

CLARKSON LAW FIRM, P.C.

Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avanness (SBN 343928)
tavaness@clarksonlawfirm.com
Valter Malkhasyan (SBN 348491)
vmalkhasyan@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (231) 788-4070

Electronically FILED by
Superior Court of California,
County of Los Angeles
5/18/2023 5:43 PM
David W. Slayton,
Executive Officer/Clerk of Court,
By D. Jackson Aubry, Deputy Clerk

Counsel for Plaintiff and the Proposed Class

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES**

MICHAEL AZAR, individually, and on
behalf of all others similarly situated,

Plaintiff,

vs.

HOUSING AUTHORITY OF THE CITY
OF LOS ANGELES, and DOES 1 through
20, inclusive,

Defendant.

Case No.: **23STCV11304**

**CLASS ACTION COMPLAINT FOR
DAMAGES:**

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE SECTION 17200, *et seq.*
2. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT (“CMIA”) CAL. CIV. CODE SECTION 56, *et seq.*
3. VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE SECTION 1798.80, *et seq.*
4. NEGLIGENCE
5. INVASION OF PRIVACY
6. BREACH OF CONFIDENCE
7. UNJUST ENRICHMENT
8. CONVERSION

DEMAND FOR JURY TRIAL

1 Plaintiff Michael Azar (“**Plaintiff**” or “**Mr. Azar**”), individually and on behalf of all others
 2 similarly situated, brings this class action complaint against Defendant Housing Authority of the
 3 City of Los Angeles (“**Defendant**” or “**HACLA**”). Plaintiff’s allegations are based upon personal
 4 knowledge as to himself and his own acts, and upon information and belief as to all other matters
 5 based on the investigation conducted by and through Plaintiff’s attorneys. Plaintiff believes that
 6 substantial additional evidentiary support will exist for the allegations set forth herein, after a
 7 reasonable opportunity for discovery.

8 INTRODUCTION

9 1. Housing authorities harbor significant personally identifiable information (“PII”) and
 10 protected health information (“PHI”) (together, “PII/PHI”) for countless members of the community
 11 who trust that their sensitive and private information is safe. Unfortunately, this trust is misplaced
 12 and violated when housing authorities knowingly subject themselves to the risk of cyberattacks.

13 2. HACLA is a state-chartered public agency providing affordable housing to low-
 14 income individuals and families in Los Angeles, California.¹ HACLA maintains more than 6,800
 15 units of public housing and oversees the city’s Section 8 housing voucher program, which provides
 16 subsidies to more than 56,800 households renting apartments on the private market. With an annual
 17 budget of more than \$1.84 billion, HACLA has grown to become one of the nation’s largest and
 18 leading public housing authorities, providing the largest supply of quality affordable housing to
 19 residents of the City of Los Angeles.² Accordingly, HACLA maintains sensitive PII/PHI for
 20 countless members of the community who trust that their sensitive and private information is safe.

21 3. Given the breadth of individuals’ information at risk (including individuals social
 22 security numbers and medical information that cannot be changed), HACLA is an attractive target
 23 for a cyber-attack.

26 ¹ Justin Luna, *Los Angeles Housing Authority Discloses Data Breach After It Suffers Ransomware*
 27 *Attack*, NEOWIN (March 14, 2023), https://www.neowin.net/news/los-angeles-housing-authority-discloses-data-breach-after-it-suffers-ransomware-attack/?&web_view=true (last accessed on
 28 May 15, 2023).

² *Fact Sheet*, HACLA, <https://www.hacla.org/sites/default/files/Documents/2022-hacla-fact-sheet-v4.pdf> (last accessed on May 15, 2023).

1 4. In or about March of 2023, HACLA issued a data breach notice to its members
2 notifying them that on December 31, 2022, HACLA discovered that it had been the victim of a
3 complex cyber-attack after finding encrypted files on certain of its computer systems.³ After a
4 forensic investigation, it was determined that there was **unauthorized access to certain servers for**
5 **almost a full year**, between January 15, 2022 through December 31, 2022.⁴

6 5. Subsequently, HACLA undertook a review of all data contained on its systems that
7 may have been the subject of any unauthorized access or acquisition. On February 13, 2023,
8 HACLA completed this review and determined that the impacted systems contained certain personal
9 information.⁵

10 6. Despite its awareness that it was storing highly sensitive personal and medical
11 information that is often valuable and vulnerable to cyber attackers, HACLA failed to take the basic
12 security precautions that could have protected Plaintiff's and the Class's (defined below) sensitive
13 data. For instance, HACLA could archive data, preventing individuals from accessing any personal
14 data by remote use of systems. Instead, HACLA used grossly inadequate computer systems and data
15 security practices that allowed hackers to easily make off with the affected individuals' personal
16 data. These extreme instances of data theft take time, and there were numerous steps along the way
17 where any company following standard IT security practices would have foiled the hackers. But
18 HACLA failed to take these basic precautions.

19 7. The HACLA database breach included unauthorized access to the types of
20 information that federal and state law require companies to take security measures to protect. This
21 includes, but is not limited to:

- 22 a. **Individual's name,**
- 23 b. **Social Security number,**
- 24 c. **Date of birth,**
- 25 d. **Passport number,**

26 _____
27 ³ Bill Toulas, *L.A Housing Authority Discloses Data Breach After Ransomware Attack*, BLEEPING
28 COMPUTER (March 13, 2023), <https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/> (last accessed on May 15, 2023).

⁴ *Id.*

⁵ *Id.*

- e. **Driver’s license number or state identification number,**
- f. **Tax identification number,**
- g. **Military identification number,**
- h. **Government issued identification number,**
- i. **Credit/debit card number,**
- j. **Financial account number,**
- k. **Health insurance information, and**
- l. **Medical information**⁶ (collectively, “PII/PHI”).

8. This data should have received extra, not substandard, protection.⁷

9. Plaintiff, and everyone affected, is now a victim of identity theft – as any combination of this private information will forever subject them to being targets of cyber-attacks. Passport number cannot be changed. Social Security number cannot be changed. Government/State IDs cannot be changed. Health Information and history remain the same. Tax Identification number remains the same. Therefore, the extent and level of the private information is highly substantial, and will affect the victims of this data breach – Plaintiff and the class, forever. Even years from now, Plaintiff and other affected victims will be subjects to cyber-attacks, and phishing scams. After passwords are changed, third parties who possess this information can easily re-set the passwords, gain access to their bank accounts, continue apply for credit, and gain access to victim’s telephones (or be able to do sim-swaps).

10. Any entity with reasonable data security practices and procedures – especially one guarding valuable data that was a known target for cyber attackers – would monitor for a data security breach. In other words, even if a company negligently left the “bank vault” open (**as HACLA did for almost a full year**), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. However, HACLA failed to implement many standard monitoring and alerting systems.

⁶ *Fact Sheet*, HACLA, <https://www.hacla.org/sites/default/files/Documents/2022-hacla-fact-sheet-v4.pdf> (last accessed on May 15, 2023).

⁷ Further discovery may demonstrate that the HACLA Database contained information regarding additional individuals.

1 11. This was the second major attack on L.A.’s public sector over the past year. The Los
2 Angeles Unified School District was hit by a ransomware attack in September 2022, and students’
3 personal information was posted in October after school administrators refused to pay.⁸ As such,
4 HACLA was aware that Los Angeles County systems were vulnerable to attack by unauthorized
5 third parties. HACLA could have taken measures to prevent the attack but failed to do so.

6 12. HACLA disregarded the rights of Plaintiff and the Class by intentionally, willfully,
7 recklessly or negligently: (a) failing to take adequate and reasonable measures to ensure the security
8 of its database; (b) concealing or otherwise omitting the material fact that they did not have systems
9 in place to safeguard individuals’ PII/PHI; (c) failing to take available steps to detect and prevent
10 the data breach; (d) failing to monitor its data base and to timely detect the data breach; and (e)
11 failing to provide Plaintiff and the Class prompt and accurate notice of the data breach.

12 13. Due to HACLA’s inadequate security practices and negligence of identifying system
13 vulnerabilities, affected Class Members now face a constant threat of repeated harm, including but
14 not limited to having to live the rest of their lives knowing that criminals have the ability to compile,
15 build and amass their profiles for decades – **exposing them to a never-ending threat of identity**
16 **theft, phishing scams, threats, extortion, bullying and harassment**.

17 14. Plaintiff and Class Members retain a significant interest in ensuring that their PII/PHI,
18 which remains in HACLA’s possession, is protected from further breaches, and seek to remedy the
19 harms suffered as a result of the data breach for himself and on behalf of similarly situated persons
20 whose PII/PHI was stolen.

21 15. Plaintiff, individually, and on behalf of similarly situated persons, seeks to recover
22 damages, equitable relief, including injunctive relief, designed to prevent a reoccurrence of the data
23 breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys’ fees, and all
24 other remedies deemed proper.

25 ///

26 ///

27 _____
28 ⁸ Jonathan Lloyd, *What to Know About the LAUSD Ransomware Attack*, NBC LOS ANGELES
(October 3, 2022), <https://www.nbclosangeles.com/news/local/lausd-ransomware-attack-stolen-hackers-files-information/2998012/> (last accessed on May 15, 2023).

1 **PARTIES**

2 16. Plaintiff Michael Azar, is and at all relevant times, was a California resident. Plaintiff
3 applied for affordable housing through the housing authority of the city of Los Angeles sometime
4 in 2019 and provided sensitive private information to HACLA.

5 17. Plaintiff is an applicant for housing with HACLA. To submit an application with
6 HACLA, Plaintiff was required to and did provide his PII/PHI. In making the decision to input
7 sensitive information into HACLA’s platform, Plaintiff reasonably expected that HACLA would
8 safeguard his PII/PHI. Plaintiff would not have trusted HACLA with his PII/PHI if he knew that his
9 PII/PHI collected by HACLA would be at risk. Plaintiff has suffered irreparable damages and
10 remains at a significant risk now that both his PII/PHI has been leaked online. Plaintiff has received
11 multiple notifications of hackers attempting to gain unauthorized access to several of his accounts
12 including social media shortly after the data breach attack. Further, Plaintiff has been experiencing
13 an exponential increase in spam texts, emails and calls.

14 18. HACLA is a state-chartered public agency providing affordable housing to low-
15 income individuals and families in Los Angeles, California. HACLA receives and expends
16 California and federal public funds.⁹ HACLA is organized and exists under and pursuant to the
17 constitution and laws of the State of California and with a primary business address of 2600 Wilshire
18 Blvd, Los Angeles, CA 90057. HACLA manages public housing developments and other rental
19 assistance programs, collecting personal and financial information from thousands of people who
20 receive or apply for housing assistance. HACLA has committed the wrongful acts alleged herein in
21 the County of Los Angeles, State of California.

22 **JURISDICTION AND VENUE**

23 19. This Court has original jurisdiction over all causes of action asserted herein pursuant
24 to the California Constitution, Article VI, section 10.

25 20. HACLA has committed the wrongful acts alleged herein in the County of Los
26 Angeles, State of California.

27
28 ⁹ *Fact Sheet* – HACLA, <https://www.hacla.org/sites/default/files/Documents/2022-hacla-fact-sheet-v4.pdf> (last accessed on May 15, 2023).

1 26. The U.S. Government Accountability Office has concluded that it is common for data
2 thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.¹³
3 In the same report, the Government Accountability Office noted that while credit monitoring
4 services can assist with detecting fraud, those services do not stop it.¹⁴

5 27. When companies entrusted with people’s data fail to implement industry best
6 practices, cyberattacks and other data exploitations can go undetected for a long period of time. This
7 worsens the ramifications and can even render the damages irreparable.

8 28. PII is a valuable commodity for which a black market exists on the dark web, among
9 other places. Personal data can be worth from \$1,000-\$1,200 on the dark web^{15,16} and the legitimate
10 data brokerage industry is valued at more than \$250 billion dollars.

11 29. In this black market, criminals seek to sell the spoils of their cyberattacks to identity
12 thieves who desire the data to extort and harass victims, take over victims’ identities in order to
13 open financial accounts, and otherwise engage in illegal financial transactions under the victims’
14 names.

15 30. PII/PHI have a distinct, high value—which is why legitimate companies and criminals
16 seek to obtain and sell it. As alleged in more detail below, there is a growing market for individuals’
17 data.¹⁷

18 31. The U.S. Department of Justice’s Bureau of Justice Statistics has found that “among
19 victims who had personal information used for fraudulent purposes, 29% spent a month or more
20 resolving problems” and that resolution of those problems could take more than a year. Medical
21 information in particular is extremely valuable to identity thieves, and thus, the medical industry
22

23 ¹³ U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches –*
24 *Range of Consumer Risks Highlights Limitations of Identity Theft Services* (March 2019),
<https://www.gao.gov/assets/700/697985.pdf> (last accessed on May 15, 2023).

25 ¹⁴ *Id.*

26 ¹⁵ Ryan Smith, *Revealed-how much is personal data worth on the dark web?*, INSURANCE BUSINESS
MAGAZINE, [https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-](https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx)
27 [personal-data-worth-on-the-dark-web-444455.aspx](https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx) (last accessed May 15, 2023).

28 ¹⁶ Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*,
MARKETWATCH (last accessed May 15, 2023).

¹⁷ Emily Wilson, *The Worrying Trend of Children’s Data Being Sold on the Dark Web*, TNW
(February 23, 2019), [https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-](https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/)
web/ (last accessed on May 15, 2023).

1 has also experienced disproportionately higher numbers of data theft events than other industries.
 2 According to a report by the Health Insurance Portability and Accountability Act (“HIPAA”)
 3 Journal, “healthcare data breach statistics clearly show there has been an upward trend in data
 4 breaches over the past nine (9) years, with 2018 seeing more data breaches reported than any other
 5 year since records first started being published.”¹⁸

6 32. A study done by Experian found that the “average total cost” of medical identity theft
 7 is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
 8 to pay out of pocket costs for healthcare they did not receive in order to restore coverage.¹⁹ Indeed,
 9 data breaches and identity theft have a crippling effect on individuals and detrimentally impact the
 10 economy as a whole.

11 **The Sensitivity of Individuals’ Data Demands Heightened, Vigilant, Protection**

12 33. Public sector entities are popular targets for cyberattacks and require top-tier security
 13 measures to protect the PII/PHI of users. This was the second major attack on L.A.’s public sector
 14 over the past year. The Los Angeles Unified School District was hit by a ransomware attack in
 15 September 2022, and students’ personal information was posted in October after school
 16 administrators refused to pay.²⁰ As such, HACLA was aware that Los Angeles County systems were
 17 vulnerable to attack by unauthorized third parties. HACLA could have taken measures to prevent
 18 the attack but failed to do so.

19 34. In the instant data breach, a ransomware gang, called LockBit, which is known to be
 20 one of the most notorious ransomware-as-a-service operators today, claimed responsibility for the
 21 cyberattack against HACLA.²¹ The threat actors uploaded a sample of the files they claim to have
 22

23
 24 ¹⁸ *Healthcare Data Breach Statistics*, THE HIPPA JOURNAL,
<https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last accessed on May 15, 2023).

25 ¹⁹ Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (March 3, 2010),
<https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last
 26 accessed on May 15, 2023).

27 ²⁰ Jonathan Lloyd, *What to Know About the LAUSD Ransomware Attack*, NBC Los Angeles,
 (October 3, 2022), [https://www.nbclosangeles.com/news/local/lausd-ransomware-attack-stolen-
 28 hackers-files-information/2998012/](https://www.nbclosangeles.com/news/local/lausd-ransomware-attack-stolen-hackers-files-information/2998012/) (last accessed on May 15, 2023).

²¹ *Hackers Target L.A.’s Housing Authority in a Suspected Ransomware Attack*, LOS ANGELES
 TIMES (January 4, 2023), [https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-
 s-housing-authority-in-a-suspected-ransomware-attack](https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-housing-authority-in-a-suspected-ransomware-attack) (last accessed on May 15, 2023).

1 stolen from HACLA on December 31, 2022, then followed it up with a threat on January 27, 2023
2 to leak all files.²² The LockBit gang tried to negotiate with the agency but failed to reach an
3 agreement.

4 35. A Los Angeles Times review of publicly available information on LockBit’s site on
5 the dark web found what appeared to be a HACLA bank statement and a list of folders.²³ The group
6 said on the website that information would be released on January 12, 2023 if a ransom were not
7 paid. LockBit’s site claimed that the group had obtained more than 15TB of files. The folder names
8 suggested a broad range of data ranging from sensitive to mundane — **from payroll, audits and**
9 **taxes to a 2021 holiday video.**

10 36. The size of the data set and the structure of the folders suggested that the attack
11 targeted a shared file storage system and not a single machine.

12 37. LockBit was described as “one of the most active and destructive ransomware variants
13 in the world” in a criminal complaint filed by the Department of Justice against an alleged
14 participant.²⁴ A ransomware gang called “LockBit” claimed responsibility for the attack and
15 uploaded samples of the files they had stolen from HACLA’s network. The attackers set a ransom
16 date, by which an undisclosed amount of money was to be made in exchange for the non-disclosure
17 of the information. They threatened to publish all the files on January 27, 2023. Upon information
18 and belief, ransom negotiations failed as the public-agency declined to meet the hackers’
19 demands.²⁵

20 38. **HACLA did not recognize its systems were infiltrated for almost a full year.**

21 _____
22 ²² Bill Toulas, *L.A Housing Authority Discloses Data Breach After Ransomware Attack*, BLEEPING
23 COMPUTER (March 13, 2023), [https://www.bleepingcomputer.com/news/security/la-housing-](https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/)
24 [authority-discloses-data-breach-after-ransomware-attack/](https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/) (last accessed on May 15, 2023).

25 ²³ *Hackers Target L.A’s Housing Authority in a Suspected Ransomware Attack*, LOS ANGELES
26 TIMES, (January 4, 2023), [https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-](https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-housing-authority-in-a-suspected-ransomware-attack)
27 [housing-authority-in-a-suspected-ransomware-attack](https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-housing-authority-in-a-suspected-ransomware-attack) (last accessed on May 15, 2023).

28 ²⁴ *Man Charged for Participation in Lockbit Global Ransomware Campaign*, The United States
Department of Justice (November 10, 2022), [https://www.justice.gov/opa/pr/man-charged-](https://www.justice.gov/opa/pr/man-charged-participation-lockbit-global-ransomware-campaign)
participation-lockbit-global-ransomware-campaign (last accessed on May 15, 2023).

²⁵ *Hackers Target L.A’s Housing Authority in a Suspected Ransomware Attack*, LOS ANGELES TIMES
(January 4, 2023), [https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-](https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-housing-authority-in-a-suspected-ransomware-attack)
[housing-authority-in-a-suspected-ransomware-attack](https://www.latimes.com/california/story/2023-01-03/hackers-target-l-a-s-housing-authority-in-a-suspected-ransomware-attack); Bill Toulas, *L.A Housing Authority Discloses Data Breach After Ransomware Attack*, BLEEPING COMPUTER (March 13, 2023),
[https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-](https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/)
[after-ransomware-attack/](https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/) (last accessed on May 15, 2023).

1 39. To date, HACLA has failed to fully explain the full scope of this breach. HACLA did
2 not disclose how many individuals' PII/PHI was breached, leaving individuals to speculate whether
3 it is likely that their PII/PHI has been compromised.

4 40. This attack allowed the hackers to access sensitive information such as full names,
5 Social Security numbers, dates of birth, passport numbers, driver's licenses, state ID numbers, tax
6 ID numbers, military ID numbers, government-issued ID numbers, credit/debit card numbers,
7 financial account numbers, health insurance information, and medical information.

8 **HACLA's Duty to Safeguard PII/PHI**

9 41. HACLA is one of the nation's largest and leading public housing authorities. HACLA
10 provides affordable housing to more than 83,000 households in its Public Housing and Section 8
11 rental assistance programs and offers a range of permanent supportive housing programs for
12 homeless households.²⁶

13 42. As a housing authority, HACLA collects, receives, and accesses its members'
14 extensive individually identifiable information. These records include personal information such as
15 individual's name, Social Security number, date of birth, passport number, driver's license number
16 or state identification number, tax identification number, military identification number,
17 government issued identification number, credit/debit card number, financial account number,
18 health insurance information, and medical information (collectively "PII/PHI").

19 43. Through the collection and use of individuals' PII/PHI, HACLA uses third-party
20 companies to advertise to consumers in order to obtain additional public funding. By obtaining,
21 collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII/PHI, HACLA
22 assumed legal and equitable duties to those individuals, including the duty to protect Plaintiff's and
23 Class Members' PII/PHI from disclosure.

24
25
26
27
28

²⁶ "About Hacla." HACLA, <https://www.hacla.org/en/about-hacla>. (last accessed on May 15, 2023).

1 44. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
2 businesses which highlight the importance of implementing reasonable data security practices.
3 According to the FTC, the need for data security should be factored into all decision-making.²⁷

4 45. The FTC has issued numerous guides for entities engaged in commerce highlighting
5 the importance of reasonable data security practices.

6 46. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide
7 for Business, which established cybersecurity guidelines for businesses.²⁸ The guidelines note that
8 businesses should protect the personal customer information that they keep; properly dispose of
9 personal information that is no longer needed; encrypt information stored on computer networks;
10 understand their network’s vulnerabilities; and implement policies to correct any security problems.

11 47. The FTC further recommends that entities not maintain PII/PHI longer than is needed
12 for authorization of a transaction; limit access to sensitive data; require complex passwords to be
13 used on networks; use industry-tested methods for security; monitor for suspicious activity on the
14 network; and verify that third-party service providers have implemented reasonable security
15 measures.²⁹

16 48. The FTC has brought enforcement actions against entities engaged in commerce for
17 failing to adequately and reasonably protect customer data, treating the failure to employ reasonable
18 and appropriate measures to protect against unauthorized access to confidential consumer data as
19 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
20 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
21 take to meet their data security obligations.

22 49. Beyond HACLA’s legal obligations to protect the confidentiality of individuals’
23 PII/PHI, HACLA’s privacy policy and online representations affirmatively and unequivocally state

24 _____
25 ²⁷ Federal Trade Commission, *Start With Security*, available
at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last
accessed on May 15, 2023).

26 ²⁸ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available
at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-
information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf)

27 ²⁹ Federal Trade Commission, *Start With Security*, available at
28 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last
accessed on May 15, 2023).

1 that any personal information provided to HACLA will remain secure and protected. For many
 2 years, HACLA represented and continues to represent that it is “committed” to value and protecting
 3 consumer privacy by making representations such as:

- 4 a. *“We are committed to protecting the privacy of our customers and others who may*
 5 *visit our website.”*³⁰
- 6 b. *“[W]e take appropriate measures to safeguard against unauthorized disclosures of*
 7 *information.”*³¹

8 50. HACLA has unequivocally failed to adhere to a single promise vis-à-vis their duty to
 9 safeguard PII/PHI of its applicants. HACLA has made these privacy policies and commitments
 10 available in a variety of documents, including its websites. HACLA included these privacy policies
 11 and commitments to maintain the confidentiality of its members’ sensitive information as terms of
 12 its contracts with those members, including contracts entered into with Plaintiff and the Class. In
 13 these contract terms and other representations to Plaintiff and Class Members and the public,
 14 HACLA promised to take specific measures to protect its members’ information, consistent with
 15 industry standards and federal and state law. However, it did not.

16 51. Plaintiff and Class Members relied to their detriment on HACLA’s uniform
 17 representations and omissions regarding data security, including HACLA’s failure to alert
 18 individuals that its security protections were inadequate, or at the very minimum warn individuals
 19 of the anticipated and foreseeable data breach.

20 52. Since the HACLA data breach, Class Members face a constant threat of continued
 21 harm. Now that their sensitive *personal and medical information - their Social Security numbers,*
 22 *dates of birth, home addresses, medical information* – is in possession of third parties, Class
 23 Members must worry about being victimized throughout the rest of their lives. Data breach affecting
 24 private information compromises individual’s whereabouts and routines, subjecting them to the
 25 danger of potential attacks, embarrassment, or even kidnapping.

26
 27 _____
 28 ³⁰ *Privacy Statement*, HACLA, <https://www.hacla.org/en/privacy-statement> (last accessed on May 15, 2023).

³¹ *Id.*

1 53. Plaintiff and other similarly situated individuals trusted HACLA with sensitive and
2 valuable PII/PHI. Had HACLA disclosed to Plaintiff and its other members that its data systems
3 were not secure at all and were vulnerable to attack, Plaintiff would not have trusted HACLA with
4 such sensitive information. In fact, HACLA would have been forced to adopt reasonable data
5 security measures and comply with the law.

6 54. HACLA knew or should have known that Plaintiff and Class Members would
7 reasonably rely upon and trust HACLA's promises regarding security and safety of its data and
8 systems.

9 55. By collecting victims' PII/PHI and utterly failing to protect it by maintaining
10 inadequate security systems, **which were under attack for almost a full year without any**
11 **detection**, failing to properly archive the PII/PHI, allowing access of third parties, and failing to
12 implement security measures, HACLA caused harm to Plaintiff and all affected individuals.

13 **HACLA's Failure to Protect Against the Data Breach**

14 56. At all material times, HACLA failed to maintain proper security measures despite its
15 promises of safety and security to individuals who were forced to entrust HACLA with their most
16 private and sensitive information.

17 57. HACLA failed to implement basic industry-accepted data security tools to prevent
18 cyber attackers from accessing the HACLA Database: HACLA allowed users to access personal
19 information for almost a full year and failed to encrypt the sensitive personal information within its
20 database. If HACLA had taken either one of these basic security steps, the cyber attackers would
21 not have been able to access or use Plaintiff's or Class Members' sensitive personal information.

22 58. It was reasonably foreseeable that HACLA's failure to adequately investigate the
23 security practices and measures in place would allow hackers to one day gain unlawful and
24 unauthorized access to this sensitive information.

25 59. HACLA knew that PII/PHI was valuable on the dark web and thus, was aware that
26 HACLA was a potential target of cybercriminals seeking to obtain that information for financial
27 gain or other nefarious purposes. HACLA knew or should have known of the importance of
28 cybersecurity and complied with state and federal law to protect victims' PII/PHI.

1 60. Despite HACLA’s full knowledge of the sensitivity of stolen data, HACLA failed to
2 implement any proper security measures to secure and protect the PII/PHI of affected individuals.
3 As a result, countless people now must live the rest of their lives knowing that criminals have the
4 ability to compile, build and amass their profiles for decades to come – exposing them to a never-
5 ending *threat of kidnapping, identity theft, extortion, bullying and harassment.*

6 **Impact of Data Breach on Affected Individuals**

7 61. The PII/PHI exposed in the data breach is highly coveted and valuable on underground
8 or black markets. For example, a cyber “black market” exists in which criminals openly post and
9 sell stolen consumer information on underground internet websites known as the “dark web” –
10 exposing consumers to identity theft and fraud for years to come. Identity thieves can use the
11 PII/PHI to: (a) create fake credit cards that can be swiped and used to make purchases as if they
12 were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from
13 ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver’s license or ID card in the
14 victim’s name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the
15 victim’s information; (g) commit medical and healthcare-related fraud; (h) access financial accounts
16 and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing,
17 or giving false information to police during an arrest.

18 62. Medical data is particularly valuable because unlike financial information, such as
19 credit card numbers which can be quickly changed, medical data is static. This is why companies
20 possessing medical information, like HACLA, are intended targets of cyber-criminals.

21 63. Accordingly, Plaintiff and the Class have suffered actual harm as a result of HACLA’s
22 conduct. HACLA failed to institute adequate security measures and neglected system vulnerabilities
23 that led to a data breach. This breach allowed hackers to access the PII/PHI of individuals. This
24 PII/PHI has since been or is subject to being publicly leaked online which has allowed for digital
25 and potential physical attacks against Plaintiff and the Class. Now that the PII/PHI has been leaked,
26 it is available for other parties to sell or trade and will continue to be at risk for the indefinite future.
27 “The hackers have encryption skills to cover their tracks and hide what they saw so we will only
28

1 know the entirety of the data they have with time.”³² In fact, the U.S. Government Accountability
2 Office found that, “once stolen data have been sold or posted on the Web, fraudulent use of that
3 information may continue for years.”³³ Cybersecurity experts warn, “in 15 years [the victims] could
4 come to find their name was used to buy a condo in Bora Bora.”³⁴

5 64. Exposure of this information to the wrong people can have serious consequences. The
6 impact of identity theft can have ripple effects, which can adversely affect the future financial
7 trajectories of victims’ lives. For example, the Identity Theft Resource Center reports that identity
8 theft can impact an individual’s ability to get credit cards and obtain loans, such as student loans or
9 mortgages.³⁵ For some victims, this could mean the difference between going to college or not,
10 becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-
11 interest loan.

12 65. There may also be a significant time lag between when personal information is stolen
13 and when it is actually misused. According to the GAO, which conducted a study regarding data
14 breaches:

15 *“[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a*
16 *year or more before being used to commit identity theft. Further, once stolen data have been*
17 *sold or posted on the Web, fraudulent use of that information may continue for years. As a*
18 *result, studies that attempt to measure the harm resulting from data breaches cannot*
19 *necessarily rule out all future harm.”³⁶*

20 _____
21 ³² Howard Blume and Alejandra Reyes-Velarde, *Private Data of 400k LAUSD Students Could be*
at Risk, LOS ANGELES TIMES (September 9, 2022), [https://www.govtech.com/education/k-](https://www.govtech.com/education/k-12/private-data-of-400k-laUSD-students-could-be-at-risk)
22 [12/private-data-of-400k-laUSD-students-could-be-at-risk](https://www.govtech.com/education/k-12/private-data-of-400k-laUSD-students-could-be-at-risk) (last accessed on May 15, 2023).

23 ³³ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the*
Full Extent Is Unknown, U.S. GOVERNMENT ACCOUNTABILITY OFFICE: REPORT TO
24 CONGRESSIONAL REQUESTERS (June 2007), <https://www.gao.gov/new.items/d07737.pdf> (last
25 accessed on May 15, 2023).

26 ³⁴ Mark Keierlber, *LAUSD Downplays Student Harm After Cyber Gang Posts Sensitive Data*
Online, LA SCHOOL REPORT (November 11, 2022), [https://www.laschoolreport.com/cyber-gang-](https://www.laschoolreport.com/cyber-gang-posts-los-angeles-students-sensitive-data-on-dark-web-after-hack/)
27 [posts-los-angeles-students-sensitive-data-on-dark-web-after-hack/](https://www.laschoolreport.com/cyber-gang-posts-los-angeles-students-sensitive-data-on-dark-web-after-hack/) (last accessed on May 15,
28 2023).

29 ³⁵ *Identity Theft: The Aftermath 2017*, Identity Theft Resource Center,
https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last
30 accessed on May 15, 2023).

31 ³⁶ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the*
Full Extent Is Unknown, U.S. GOVERNMENT ACCOUNTABILITY OFFICE: REPORT TO

1 66. **Threat of Identity Theft:** As a direct and proximate result of HACLA’s breach of
2 confidence and failure to protect the PII/PHI of individuals, Plaintiff and the Class have also been
3 injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and
4 other misuse of this PII/PHI, resulting in ongoing monetary loss and economic harm, loss of value
5 of privacy and confidentiality of the stolen PII/PHI, illegal sales of the compromised PII/PHI on the
6 black market, mitigation expenses and time spent on credit monitoring, identity theft insurance,
7 credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties,
8 decreased credit scores, lost work time, and other injuries. HACLA, through its misconduct, has
9 enabled numerous bad actors to sell and profit off of PII/PHI that belongs to Plaintiff and the Class.

10 67. But for HACLA’s unlawful conduct, scammers would not have access to Plaintiff’s
11 and the Class Members’ contact information. HACLA’s unlawful conduct has directly and
12 proximately resulted in a widespread threat of digital attacks against Plaintiff and the Class.

13 68. **Credit Card Fraud:** Plaintiff has experienced unauthorized credit card inquiries on
14 several of his banking accounts shortly after the data breach attack. Plaintiff and the Class face
15 ongoing, imminent threats of similar fraud claims and scams, resulting in ongoing monetary loss
16 and economic harm, mitigation expenses, and time spent on credit monitoring, credit
17 freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties,
18 decreased credit scores, lost work time, and other injuries.

19 69. **Loss of Time:** As a result of this breach, Plaintiff was forced to spend significant time
20 monitoring all of his personal accounts for fraudulent activity. Plaintiff is experiencing a great
21 amount of distress and frustration in attempting to change his passwords and associated accounts
22 which may be connected to various pieces of stolen PII/PHI. Plaintiff has been living in constant
23 fear and apprehension of further attacks against them.

24 70. Plaintiff is now forced to research and subsequently acquire reasonable identity theft
25 defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending
26 out of pocket expenses to pay for these services.

27
28 _____
CONGRESSIONAL REQUESTERS (June 2007), <https://www.gao.gov/new.items/d07737.pdf> (last
accessed on May 15, 2023).

1 71. HACLA also used Plaintiff’s and Class Members’ PII/PHI for profit and continued to
2 use Plaintiff’s and Class Members’ PII/PHI to share their information with various third parties for
3 HACLA’s own benefit. Specifically, through the collection and use of individuals’ PII/PHI,
4 HACLA uses third-party companies to advertise to community members in order to obtain
5 additional applications for housing, which ultimately results in HACLA receiving increased public
6 funding. According to HACLA’s online website, its funds come from five main sources; HUD’s
7 annual operating subsidy, HUD’s annual Capital Fund, Section 8 administrative fees, rent from
8 public housing residents plus other programs and capital grants from various sources.³⁷

9 72. **Phishing Scams:** Phishing scammers use emails and text messages to trick people
10 into giving them their personal information, including but not limited to passwords, account
11 numbers, and Social Security numbers. Phishing scams are frequently successful, and the FBI
12 reported that people lost approximately \$57 million to such scams in 2019 alone.³⁸

13 73. As a result of the data breach, Plaintiff and Class Members are at high risk of receiving
14 high-volume of phishing emails and spam telephone calls. Such scams trick individuals into giving
15 account information, passwords, and other valuable personal information to scammers. This
16 significantly increases the risk of further substantial damage to Plaintiff and the Class, including,
17 but not limited to, monetary and identity theft. Due to the breach, Plaintiff and Class Members now
18 need to spend a substantially increased amount of time and effort discerning between genuine emails
19 and emails that are trying to phish sensitive PII/PHI.

20 74. **SIM-Swap:** The data leak can also lead to SIM-swap attacks against the impacted
21 individuals.⁹ A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the
22 victim’s phone number to the scammer’s SIM card. By doing so, the attacker is able to bypass two-
23 factor authentication accounts, as are used to access cryptocurrency wallets and other important
24 accounts. The type of personal information that has been leaked poses a profound tangible risk of
25 SIM-swap attacks for the Class.

27 ³⁷ *About Us*, HACLA, <https://www.hacla.org/en/about-us> (last accessed on May 15, 2023).

28 ³⁸ *How to Recognize and Avoid Phishing Scams*, FTC CONSUMER ADVICE, <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams> (last accessed on May 15, 2023).

1 75. Individuals who trusted HACL A with their PII/PHI are now more likely to become
2 victims of SIM Swap attacks because of the released personal information.

3 76. Given the highly sensitive nature of the information stolen, and its dissemination to
4 unauthorized parties, Plaintiff has already suffered injury and remain at a substantial and imminent
5 risk of future harm.

6 **Summary of Actual Economic and Noneconomic Damages**

7 77. In sum, Plaintiff and similarly situated individuals were injured as follows:

- 8 a. Theft of their PII/PHI and the resulting loss of privacy rights in that information;
- 9 b. Improper disclosure of their PII/PHI;
- 10 c. Loss of value of their PII/PHI;
- 11 d. The amount of ongoing reasonable identity defense services made necessary as
12 mitigation measures;
- 13 e. Economic and non-economic impacts that flow from imminent, and ongoing
14 threat of fraud and identity theft to which Plaintiff is now exposed to;
- 15 f. Ascertainable out-of-pocket expenses and the value of their time allocated to
16 fixing or mitigating the effects of this data breach;
- 17 g. Emotional distress, and fear associated with the imminent threat of harm from
18 the continued phishing scams and attacks as a result of this data breach.

19 **CLASS ALLEGATIONS**

20 78. Plaintiff brings this action on his own behalf and on behalf of all other persons
21 similarly situated. The Class which Plaintiff seeks to represent comprises:

22 “All persons in the United States and whose PII/PHI was accessed, compromised, or stolen
23 in the data breach discovered by HACL A on December 31, 2022.” (the “Class”).

24 79. The Class is comprised of numerous of individuals throughout the United States and
25 the state of California. The Class is so numerous that joinder of all members is impracticable and
26 the disposition of their claims in a class action will benefit the parties.

27 80. There is a well-defined community of interest in the questions of law and fact involved
28 affecting the parties to be represented in that the Class was exposed to the same common and

1 uniform false and misleading advertising and omissions. The questions of law and fact common to
2 the Class predominate over questions which may affect individual Class Members. Common
3 questions of law and fact include, but are not limited to, the following:

- 4 a. Whether HACLA's conduct is an unlawful business act or practice within the
5 meaning of Business and Professions Code section 17200, *et seq.*;
- 6 b. Whether HACLA's conduct is an unfair business act or practice within the
7 meaning of Business and Professions Code section 17200, *et seq.*;
- 8 c. Whether HACLA's conduct is in violation of California Civil Code Sections
9 1709, 1710;
- 10 d. Whether HACLA's failure to implement effective security measures to protect
11 Plaintiff's and the Class's PII/PHI was negligent;
- 12 e. Whether HACLA represented to Plaintiff and the Class that they would protect
13 Plaintiff's and the Class Members' PII/PHI;
- 14 f. Whether HACLA owed a duty to Plaintiff and the Class to exercise due care in
15 collecting, storing, and safeguarding their PII/PHI;
- 16 g. Whether HACLA breached a duty to Plaintiff and the Class to exercise due care
17 in collecting, storing, and safeguarding their PII/PHI;
- 18 h. Whether Class Members' PII/PHI was accessed, compromised, or stolen in the
19 breach;
- 20 i. Whether HACLA's conduct caused or resulted in damages to Plaintiff and the
21 Class;
- 22 j. Whether HACLA failed to notify the public of the breach in a timely and
23 adequate manner;
- 24 k. Whether HACLA knew or should have known that its systems were vulnerable
25 to a data breach;
- 26 l. Whether HACLA adequately addressed the vulnerabilities that allowed for the
27 data breach; and
28

1 m. Whether, as a result of HACLA’s conduct, Plaintiff and the Class are entitled to
2 injunctive relief.

3 81. Plaintiff’s claims are typical of the claims of the proposed Class, as Plaintiff and the
4 members of the Class were harmed by HACLA’s uniform unlawful conduct.

5 82. Plaintiff will fairly and adequately represent and protect the interests of the proposed
6 Class. Plaintiff has retained competent and experienced counsel in class action and other complex
7 litigation.

8 83. Plaintiff and the Class have suffered injury in fact as a result of HACLA’s false,
9 deceptive, and misleading representations.

10 84. Plaintiff would not have entrusted HACLA with his PII/PHI but for the reasonable
11 belief that HACLA would safeguard his data and PII/PHI.

12 85. The Class is identifiable and readily ascertainable. Notice can be provided to such
13 purchasers using techniques and a form of notice similar to those customarily used in class actions,
14 and by internet publication, radio, newspapers, and magazines.

15 86. A class action is superior to other available methods for fair and efficient adjudication
16 of this controversy. The expense and burden of individual litigation would make it impracticable or
17 impossible for proposed members of the Class to prosecute their claims individually.

18 87. The litigation and resolution of the Class’s claims are manageable. Individual
19 litigation of the legal and factual issues raised by HACLA’s conduct would increase delay and
20 expense to all parties. The class action device presents far fewer management difficulties and
21 provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive
22 supervision.

23 88. HACLA has acted on grounds generally applicable to the entire Class, thereby making
24 final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class
25 as a whole. The prosecution of separate actions by individual Class Members would create the risk
26 of inconsistent or varying adjudications with respect to individual member of the Class that would
27 establish incompatible standards of conduct for HACLA.

28

1 89. Absent a class action, HACLA will likely retain the benefits of its wrongdoing.
2 Because of the small size of the individual Class Members' claims, few, if any, Class Members
3 could afford to seek legal redress for the wrongs complained of herein. Absent a representative
4 action, the Class Members will continue to suffer losses and HACLA (and similarly situated
5 companies) will be allowed to continue these violations of law.

6 **COUNT ONE**

7 **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**
8 **BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.***

9 90. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully
10 incorporates all allegations in all preceding paragraphs.

11 **A. "Unfair" Prong**

12 91. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200,
13 *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide
14 to individuals and the injury is one that the individuals themselves could not reasonably avoid."
15 *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

16 92. HACLA's conduct of failing to protect and secure its data-holding systems as alleged
17 herein does not confer any benefit to individuals.

18 93. HACLA's conduct as alleged herein causes injuries to individuals who do not receive
19 security consistent with their reasonable expectations.

20 94. HACLA's conduct as alleged herein causes injuries to individuals, who entrusted
21 HACLA with their PII/PHI and whose PII/PHI was leaked as a result of HACLA's unlawful
22 conduct.

23 95. HACLA's failure to implement and maintain reasonable security measures was also
24 contrary to legislatively declared public policy that seeks to protect individuals' data and ensure
25 entities that are trusted with it use appropriate security measures. These policies are reflected in
26 laws, including California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56 as
27 well as Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.
28

1 96. HACLA’s failure to adequately protect the personal customer information that they
2 keep; properly dispose of personal information that is no longer needed; encrypt information stored
3 on computer networks; understand their network’s vulnerabilities; and implement policies to correct
4 any security problems violates Section 5 of the FTC Act which prohibits “unfair or deceptive acts
5 or practices in or affecting commerce.”

6 97. Individuals cannot avoid any of the injuries caused by HACLA’s conduct as alleged
7 herein.

8 98. The injuries caused by HACLA’s conduct as alleged herein outweigh any benefits.

9 99. HACLA’s conduct, as alleged in the preceding paragraphs, is false, deceptive,
10 misleading, and unreasonable and constitutes an unfair business practice within the meaning of
11 California Business and Professions Code Section 17200.

12 100. HACLA could have furthered its legitimate business interests in ways other than by
13 unfair conduct.

14 101. HACLA’s conduct threatens individuals by misleadingly advertising their systems as
15 “secure” and exposing individuals’ PII/PHI to hackers. HACLA’s conduct also threatens other
16 entities, large and small, who play by the rules.

17 102. All of the conduct alleged herein occurs and continues to occur in HACLA’s
18 enterprise. HACLA’s wrongful conduct is part of a pattern or generalized course of conduct repeated
19 on approximately thousands of occasions daily.

20 103. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class
21 seek an order enjoining HACLA from continuing to engage, use, or employ its unfair business
22 practices.

23 104. Plaintiff and the Class have suffered injury-in-fact and have lost money or property
24 as a result of HACLA’s unfair conduct. Plaintiff relied on and trusted that HACLA would keep his
25 PII/PHI safe and secure in part based on HACLA’s representations regarding its security measures.
26 Plaintiff accordingly provided his PII/PHI to HACLA, reasonably believing and expecting that this
27 information would be safe and secure. Plaintiff and the Class would not have given HACLA
28 sensitive PII/PHI, had they known that their PII/PHI was vulnerable to a data breach. Likewise,

1 Plaintiff and the members of the Class seek an order mandating that HACLA implement adequate
2 security practices to protect individuals' PII/PHI. Additionally, Plaintiff and the members of the
3 Class seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully
4 acquired by HACLA by means of HACLA's unfair and unlawful practices.

5 105. On March 30, 2023, Plaintiff submitted a Government Claim Form along with a
6 attached copy of the complaint under the Government Tort Claims Act ("GTCA") to Defendant.

7 **B. "Fraudulent" Prong**

8 106. California Business and Professions Code Section 17200, *et seq.* considers conduct
9 fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the*
10 *West v. Superior Court* (1992) 2 Cal. 4th 1254, 1267.

11 107. HACLA's representations that it adequately protects individuals' PII/PHI is likely to
12 deceive members of the public into believing that HACLA can be entrusted with their PII/PHI, and
13 that PII/PHI gathered by HACLA is not in danger of being compromised.

14 108. HACLA's representations about its data-holding systems, as alleged in the preceding
15 paragraphs, are false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

16 109. HACLA knew or should have known of its fraudulent conduct.

17 110. As alleged in the preceding paragraphs, the material misrepresentations by HACLA
18 detailed above constitute a fraudulent business practice in violation of California Business &
19 Professions Code Section 17200.

20 111. HACLA could have implemented robust security measures to prevent the data breach
21 but failed to do so.

22 112. HACLA's wrongful conduct is part of a pattern or generalized course of conduct.

23 113. Pursuant to Business & Professions Code Section 17203, Plaintiff and the Class seek
24 an order enjoining HACLA from continuing to engage, use, or employ its practice of false and
25 deceptive advertising about the strength or adequacy of its security systems. Likewise, Plaintiff and
26 the Class seek an order requiring HACLA to disclose such misrepresentations.

1 resident shall implement and maintain reasonable security procedures and practices appropriate to
2 the nature of the information, to protect the personal information from unauthorized access,
3 destruction, use, modification, or disclosure.”

4 138. As described above, HACLA failed to implement and maintain reasonable security
5 procedures and practices to protect the Plaintiff’s PII/PHI, and thereby violated the California
6 Customer Records Act.

7 139. Under California Civil Code § 1798.82, any business that obtains and retains PII/PHI
8 must promptly and “in the most expedient time possible and without unreasonable delay” disclose
9 any Data Breach involving such retained data.

10 140. By its above-described wrongful actions, inaction, omissions, and want of ordinary
11 care, HACLA failed to design, adopt, implement, control, direct, oversee, manage, monitor and
12 audit appropriate data security processes, controls, policies, procedures, protocols, and software and
13 hardware systems to safeguard and protect Plaintiff’s PII/PHI.

14 141. HACLA also unreasonably delayed and failed to disclose the Data Breach (and threat
15 of the data breach) to impacted individuals, including Plaintiff, in the most expedient time possible
16 and without unreasonable delay when they knew, or reasonably believed, Plaintiff’s PII/PHI had
17 been wrongfully disclosed to an unauthorized person or persons.

18 142. As a direct and proximate result of HACLA’s above-described wrongful actions,
19 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
20 and its violations of the California CRA, Plaintiff has suffered (and will continue to suffer)
21 economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,
22 immediate and the continuing increased risk of identity theft, identity fraud and financial fraud—
23 risks justifying expenditures for protective and remedial services for which he is entitled to
24 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of his PII/PHI, (iv)
25 deprivation of the value of his PII/PHI, for which there is a well-established national and
26 international market, and/or (v) the financial and temporal cost of monitoring his credit, monitoring
27 his financial accounts, and mitigating his damages.
28

1 143. Plaintiff is also entitled to injunctive relief under California Civil Code Section
2 1798.84(e).

3 **COUNT FOUR**

4 **NEGLIGENCE**

5 144. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all
6 preceding paragraphs.

7 145. HACLA owed a duty to the Plaintiff and the Class to exercise due care in collecting,
8 storing, and safeguarding their PII/PHI. This duty included but was not limited to: (a) designing,
9 implementing, and testing security systems to ensure that individuals' PII/PHI was consistently and
10 effectively protected; (b) implementing security systems that are compliant with state and federal
11 mandates; (c) implementing security systems that are compliant with industry practices; and (d)
12 promptly detecting and notifying affected parties of a data breach.

13 146. HACLA also had a duty to destroy Plaintiff's and Class Members' PII/PHI within an
14 appropriate amount of time after it was no longer required by HACLA, in order to mitigate the risk
15 of the stale PII/PHI being compromised in a data breach.

16 147. HACLA's duties to use reasonable care arose from several sources, including those
17 described below. HACLA had a common law duty to prevent foreseeable harm to others, including
18 the Plaintiff and members of the Class, who were the foreseeable and probable victims of any
19 inadequate security practices.

20 148. HACLA had a special relationship with the Plaintiff and Class Members. Plaintiff and
21 Class Members were compelled to entrust HACLA with their PII/PHI. At relevant times, Plaintiff
22 and Class Members understood that HACLA would take adequate security precautions to safeguard
23 that information. Only HACLA had the ability to protect the Plaintiff's and Class Members' PII/PHI
24 stored on the HACLA data base.

25 149. Further, HACLA's duties to use reasonable data security measures also arose under
26 Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits
27 "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC,
28 the unfair practice of failing to use reasonable measures to protect PII/PHI. Various FTC

1 publications and data security breach orders further form the basis of HACLA’s duties. In addition,
2 individual states have enacted statutes based upon the FTC Act that also created a duty. Plaintiff
3 and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar
4 state statutes) were intended to protect.

5 150. HACLA knew or should have known that the Plaintiff’s and the Class Members’
6 PII/PHI is information that is frequently sought after by hackers.

7 151. HACLA knew or should have known that the Plaintiff and the Class Members would
8 suffer harm if their PII/PHI was leaked.

9 152. HACLA knew or should have known that its security systems were not adequate to
10 protect the Plaintiff’s and the Class Members’ PII/PHI from a data breach, especially in light of the
11 increase in data breaches in the public entity sector.

12 153. HACLA knew or should have known that adequate and prompt notice of the data
13 breach was required such that the Plaintiff and the Class could have taken more swift and effective
14 action to change or otherwise protect their PII/PHI, rather than waiting two full days to notify.
15 HACLA failed to provide timely notice upon discovery of the data breach.

16 154. HACLA’s conduct as described above constituted an unlawful breach of its duty to
17 exercise due care in collecting, storing, and safeguarding Plaintiff’s and the Class Members’ PII/PHI
18 by failing to design, implement, and maintain adequate security measures to protect this
19 information. Moreover, HACLA did not implement, design, or maintain adequate measures to
20 detect a data breach when it occurred.

21 155. HACLA’s conduct as described above constituted an unlawful breach of its duty to
22 provide adequate and prompt notice of the data breach.

23 156. HACLA and the Class entered into a special relationship when Class Members
24 entrusted HACLA to protect their PII/PHI. Plaintiff and the Class trusted HACLA and in doing so,
25 provided HACLA with their PII/PHI, based upon HACLA’s representations that it would implement
26 adequate systems to secure their information. HACLA did not do so. HACLA knew or should have
27 known that their security system was vulnerable to a data breach, especially after similar public
28 entities were recently targeted with cybersecurity attacks.

1 157. HACLA breached its duty in this relationship to implement and maintain reasonable
2 measures to protect the PII/PHI of the Class.

3 158. Plaintiff's and Class Members' PII/PHI would have remained private and secure had
4 it not been for HACLA's wrongful and negligent breach of its duties. The leak of Plaintiff's and the
5 Class Members' PII/PHI, and all subsequent damages, was a direct and proximate result of
6 HACLA's negligence.

7 159. HACLA's negligence was, at least, a substantial factor in causing Plaintiff's and the
8 Class Members' PII/PHI to be improperly accessed, disclosed, and otherwise compromised, and in
9 causing the Class Members' other injuries because of the data breaches.

10 160. The damages suffered by the Plaintiff and the Class Members was the direct and
11 reasonably foreseeable result of HACLA's negligent breach of its duties to adequately design,
12 implement, and maintain security systems to protect Plaintiff's and the Class Members' PII/PHI.
13 HACLA knew or should have known that their security for safeguarding Plaintiff's and the Class
14 Members' PII/PHI was vulnerable to a data breach.

15 161. HACLA's negligence directly caused significant harm to Plaintiff and the Class.
16 Specifically, Plaintiff and the Class are now subject to numerous attacks, including various phishing
17 scams and identity theft.

18 162. HACLA had a fiduciary duty to protect the confidentiality of its communications with
19 the Plaintiff and members of the Class by virtue of the explicit privacy representations HACLA
20 made on its website to the Plaintiff and members of the Class.

21 163. HACLA had information relating to the Plaintiff and members of the Class that it
22 knew or should have known to be confidential.

23 164. Plaintiff's and Class Members' communications with HACLA about sensitive
24 PII/PHI information and their status as applicants for low-income housing was not matters of
25 general knowledge.

26 165. HACLA breached its fiduciary duty of confidentiality by designing its data protection
27 systems in a way to allow for a data breach of a massive caliber.

1 highly vulnerable to cyberattacks and thus, using inadequate security software was vulnerable to
2 data breaches prior to the Data Beach.

3 175. As a proximate result of such unauthorized disclosures, Plaintiff's and Class
4 Members' reasonable expectations of privacy in their PII/PHI was unduly frustrated and thwarted
5 and caused damages to Plaintiff and Class Members.

6 176. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and
7 all other relief that may be available at law or equity. Unless and until enjoined, and restrained by
8 order of this Court, HACLA's wrongful conduct will continue to cause irreparable injury to Plaintiff
9 and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries
10 in that a judgment for monetary damages will not end the invasion of privacy for the Plaintiff and
11 the Class.

12 **COUNT SIX**

13 **BREACH OF CONFIDENCE**

14 177. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all
15 preceding paragraphs.

16 178. At all times during Plaintiff's and Class Members' interactions with Defendant,
17 HACLA was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members'
18 PII/PHI that Plaintiff and Class Members provided to Defendant.

19 179. Defendant's relationship with Plaintiff and Class Members was governed by terms
20 and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and
21 protected in confidence, and would not be disclosed to unauthorized third parties.

22 180. Plaintiff and Class Members provided their PII/PHI to Defendant with the explicit and
23 implicit understandings that Defendant would protect and not permit the PII/PHI to be disseminated
24 to any unauthorized third parties.

25 181. Plaintiff and Class Members provided their PII/PHI to Defendant with the explicit and
26 implicit understandings that Defendant would take precautions to protect that PII/PHI from
27 unauthorized disclosure.
28

1 182. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII/PHI
2 with the understanding that PII/PHI would not be disclosed or disseminated to unauthorized third
3 parties or to the public.

4 183. Due to Defendant's failure to prevent and avoid the Data Breach from occurring,
5 Plaintiff's and Class Members' PII/PHI was disclosed and misappropriated to unauthorized third
6 parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

7 184. As a proximate result of such unauthorized disclosures, Plaintiff and Class Members
8 suffered damages.

9 185. But for Defendant's disclosure of Plaintiff's and Class Members' PII/PHI in violation
10 of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen,
11 viewed, access, and used by unauthorized third parties.

12 186. The injury and harm suffered by Plaintiff and Class Members was the reasonably
13 foreseeable result of Defendant's inadequate security of Plaintiff's and Class Members' PII/PHI.
14 Defendant knew or should have known that its methods of accepting, storing, transmitting and using
15 Plaintiff's and Class Members' PII/PHI was inadequate.

16 187. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class
17 Members have suffered injury, including but not limited to: (i) threat of identity theft; (ii) the loss
18 of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of
19 their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery
20 from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their
21 PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized
22 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
23 Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of
24 time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of
25 the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff
26 and Class Members.

27 188. As a direct proximate result of such unauthorized disclosures, Plaintiff and Class
28 Members have suffered and will continue to suffer other forms of injury and/or harm, including, but

1 not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic
2 losses.

3 **COUNT SEVEN**

4 **UNJUST ENRICHMENT**

5 189. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all
6 preceding paragraphs.

7 190. Plaintiff and Class Members conferred a monetary benefit on HACLA – namely, they
8 provided and entrusted HACLA with their PII/PHI.

9 191. In exchange, Plaintiff and Class Members should have been entitled to have HACLA
10 protect their PII/PHI with adequate data security.

11 192. HACLA appreciated, accepted and retained the benefit bestowed upon it under
12 inequitable and unjust circumstances arising from HACLA’s conduct toward Plaintiff and Class
13 Members as described herein – namely, (a) Plaintiff and Class Members conferred a benefit on
14 HACLA, and HACLA accepted or retained that benefit; and (b) HACLA used Plaintiff and Class
15 Members’ PII/PHI for business purposes.

16 193. HACLA failed to secure Plaintiff’s and Class Members’ PII/PHI and, therefore, did
17 not provide full compensation for the benefit Plaintiff and Class Members provided.

18 194. HACLA acquired the PII/PHI through inequitable means in that they failed to disclose
19 the inadequate security practices previously alleged.

20 195. Plaintiff and Class Members have no adequate remedy at law.

21 196. Under the circumstances, it would be unjust and unfair for HACLA to be permitted to
22 retain any of the benefits that Plaintiff and Class Members conferred on it.

23 197. Under the principles of equity and good conscience, HACLA should not be permitted
24 to retain the PII/PHI belonging to Plaintiff and Class Members because HACLA failed to implement
25 the data management and security measures that industry standards mandate.

26 198. HACLA should be compelled to disgorge into a common fund or constructive trust,
27 for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from the use of
28 Plaintiff and Class Members’ PII/PHI.

1 **COUNT EIGHT**

2 **CONVERSION**

3 199. Plaintiff incorporates the substantive allegations contained in all previous paragraphs
4 as if fully set forth herein.

5 200. Plaintiff and Class Members were the owners and possessors of their PII/PHI.

6 201. Courts recognize that internet users have a property interest in their personal
7 information and data. *See Calhoun v. Google, LLC*, 526 F. Supp. 3d 605, at *21 (N.D. Cal. Mar. 17,
8 2021) (recognizing property interest in personal information and rejecting Google’s argument that
9 “the personal information that Google allegedly stole in not property”); *In re Experian Data Breach*
10 *Litigation*, 2016 U.S. Dist. LEXIS 184500, at *5 (C.D. Cal. Dec. 29, 2016) (loss of value of PII is
11 a viable damages theory); *In re Marriott Int’l Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp.
12 3d 447, 460 (D. Md. 2020) (“The growing trend across courts that have considered this issue is to
13 recognize the lost property value of this [personal] information.”); *Simona Opris v. Sincera*, 2022
14 U.S. Dist. LEXIS 94192, (E.D Pa. 2022) (collecting cases).

15 202. The economic value of this property interest in personal information is well
16 understood, as a robust market for such data drives the entire technology economy. As experts have
17 noted, the world’s most valuable resource is “no longer oil, but data,” and has been for years now.³⁹

18 203. As the result of Defendant’s wrongful conduct, Defendant has interfered with
19 Plaintiff’s and Class Members’ rights to possess and control such property, to which they had a
20 superior right of possession and control at the time of conversion.

21 204. As a direct and proximate result of Defendant’s conduct, Plaintiff and the Class
22 Members suffered injury, damage, loss or harm.

23 205. In failing to adequately safeguard Plaintiff’s PII/PHI, Defendant has acted with
24 malice, oppression and in conscious disregard of the Plaintiff’s and Class Members’ rights.

25 206. Plaintiff and the Class Members did not consent to Defendant’s mishandling and loss
26 of their PII/PHI.

27
28 _____
³⁹ *The world’s most valuable resource is no longer oil, but data.* The Economist (May 6, 2017).

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

- attacks, penetration tests, and audits on HACLA’s systems on a periodic basis;
- h. Requiring HACLA to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;
 - i. Requiring HACLA to segment data by, among other things, creating firewalls and access controls so that if one area of HACLA’s network is compromised, hackers cannot gain access to other portions of HACLA’s systems
 - j. Requiring HACLA to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;
 - k. Requiring HACLA to conduct systematic scanning for data breach related issues;
 - l. Requiring HACLA to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII/PHI data;
 - m. Requiring HACLA to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - n. Requiring HACLA to implement a system of testing 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 HACLA’s policies, programs and systems for protecting PII/PHI;
 - o. Requiring HACLA to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately

1 monitor HACLA’s information networks for threats, both internal and
2 external, and assess whether monitoring tools are appropriately
3 configured, tested, and updated; and

4 p. Requiring all further and just corrective action, consistent with permissible
5 law and pursuant to only those causes of action so permitted.

6 C. That the Court award Plaintiff and the Class damages (both actual damages for
7 economic and non-economic harm and statutory damages) in an amount to be
8 determined at trial;

9 D. That the Court issue appropriate equitable and any other relief (including
10 monetary damages, restitution, and/or disgorgement) against HACLA to which
11 Plaintiff and the Class are entitled, including but not limited to restitution and an
12 Order requiring HACLA to cooperate and financially support civil and/or criminal
13 asset recovery efforts;

14 E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including
15 pursuant to statutory rates of interest set under State law);

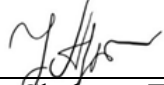
16 F. Plaintiff and the Class be awarded with the reasonable attorneys’ fees and costs of
17 suit incurred by their attorneys;

18 G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as
19 they are allowed by applicable laws; and

20 H. Any and all other such relief as the Court may deem just and proper under the
21 circumstances.

22
23 Dated: May 18, 2023

CLARKSON LAW FIRM, P.C.

24 
25 _____
26 Ryan Clarkson, Esq.
27 Yana Hart, Esq.
28 Tiara Avanes, Esq.
Valter Malkhasyan, Esq.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Housing Authority of the City of Los Angeles Facing Another Class Action Over Lengthy 2022 Cyberattack](#)
