Plaintiff’s and Class  
20 Members’ sensitive data also breached duties it owed Representative Plaintiff and Class Members  
21 under statutory and common law. Under HIPAA, healthcare providers have an affirmative duty to  
22 keep patients’ Protected Health Information private. As a covered entity, Defendant has a statutory  
23 duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff’s and  
24 Class Members’ data. Moreover, Representative Plaintiff and Class Members surrendered their  
25 highly sensitive personal data to Defendant under the implied condition that Defendant would keep

26 <sup>12</sup> “Cyber Attacks on Municipalities are on the Rise—Sending Shockwaves Through  
27 Communities.”

28 <sup>13</sup> City of Oakland, California: Single Audit Report for the Year Ended June 30, 202, Finance  
Department, at 143 (December 2021), available at:  
<https://cao-94612.s3.amazonaws.com/documents/SAR-2021.pdf/> (last accessed April 16, 2023).

1 it private and secure. Accordingly, Defendant also had an implied duty to safeguard their data,  
2 independent of any statute.

3 57. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to  
4 comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E  
5 (“Standards for Privacy of Individually Identifiable Health Information”) and Security Rule  
6 (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R.  
7 Part 160 and Part 164, Subparts A and C.

8 58. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health  
9 Information establishes national standards for the protection of health information.

10 59. HIPAA’s Privacy Rule or Security Standards for the Protection of Electronic  
11 Protected Health Information establishes a national set of security standards for protecting health  
12 information that is kept or transferred in electronic form.

13 60. HIPAA requires Defendant to “comply with the applicable standards,  
14 implementation specifications, and requirements” of HIPAA “with respect to electronic protected  
15 health information.” 45 C.F.R. § 164.302.

16 61. “Electronic protected health information” is “individually identifiable health  
17 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45  
18 C.F.R. § 160.103.

19 62. HIPAA’s Security Rule requires Defendant to do the following:

- 20 a. Ensure the confidentiality, integrity and availability of all electronic protected  
21 health information the covered entity or business associate creates, receives,  
22 maintains or transmits;  
23 b. Protect against any reasonably anticipated threats or hazards to the security or  
24 integrity of such information;  
25 c. Protect against any reasonably anticipated uses or disclosures of such  
26 information that are not permitted; and  
27 d. Ensure compliance by its workforce.

28 63. HIPAA also requires Defendant to “review and modify the security measures  
implemented [...] as needed to continue provision of reasonable and appropriate protection of



1 | electronic protected health information” under 45 C.F.R. § 164.306(e), and to “[i]mplement  
2 | technical policies and procedures for electronic information systems that maintain electronic  
3 | protected health information to allow access only to those persons or software programs that have  
4 | been granted access rights.” 45 C.F.R. § 164.312(a)(1).

5 |         64.     Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414,  
6 | requires Defendant to provide notice of the Data Breach to each affected individual “without  
7 | unreasonable delay and in no case later than 60 days following discovery of the breach.”

8 |         65.     Defendant was also prohibited by the Federal Trade Commission Act (the “FTC  
9 | Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting  
10 | commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure  
11 | to maintain reasonable and appropriate data security for consumers’ sensitive personal information  
12 | is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,  
13 | 799 F.3d 236 (3d Cir. 2015).

14 |         66.     In addition to its obligations under federal and state laws, Defendant owed a duty  
15 | to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,  
16 | securing, safeguarding, deleting and protecting the PHI/PII in Defendant’s possession from being  
17 | compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty  
18 | to Representative Plaintiff and Class Members to provide reasonable security, including  
19 | consistency with industry standards and requirements and to ensure that its computer systems,  
20 | networks and protocols adequately protected Representative Plaintiff’s and Class Members’  
21 | PHI/PII.

22 |         67.     Defendant owed a duty to Representative Plaintiff and Class Members to design,  
23 | maintain and test its computer systems, servers and networks to ensure that the PHI/PII in its  
24 | possession was adequately secured and protected.

25 |         68.     Defendant owed a duty to Representative Plaintiff and Class Members to create and  
26 | implement reasonable data security practices and procedures to protect the PHI/PII in its  
27 | possession, including not sharing information with other entities who maintained sub-standard data  
28 | security systems.

69. Defendant owed a duty to Representative Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

70. Defendant owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

71. Defendant owed a duty to Representative Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to Defendant.

72. Defendant owed a duty of care to Representative Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

73. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

#### **Value of the Relevant Sensitive Information**

74. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, prescription information, treatment plans, etc.) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and is acutely affected by cyberattacks.

75. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,

1 and bank details have a price range of \$50 to \$200.<sup>14</sup> Experian reports that a stolen credit or debit  
2 card number can sell for \$5 to \$110 on the dark web.<sup>15</sup> Criminals can also purchase access to entire  
3 company data breaches from \$999 to \$4,995.<sup>16</sup>

4 76. Between 2005 and 2019, at least 249 million people were affected by health care  
5 data breaches.<sup>17</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed,  
6 stolen or unlawfully disclosed in 505 data breaches.<sup>18</sup>

7 77. These criminal activities have and will result in devastating financial and personal  
8 losses to Representative Plaintiff and Class Members.

9 78. The FTC defines identity theft as “a fraud committed or attempted using the  
10 identifying information of another person without authority.” The FTC describes “identifying  
11 information” as “any name or number that may be used, alone or in conjunction with any other  
12 information, to identify a specific person,” including, among other things, “[n]ame, Social Security  
13 number, date of birth, official State or government issued driver’s license or identification number,  
14 alien registration number, government passport number, employer or taxpayer identification  
15 number.”

16 79. Identity thieves can use PHI/PII, such as that of Representative Plaintiff and Class  
17 Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm  
18 victims. For instance, identity thieves may commit various types of government fraud such as  
19 immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with  
20  
21

22 <sup>14</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.  
23 16, 2019, *available at*: [https://www.digitaltrends.com/computing/personal-data-sold-on-the-](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)  
24 [dark-web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/) (last accessed July 28, 2021).

25 <sup>15</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.  
26 6, 2017, *available at*: [https://www.experian.com/blogs/ask-experian/heres-how-much-your-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)  
27 [personal-information-is-selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/) (last accessed November 5, 2021).

28 <sup>16</sup> *In the Dark*, VPNOOverview, 2019, *available at*:  
<https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 5,  
2021).

<sup>17</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last  
accessed November 4, 2021).

<sup>18</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
November 4, 2021).

1 another's picture, using the victim's information to obtain government benefits or filing a  
2 fraudulent tax return using the victim's information to obtain a fraudulent refund.

3 80. Stolen medical data is often processed and packaged with fragmentary data  
4 obtained unlawfully from other sources. In doing so, cybercriminals create full record sets on  
5 individuals ("fullz") which contain comprehensive information about a particular individual.<sup>19</sup>  
6 This enhances the value of the stolen information, since a single data element is not always wholly  
7 sufficient to impersonate someone on its own. Moreover, stolen medical information can also be  
8 used to blackmail patients.<sup>20</sup>

9 81. Stolen internal reports can be published on the dark web to be downloaded for free  
10 by members of the public. The public can, thereafter, publish the substance (or the entireties) of  
11 these reports on the "clear web," (the indexed version of the internet visible to the general public)  
12 publicly humiliating the report's subject. Such reports are deeply interesting to certain members  
13 of the public if the reports concern certain politically charged subjects (such as government  
14 officials or peace officers, as were disclosed here), and those responsible for placing the  
15 information on the "clear web" may reap substantial rewards. For instance, a leak of the TSA "No-  
16 Fly" list (a controversial list of individuals not permitted to fly on United States airlines) published  
17 on the "clear web" attracted viral attention and public debate in 2023.<sup>21</sup> The hacker responsible for  
18 the leak attracted instant online celebrity status and reaped substantial benefits in the form of online  
19 donations and followers.<sup>22</sup> Thus, those with access to the "dark web" leaks may be highly  
20 incentivized to leak information to the general public, where it may spread exponentially.

21 82. Internal reports concerning peace officers, such as those disclosed here, are of  
22 particular interest to the public. The public's animosity towards peace officers has increased  
23

24 <sup>19</sup> <https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims%20names/> (last accessed April 11, 2023).

25 <sup>20</sup> "Patient Data is Used for Blackmail," <https://communications.sectra.com/resources/1-patient-data-is-used-for-blackmail/> (last accessed April 11, 2023).

26 <sup>21</sup> "No Fly List Leaked onto Blog, but How and Why?" <http://fourteeneastmag.com/index.php/2023/02/17/no-fly-list-leaked-onto-blog-but-how-and-why/> (last accessed April 16, 2023).

27 <sup>22</sup> *Id.*

1 substantially since 2020, leading to intense public scrutiny and record numbers of peace officer  
2 resignations.<sup>23</sup> The public has become increasingly critical of “use of force” incidents, or incidents  
3 where peace officers make life-or-death decisions to defend themselves from criminal suspects by  
4 using physical force.<sup>24</sup> These incidents are documented in internal reports, such as those disclosed  
5 in the Data Breach. Public knowledge of these incidents leads to increased calls for both police  
6 culture reform and tracking of reform results, often with devastating results for the peace officers  
7 implicated.<sup>25</sup> Sites such as “prosecutekillercops.org” document every piece instance of alleged use  
8 of force incidents that their publishers can attain.<sup>26</sup> This has led to a precipitous decline in peace  
9 officer mental health, an increase in depression and high resignation levels.<sup>27</sup> Thus, the internal  
10 reports breached may be potentially devastating to the peace officers implicated in the reports.

11 83. In short, cybercriminal groups are not merely encrypting information networks and  
12 demanding ransoms (indeed, many groups have dispensed with encryption attacks altogether).  
13 Instead, these groups are often stealing data and processing it for sale to third parties or publishing  
14 the data intentionally to humiliate or threaten their targets. Like any other merchandise, sellers  
15 must know what they’re offering. As such, these groups are reviewing the information they obtain  
16 in order to market it to third parties. Because no ransom was paid here, Representative Plaintiff  
17 believes this is what happened to their PHI.

18 84. The ramifications of Defendant’s failure to keep Representative Plaintiff’s and  
19 Class Members’ PHI/PII secure are long lasting and severe. Once PHI/PII is stolen, particularly  
20 identification numbers, fraudulent use of that information and damage to victims may continue for  
21 years. Indeed, the PHI/PII of Representative Plaintiff and Class Members was taken by hackers to  
22

23 <sup>23</sup> “Cops Say Low Morale and Department Scrutiny are Driving Them Away from the Job,”  
24 <https://www.npr.org/2021/06/24/1009578809/cops-say-low-morale-and-department-scrutiny-are-driving-them-away-from-the-job/> (last accessed April 16, 2023).

25 <sup>24</sup> “Tyre Nichols Case Revives Calls for Change in Police Culture,”  
26 <https://apnews.com/article/law-enforcement-los-angeles-george-floyd-memphis-religion-21d9b66a447798e66e4f84a6b7bc3146/> (last accessed April 16, 2023).

27 <sup>25</sup> *Id.*

28 <sup>26</sup> “Prosecute Killer Cops,” <https://prosecutekillercops.org/> (Last accessed April 16, 2023).

<sup>27</sup> “Violence, Stress, Scrutiny Weigh on Police Mental Health,”  
<https://www.gpb.org/news/2021/06/14/violence-stress-scrutiny-weigh-on-police-mental-health/>  
(Last accessed April 15, 2023).

1 engage in identity theft and/or to sell it to other criminals who will purchase the PHI/PII for that  
2 purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

3 85. There may be a time lag between when harm occurs versus when it is discovered  
4 and between when PHI/PII is stolen and when it is used. According to the U.S. Government  
5 Accountability Office (“GAO”), which conducted a study regarding data breaches:

6 [L]aw enforcement officials told us that in some cases, stolen data may be held for  
7 up to a year or more before being used to commit identity theft. Further, once stolen  
8 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.<sup>28</sup>

9 86. The harm to Representative Plaintiff and Class Members is especially acute given  
10 the nature of the leaked data. Medical identity theft is one of the most common, most expensive  
11 and most difficult-to-prevent forms of identity theft.

12 87. “Medical identity theft is a growing and dangerous crime that leaves its victims  
13 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy  
14 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover  
15 erroneous information has been added to their personal medical files due to the thief’s activities.”<sup>29</sup>

16 88. If cybercriminals manage to access financial information, health insurance  
17 information and other personally sensitive data—as they did here—there is no limit to the amount  
18 of fraud to which Defendant may expose Representative Plaintiff and Class Members.

19 89. A study by Experian found that the average total cost of medical identity theft is  
20 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced  
21 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>30</sup> Almost  
22 half of medical identity theft victims lose their healthcare coverage as a result of the incident, while  
23  
24  
25

26 <sup>28</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:  
<http://www.gao.gov/new.items/d07737.pdf> (last accessed November 4, 2021).

27 <sup>29</sup> *Id.*

28 <sup>30</sup> See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3,  
2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last  
accessed November 4, 2021).

1 nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their  
2 identity theft at all.<sup>31</sup>

3 90. And data breaches are preventable.<sup>32</sup> As Lucy Thompson wrote in the DATA  
4 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could  
5 have been prevented by proper planning and the correct design and implementation of appropriate  
6 security solutions.”<sup>33</sup> She added that “[o]rganizations that collect, use, store, and share sensitive  
7 personal data must accept responsibility for protecting the information and ensuring that it is not  
8 compromised....”<sup>34</sup>

9 91. Most of the reported data breaches are a result of lax security and the failure to  
10 create or enforce appropriate security policies, rules and procedures. Appropriate information  
11 security controls, including encryption, must be implemented and enforced in a rigorous and  
12 disciplined manner so that a *data breach never occurs*.<sup>35</sup>

13 92. Here, Defendant knew or should have known of the importance of safeguarding  
14 PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiff’s and  
15 Class Members’ PHI/PII was stolen, including the significant costs that would be placed on  
16 Representative Plaintiff and Class Members as a result of a breach of this magnitude. As detailed  
17 above, Defendant is a large, sophisticated municipality with the resources to deploy robust  
18 cybersecurity protocols. It knew or should have known the development and use of such protocols  
19 were necessary to fulfill its statutory and common law duties to Representative Plaintiff and Class  
20 Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

21 93. Defendant disregarded the rights of Representative Plaintiff and Class Members by,  
22 *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and  
23 reasonable measures to ensure that its network servers were protected against unauthorized

24  
25 <sup>31</sup> *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last accessed November 4, 2021).

26 <sup>32</sup> Lucy L. Thompson, “*Despite the Alarming Trends, Data Breaches Are Preventable*,” in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

27 <sup>33</sup> *Id.* at 17.

28 <sup>34</sup> *Id.* at 28.

<sup>35</sup> *Id.*

1 intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and  
2 training practices in place to adequately safeguard Representative Plaintiff's and Class Members'  
3 PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach,  
4 (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time,  
5 and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice  
6 of the Data Breach.

7  
8 **FIRST CAUSE OF ACTION**  
9 **Information Practices Act of 1977**  
10 **(Civ. Code, § 1798, *et seq.*)**

11 94. Each and every allegation of the preceding paragraphs is incorporated in this claim  
12 with the same force and effect as though fully set forth herein.

13 95. Defendant was legally obligated to "establish appropriate and reasonable  
14 administrative, technical, and physical safeguards to ensure compliance with the [Information  
15 Practices Act of 1977], to ensure the security and confidentiality of records, and to protect against  
16 anticipated threats or hazards to its security or integrity which could result in any injury." Civ.  
Code, § 1798.21.

17 96. Defendant failed to establish appropriate and reasonable administrative, technical  
18 and physical safeguards to ensure compliance with the Information Practices Act of 1977 with  
19 regard to Representative Plaintiff's and Class Members' PHI/PII.

20 97. Defendant failed to ensure the security and confidentiality of records containing  
21 Representative Plaintiff's and Class Members' PHI/PII.

22 98. Defendant failed to protect against anticipated threats and hazards to the security  
23 and integrity of records containing Representative Plaintiff's and Class Members' PHI/PII.

24 99. As a result of these failures, Representative Plaintiff and Class Members have  
25 suffered and will continue to suffer economic damages and other injury and actual harm in the  
26 form of, *inter alia*, (i) an imminent, immediate and continuing increased risk of identity theft,  
27 identify fraud and medical fraud—risks justifying expenditures for protective and remedial  
28 services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the



1 confidentiality of their PHI/PII, (iv) deprivation of the value of their PHI/PII, for which there is a  
2 well-established national and international market, and/or (v) the financial and temporal cost of  
3 monitoring their credit, monitoring their financial accounts and mitigating their damages.

4 100. Representative Plaintiff and Class Members are also entitled to injunctive relief  
5 under Civil Code, § 1798.47.

6  
7 **SECOND CAUSE OF ACTION**  
8 **Negligence**

9 101. Each and every allegation of the preceding paragraphs is incorporated in this claim  
10 with the same force and effect as though fully set forth herein.

11 102. At all times herein relevant, Defendant owed Representative Plaintiff and Class  
12 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII  
13 and to use commercially reasonable methods to do so. Defendant took on this obligation upon  
14 accepting and storing Representative Plaintiff's and Class Members' PHI/PII in its computer  
15 systems and on its networks.

16 103. Among these duties, Defendant was expected:

- 17 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding  
18 deleting and protecting PHI/PII in its possession;
- 19 b. to protect Representative Plaintiff's and Class Members' PHI/PII using  
20 reasonable and adequate security procedures and systems that were/are  
21 compliant with industry-standard practices;
- 22 c. to implement processes to quickly detect the Data Breach and to timely act  
23 on warnings about data breaches; and
- 24 d. to promptly notify Representative Plaintiff and Class Members of any data  
25 breach, security incident or intrusion that affected or may have affected their  
26 PHI/PII.

25 104. Defendant knew that the PHI/PII was private and confidential and should be  
26 protected as private and confidential and, thus, Defendant owed a duty of care not to subject  
27 Representative Plaintiff and Class Members to an unreasonable risk of harm because they were  
28 foreseeable and probable victims of any inadequate security practices.

1           105. Defendant knew or should have known of the risks inherent in collecting and  
2 storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate  
3 security. Defendant knew about numerous, well-publicized data breaches.

4           106. Defendant knew or should have known that its data systems and networks did not  
5 adequately safeguard Representative Plaintiff's and Class Members' PHI/PII.

6           107. Only Defendant was in the position to ensure that its systems and protocols were  
7 sufficient to protect the PHI/PII that Representative Plaintiff and Class Members had entrusted to  
8 it.

9           108. Defendant breached its duties to Representative Plaintiff and Class Members by  
10 failing to provide fair, reasonable or adequate computer systems and data security practices to  
11 safeguard the PHI/PII of Representative Plaintiff and Class Members.

12           109. Because Defendant knew that a breach of its systems could damage thousands of  
13 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to  
14 adequately protect its data systems and the PHI/PII contained thereon.

15           110. Representative Plaintiff's and Class Members' willingness to entrust Defendant  
16 with their PHI/PII was predicated on the understanding that Defendant would take adequate  
17 security precautions. Moreover, only Defendant had the ability to protect its systems and the  
18 PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with  
19 Representative Plaintiff and Class Members.

20           111. Defendant also had independent duties under state and federal laws that required  
21 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and  
22 promptly notify them about the Data Breach. These "independent duties" are untethered to any  
23 contract between Defendant and Representative Plaintiff and/or the remaining Class Members.

24           112. Defendant breached its general duty of care to Representative Plaintiff and Class  
25 Members in but not limited to the following ways:

- 26                   a. by failing to provide fair, reasonable, or adequate computer systems and  
27 data security practices to safeguard the PHI/PII of Representative Plaintiff  
28 and Class Members;

- b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;
- d. by failing to provide adequate supervision and oversight of the PHI/PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII of Representative Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent;
- e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PHI/PII;
- g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and
- h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

113. Defendant's willful failure to abide by these duties was wrongful, reckless and grossly negligent in light of the foreseeable risks and known threats.

114. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

115. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

116. Defendant breached its duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting a month after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiff and Class Members

1 regarding the extent of the unauthorized access and continues to breach its disclosure obligations  
2 to Representative Plaintiff and Class Members.

3 117. Further, through its failure to provide timely and clear notification of the Data  
4 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative  
5 Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII.

6 118. There is a close causal connection between Defendant's failure to implement  
7 security measures to protect the PHI/PII of Representative Plaintiff and Class Members and the  
8 harm suffered, or risk of imminent harm suffered, by Representative Plaintiff and Class Members.  
9 Representative Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of  
10 Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting,  
11 implementing and maintaining appropriate security measures.

12 119. Defendant's wrongful actions, inactions and omissions constituted (and continue to  
13 constitute) common law negligence.

14 120. The damages Representative Plaintiff and Class Members have suffered (as alleged  
15 above) and will continue to suffer were and are the direct and proximate result of Defendant's  
16 grossly negligent conduct.

17 121. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair [...] practices  
18 in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or  
19 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII.  
20 The FTC publications and orders described above also form part of the basis of Defendant's duty  
21 in this regard.

22 122. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect  
23 PHI/PII and by not complying with applicable industry standards, as described in detail herein.  
24 Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it  
25 obtained and stored and the foreseeable consequences of the immense damages that would result  
26 to Representative Plaintiff and Class Members.

27 123. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se*.  
28

1           124. As a direct and proximate result of Defendant's negligence and negligence *per se*,  
2 Representative Plaintiff and Class Members have suffered and will continue to suffer injury,  
3 including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their  
4 PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket  
5 expenses associated with the prevention, detection and recovery from identity theft, tax fraud  
6 and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended  
7 and the loss of productivity addressing and attempting to mitigate the actual and future  
8 consequences of the Data Breach, including but not limited to efforts spent researching how to  
9 prevent, detect, contest and recover from embarrassment and identity theft, (vi) the continued risk  
10 to their PHI/PII, which may remain in Defendant's possession and is subject to further  
11 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate  
12 measures to protect Representative Plaintiff's and Class Members' PHI/PII in its continued  
13 possession, and (vii) future costs in terms of time, effort and money that will be expended to  
14 prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data  
15 Breach for the remainder of the lives of Representative Plaintiff and Class Members.

16           125. As a direct and proximate result of Defendant's negligence and negligence *per se*,  
17 Representative Plaintiff and Class Members have suffered and will continue to suffer other forms  
18 of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and  
19 other economic and non-economic losses.

20           126. Additionally, as a direct and proximate result of Defendant's negligence and  
21 negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to  
22 suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession  
23 and is subject to further unauthorized disclosures so long as Defendant fails to undertake  
24 appropriate and adequate measures to protect the PHI/PII in its continued possession.  
25  
26  
27  
28

**THIRD CAUSE OF ACTION**  
**Breach of Implied Contract**

127. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

128. Through their course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied-in-fact contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.

129. Defendant required Representative Plaintiff and Class Members to provide and entrust their PHI/PII in its ordinary course of business.

130. Defendant solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

131. As a condition of being Defendant's citizens and/or employees, Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

132. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendant in exchange for, amongst other things, the protection of their PHI/PII.

133. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

134. Defendant breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

135. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i) ongoing, imminent, and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and non-economic harm.

### **RELIEF SOUGHT**

**WHEREFORE**, Representative Plaintiff, on Representative Plaintiff's own behalf and on behalf each member of the proposed Class, respectfully requests the Court enter judgment in Representative Plaintiff's favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and/or any other appropriate subclasses under Civ. Proc. Code, § 382;

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

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

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

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

- c. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PHI/PII;
  - d. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;
  - e. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;
  - f. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's networks is compromised, hackers cannot gain access to other portions of Defendant's systems;
  - g. requiring Defendant to conduct regular database scanning and securing checks;
  - h. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;
  - i. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting PHI/PII;
  - j. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats and assess whether monitoring tools are properly configured, tested and updated;
  - k. requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.
5. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
  6. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;
  7. For all other Orders, findings and determinations sought in this Complaint.



COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12TH STREET, SUITE 1725  
OAKLAND, CA 94607  
TEL: (510) 891-9800

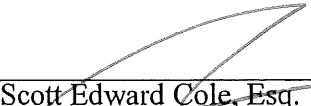
**JURY DEMAND**

Representative Plaintiff, individually, and on behalf of the Plaintiff Class, hereby demands  
a trial by jury for all issues triable by jury.

Dated: April 25, 2023

**COLE & VAN NOTE**

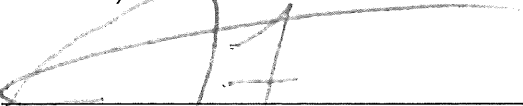
By:

  
\_\_\_\_\_  
Scott Edward Cole, Esq.  
Attorneys for Representative Plaintiff  
and the Plaintiff Class

Dated: April 25, 2023

**RAINS LUCIA STERN ST. PHALLE &  
SILVER, P.C.**

By:

  
\_\_\_\_\_  
Joseph Rockne/Lucia, Esq.  
Attorneys for Representative Plaintiff  
and the Plaintiff Class

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Oakland Settlement Resolves California Data Breach Lawsuit Over Cyberattack Discovered in February 2023](#)

---