Electronically Filed Superior Court of CA County of Contra Costa 8/30/2023 3:43 PM By: A. Stewart, Deputy

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Kenneth Grunfeld (*pro hac vice* forthcoming)
Kevin W. Fay (*pro hac vice* forthcoming)
GOLOMB SPIRT GRUNFELD
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Telephone: 215.985.9177
kgrunfeld@golomblegal.com
kfay@golomblegal.com

Attorneys for Plaintiff and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF CONTRA COSTA

STAR JOSHUA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

THE COUNTY OF CONTRA COSTA; MARC SHORR, in his official capacity; and DOES 1 through 100, inclusive,

Defendants.

Case No. C23-01684

[Case Assigned for All Purposes to: Dept. 12, Hon. Charles S. Treat]

FIRST AMENDED CLASS ACTION COMPLAINT FOR DAMAGES; INJUNCTIVE AND EQUITABLE RELIEF

DEMAND FOR JURY TRIAL

Plaintiff STAR JOSHUA ("Plaintiff") brings this First Amended Class Action Complaint against The County of Contra Costa, Marc Shorr, and the DOE Defendants (collectively "Defendants," individually, the "County," "Defendant Shorr," and "DOE Defendants" respectively), in her individual capacity and on behalf of all others similarly situated. In the event Defendants fail to rectify the problems associated with the actions detailed below pursuant to the California Government Tort Claims Act, Cal. Gov't Code §§ 810 – 996.6 (the "GTCA"), Plaintiff will amend this Complaint to seek restitution and all damages available under each respective cause of action alleged herein. Plaintiff hereby makes the following allegations upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard her and Class Members' Personally Identifiable Information ("PII") that Defendants required Plaintiff and Class Members to provide, including without limitation: first and last names, Social Security numbers, driver's license numbers, and government issued identification numbers.

2. Defendant County is a county located in the state of California and is home to more than one million residents.[1] Defendant County was one of the original 27 counties established in California in 1850 and is comprised of 19 cities, and many established communities in the unincorporated area.[2] It is also the ninth most populous county in the state.[3]

3. Defendant Marc Shorr is an employee of the County and is employed as the County's Chief Information Officer.[4] Upon information and belief, Defendant Shorr was employed before and during the time in which the Data Breach occurred. Furthermore, upon information and belief, in his official capacity as the Chief Information Officer, Defendant Shorr is responsible for maintaining, operating, and testing the County's data protection and cybersecurity protocols, systems, and practices. Defendant Shorr is also

[1] *See* https://www.contracosta.ca.gov/31/Our-County (last visited July 7, 2023).
[2] *Id.*
[3] *Id.*
[4] *See* https://www.contracosta.ca.gov/Directory/Home/DepartmentListing?DID=6 (last visited August 14, 2023.)

responsible for ensuring that the County's data protection and cyber security measures comply with industry standards and practices.

4. DOE Defendants 1 through 20 are agencies or entities responsible for the unlawful practices and policies alleged herein. DOES 21 through 100 are present or former employees of the County responsible for the unlawful practices and policies alleged herein. The DOE Defendants also includes the County employees whose email accounts and attachments were accessed by an unauthorized third party between September 19, 2022 and September 20, 2022 as described in further detail below.

5. Between September 19, 2022, and September 20, 2022, the County suffered a cybersecurity incident when an unauthorized party accessed two email accounts and attachments in those two accounts (the "Data Breach"). Based on the County's investigation, and as a result of the Data Breach, the County determined that Plaintiff, and an unknown number of Class Members, had their most sensitive personal information accessed and exfiltrated by cybercriminals thereby causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. According to the County, the PII compromised and accessed by the unauthorized party in the Data Breach include an affected individual's name, Social Security number, driver's license number, and government issued identification numbers. (the PII at issue is "Private Information").

7. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. Defendants failed to adequately protect Plaintiff's and Class Members' Private Information and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and the utter failure to protect sensitive data. An unauthorized party obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risk to these individuals will remain for their respective lifetimes.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

10. Defendants maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition. Defendants did not even take basic precautions by encrypting the Private Information.

11. Furthermore, Defendants are uniquely aware of the risks posed by potential cyberattacks because Defendants have already suffered two separate cyberattacks in or around the fall of 2019[5] and another in or around June 2021 through August 2021.[6] Indeed, the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant given Defendant's significant history of known cyber vulnerability and data breaches.[7][8] Indeed, the 2019 data breach incident should have and did provide the Defendants with notice of glaring weaknesses in their systems. Plaintiff was also a victim of this 2019 data breach and received notice of that breach.

---

[5] *See* https://www.cc-courts.org/civil/docs/grandjury/2020-2021/2104/2104-CyberAttackPreparedness Report.pdf (last visited July 7, 2023).

[6] *See* https://www.contracosta.ca.gov/DocumentCenter/View/74911/County-Notice-of-Privacy-Cyber-Incident -News-Release-4152022 (last visited July 7, 2023).

[7] *See* https://www.cc-courts.org/civil/docs/grandjury/2020-2021/2104/2104-CyberAttackPreparedness Report.pdf at p. 1 (last visited August 29, 2023).

[8] Additional reports of potential data exposure maintained by Contra Costa County and controlled by Mr. Shorr exist as well. See, i.e. https://www.mercurynews.com/2022/04/19/hacked-contra-costa-county-emails-could-have-contained-residents-personal-information/ (last visited August 29, 2023); https://www.kron4.com/news/bay-area/patients-embarrassing-private-health-information-posted-to-facebook-after-contra-costa-county-medical-privacy-breach/ (last visited August 29, 2023).

12. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained was accessed and exfiltrated by data thieves.

13. Armed with the Private Information accessed in the Data Breach, cyberthieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now, and in the future, closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out of pocket costs; for example, purchasing credit monitoring services, identity theft insurance, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

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

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

19. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

20. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring and identity theft protection services funded by Defendants for Class Members' respective lifetimes.

II. PARTIES

Plaintiff Star Joshua

21. Plaintiff Star Joshua formerly resided in Contra Costa County and is currently a resident and citizen of Stockton, California. Plaintiff Joshua received a letter from the County dated May 10, 2023, on or about that date.

///

///

22. The letter notified Plaintiff Joshua that "between September 19, 2022, and September 20, 2022" an "unauthorized party accessed two email accounts."[9]

23. The letter from the County further informed Plaintiff that her "name, Social Security number, driver's license number, and/or government issued identification number" were compromised, accessed, and exfiltrated by unauthorized third parties in the Data Breach.[10] This is the second time that Contra Costa County informed the Plaintiff that her data had been breached.

24. Upon information and belief, Defendants continue to maintain copies of Plaintiff Joshua's Private Information.

25. Plaintiff Joshua worked for Contra Costa County from approximately 2019 through 2021. She was required to provide her PII when she applied for employment with the County. She and her family have also received medical care from various clinics and facilities operated by the Contra Costa County.

26. Plaintiff Joshua typically takes measures to protect her Private Information and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

27. Plaintiff Joshua stores any documents containing her Private Information in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

28. Following, and as a result of, the Data Breach, Plaintiff Joshua has experienced a substantial increase in suspicious scam phone calls and emails, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

29. As a result of the Data Breach, and at the direction of the County's Notice Letter, Plaintiff Joshua made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and enrolling in the credit monitoring and identity

[9] *See* Notice of Data Breach dated May 10, 2023, attached hereto as "Exhibit A."

[10] *Id.*

theft protection services offered by the County through Experian; and freezing her credit. Plaintiff Joshua has spent at least five hours dealing with the Data Breach and continues to spend time dealing with it; valuable time Plaintiff Joshua otherwise would have spent on other activities, including but not limited to work and/or recreation.

30. Plaintiff Joshua suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Joshua; (b) violation of her privacy rights; (c) increased anxiety; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

31. As a result of the Data Breach, Plaintiff Joshua anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Joshua is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

32. Plaintiff Joshua is very concerned about her PII being accessed and exfiltrated by cybercriminals.

33. If Plaintiff Joshua had known that Defendants would not adequately protect her Private Information, she would not have allowed Defendants access to this sensitive and private information.

Defendant County of Contra Costa

34. Defendant County of Contra Costa is a county located in California. The County Administrator's Office is located at 1025 Escobar Street Martinez, CA 94553.

Defendant Marc Shorr

35. Defendant Marc Shorr is an employee of the County and is employed as the County's Chief Information Officer.[11] Upon information and belief, Defendant Shorr was employed before and during the time in which the Data Breach occurred. Furthermore, upon information and belief, Defendant Shorr, in

[11] *See* https://www.contracosta.ca.gov/Directory/Home/DepartmentListing?DID=6 (last visited August 14, 2023.)

his official capacity as the Chief Information Officer, is responsible for maintaining, operating, and testing the County's data protection and cybersecurity protocols, systems, and practices. Defendant Shorr is also responsible for ensuring that the County's data protection and cyber security measures comply with industry standards and practices. Defendant Shorr was employed by the County before and during the time in which the Data Breach occurred.

DOE Defendants

36. Plaintiff is ignorant of the true names and capacities of Defendants sued herein as DOES 1 through 100, inclusive, and therefore sues these Defendants by such fictitious names. DOES 1 through 20 are agencies or entities responsible for the unlawful practices and policies alleged herein. DOES 21 through 100 are present or former employees of the County responsible for the unlawful practices and policies alleged herein. The DOE Defendants also includes the County employees whose email accounts and attachments were accessed by an unauthorized third party thereby causing the Data Breach. DOE Defendants were employed by the County before and during the time in which the Data Breach occurred.

37. Plaintiff will seek leave to amend this complaint to allege their true names and capacities when ascertained.

III. JURISDICTION AND VENUE

38. This Court has jurisdiction over this action under Code of Civil Procedure § 410.10. The total amount of damages incurred by Plaintiff and the Class in the aggregate exceeds the $25,000 jurisdictional minimum of this Court. Further, upon information and belief, the amount in controversy as to Plaintiff individually does not exceed $75,000.

39. This action does not qualify for federal jurisdiction under the Class Action Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies to this action because (1) more than two-thirds of the members of the proposed Class are citizens of the State of California, (2) Defendant County is a citizen of the State of California, given that it is headquartered in California, (3) Defendant Marc Shorr is a citizen of, and resides in, the State of California, and (4) on information and belief, the DOE Defendants are citizens of, and reside in, the State of California.

40. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because the County, and/or its parents or affiliates, are headquartered in this judicial district, Defendant Shorr is a resident of this judicial district, the DOE Defendants are residents of this judicial district, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this judicial district.

IV. FACTUAL ALLEGATIONS

Defendants' Business

41. The County of Contra Costa is a county located in California that:

> [I]s home to more than one million residents, and was one of the original 27 counties established in California in 1850. Comprised of 19 cities and many established communities in the unincorporated area, it is the ninth most populous county in the state.

42. Defendant Marc Shorr is employed as the County's Chief Information Officer and is responsible for maintaining, operating, and testing Defendant County's data protection and cybersecurity protocols, systems, and practices. Defendant Shorr is also responsible for ensuring that the County's data protection and cyber security measures comply with industry standards and practices.

43. DOE Defendants are employed by the County and are responsible for ensuring that the PII collected by them as part of their employment is kept safe, confidential, and that the privacy of this sensitive information is maintained.

44. On information and belief, Defendants made promises and representations to Plaintiff and Class Members that the PII collected as part of County's operations would be kept safe, confidential, and that the privacy of that information would be maintained.

45. Plaintiff and Class Members, individuals whose PII was in the possession of the Defendants, including current and former employees, relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

46. On information and belief, in the ordinary course of business as a condition of service or within the scope of employment, Defendants required individuals to provide copious amounts of sensitive personal and private information as a condition of receiving services or employment including but not limited to the Private Information compromised in the Data Breach.

47. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties, and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

48. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

50. Plaintiff and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

51. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

The Cyberattack and Data Breach

52. According the Notice, "between September 19, 2022 and September 20, 2022" an "unauthorized party accessed [] two [County Email] accounts" as well as the "attachments in [the] two County email accounts."[12] The County determined after its investigation that "the likely purpose of the unauthorized access was to perpetrate an email phishing scheme" but that it "cannot rule out the possibility

[12] *See* Exhibit A.

that emails and attachments in the email accounts may have been viewed or accessed as a result of this incident."[13]

53. The language in the notices to Class Members is unequivocal: the Data Breach resulted in an "unauthorized party" "viewing" or "accessing" the Private information that included PII, including, among many other things, each Class Members' "name, Social Security number, driver's license number, and/or government issued identification number."[14]

54. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been shared with Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

55. Unauthorized individuals can now easily access the PII of Plaintiff and Class Members.

56. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

Defendants Failed to Comply With Industry Standards

57. Several best practices have been identified that at minimum should be implemented by public entities like the County, including, but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

58. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

---

[13] *Id.*

[14] *Id.*

59. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC).

60. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[15]

61. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

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

[15] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 7, 2023).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

62. To prevent and detect cyber-attacks Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….

- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic[16]….

63. To prevent and detect cyber-attacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

-Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

-Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection

[16] *See* Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 7, 2023).

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[17]

64. Given that Defendants were storing the PII of Plaintiff and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

65. These foregoing frameworks are existing and applicable industry standards for reasonable cybersecurity readiness and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

66. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

Defendants Knew the Private Information on Its Network Was a Target

67. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

68. In fact, according to the cybersecurity firm Mimecast, in the year 2021 public agencies have experienced a 49% increase in phishing attacks, a 44% increase in internal threats or data leaks by careless or negligent employees, and a 44% increase in internal threats or data leaks by malicious insiders.[19]

---

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited July 7, 2023).

[18] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 7, 2023).

[19] *See* Tightening Cybersecurity at State and Local Governments (July 28, 2022), https://www.mimecast.com/blog/tightening-cybersecurity-at-state-and-local-governments/ (last visited July 7, 2023).

69. Defendants knew and understood unprotected or exposed PII in the custody of public agencies, such as the County, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

70. The increase in cyberattacks targeting public entities, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, and particularly to Defendants.

71. As a public entity, the County, and therefore Defendant Shorr, knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

72. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

V. DEFENDANTS' BREACH

73. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices; and;

f. Failing to adhere to industry standards for cybersecurity.

74. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems which contained unsecured and unencrypted Private Information.

75. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft.

A. Cyberattacks And Data Breaches Cause Disruption And Put Consumers At A Present And Substantially Increased Risk Of Fraud And Identity Theft

76. Cyberattacks and data breaches of public entities like the County are especially problematic because they can negatively impact the daily lives of individuals affected by the attack.

77. "Mental health professionals say data breaches and other cybercrimes are increasingly taking a heavy psychological toll on the millions of Americans whose personal information is plundered by fraudsters… 'Depending on who the attackers and the victims are, the psychological effects of cyber-attacks may even rival those of traditional terrorism,' says Dr. Maria Bada, research associate at the Cambridge Cybercrime Centre at the University of Cambridge."[20]

78. In addition to the psychological toll that data breaches and cybercrime takes from its victims, such issues also impose great financial costs to victims. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

79. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves

[20] *See* Anxiety, depression and PTSD: The hidden epidemic of data breaches and cyber crimes (February 24, 2020), https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/ (last visited July 7, 2023).

[21] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited July 7, 2023).

who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

80. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

81. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

82. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

///

///

[22] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited July 7, 2023).

83. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[23]

84. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

85. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used.

86. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

87. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

88. There is a strong probability that entire batches of information stolen from Defendants have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

89. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come. In fact, the County warned impacted individuals in the notices about

[23] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[24] *See* GAO Report, at p. 29.

the Data Breach to review all statements, monitor accounts and credit reports for suspicious activity, and to sign up for credit monitoring and identity theft protection.

90. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

91. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[26] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[27] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

92. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

93. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

---

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 7, 2023).

[26] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July, 2023).

[27] *Id.* at 4.

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions worrying-about-identity-theft (last visited July 7, 2023).

94. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

95. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[30] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[31]

96. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[32]

97. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2023).

[30] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited July 7, 2023).

[31] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited July 7, 2023).

[32] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed on July 7, 2023).

> your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

98. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[33] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[34]

99. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[35]

100. For this reason, Defendants knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach yet failed to properly prepare for that risk.

B. Plaintiff's and Class Members' Damages

101. To date, Defendants have done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

102. Plaintiff's and Class Members' Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendants' computer system and removed the Private Information. Upon information and belief, these cybercriminals have published Plaintiff's and Class Members' Private Information to the internet.

---

[33] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises -customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed on July 7, 2023).

[34] *Id.*

[35] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed on July 7, 2023).

103. Plaintiff's and Class Members' Private Information was compromised and accessed as a direct and proximate result of the Data Breach.

104. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

105. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

106. Plaintiff and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

107. Plaintiff and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

108. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

109. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

110. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

111. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

112. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected or at the very least encrypted.

113. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—have been disclosed to the world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

VI. CLASS ALLEGATIONS

114. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to the Code of Civil Procedure §382, for the following classes defined as:

> **All citizens of the state of California who were mailed a letter sent from the County of Contra Costa entitled "NOTICE OF DATA BREACH" on or about May 10, 2023 (the "Class").**

115. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

116. Plaintiff reserves the right under California Rules of Court, rule 3.765, to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

117. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. The Class is apparently identifiable within the County's records.

118. Commonality and Predominance: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether Defendants owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;
b. Whether Defendants breached that duty;
c. Whether Plaintiff's and the Class Members' Private Information was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;
d. When and how Defendants should have learned and actually learned of the Data Breach;
e. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
f. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
g. Whether Defendants' response to the Data Breach was adequate;

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

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

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether an implied contract existed between Defendants and Plaintiff and Class Members;

l. Whether Defendants breached its implied contract with Plaintiff and Class Members;

m. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

n. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

o. Whether Plaintiff and Class Members are entitled to equitable relief; and

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

119. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Class.

120. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and

Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class each as a whole, not on facts or law applicable only to Plaintiff.

121. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

122. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large public entity, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

123. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

125. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

126. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

FIRST CAUSE OF ACTION
NEGLIGENCE
GOVERNMENT CODE SECTIONS 815.2 & 820
(On Behalf of Plaintiff and the Class)

127. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

128. Plaintiff brings this Count on her own behalf and on behalf of the Class.

129. Under California Government Code § 815.2, Defendant County is liable for the negligent acts of each and every one of its employees acting within the scope of their employment, whether or not named in this complaint. This liability includes liability for those acting pursuant to policy or higher-level instruction even though the individual, or individuals, who acted so are not named in the complaint.

130. Additionally, under California Government Code § 820, each and every one of Defendant County's employees, whether or not named in this complaint, are liable for injuries caused by their acts or omissions to the same extent as a private person.

131. Upon information and belief, Defendant Marc Shorr ("Defendant Shorr") is an employee of the County and is employed as County's Chief Information Officer. Defendant Shorr was employed by the County before and during the time in which the Data Breach occurred. In his official capacity as the

Chief Information Officer, Defendant Shorr is responsible for maintaining, operating, and testing the County's data protection systems and cybersecurity policies, protocols, systems, and practices. Defendant Shorr is responsible for ensuring that the County's data protection and cyber security measures comply with industry standards and practices. Defendant Shorr is not immune from liability and Defendant Shorr's negligent conduct, while acting within the scope of his employment, would indeed give rise to a negligence cause of action against Defendant Shorr, as set forth herein.

132. Upon information and belief, DOE Defendants are present or former employees of the County responsible for the unlawful practices and policies alleged herein. DOE Defendants were employed by the County before and during the time in which the Data Breach occurred. In their capacity as employees of the County, DOE Defendants are responsible for ensuring that the PII collected by them as part of their employment is kept safe, confidential, and that the privacy of this sensitive information is maintained. DOE Defendants are not immune from liability and DOE Defendants' negligent conduct, while acting within the scope of their employment, would indeed give rise to a negligence cause of action against DOE Defendants, as set forth herein.

133. Defendant Shorr's and DOE Defendants' own negligent conduct while acting within the scope of their employment created a foreseeable risk of harm to Plaintiff and Class Members. Defendant Shorr's and DOE Defendants' negligent conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant Shorr and DOE Defendants knew or should have known that their conduct did not comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the Private Information of Plaintiff and Class Members.

134. Defendant Shorr and DOE Defendants had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, maintaining, operating, adhering to, and testing Defendant County's security protocols to ensure Private Information in Defendants' possession was adequately secured and protected, including encrypting Private Information

in motion, and at rest and requiring two party authentications to access to Private Information, and that any employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant Shorr and DOE Defendants also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Members' Private Information.

135. As a condition of receiving services or employment, Plaintiff and Class Members were obligated to provide Defendant County and thereby Defendant Shorr and DOE Defendants directly with their Private Information. As such, Plaintiff and the Class Members entrusted their Private Information to Defendant County and its employees with the understanding Defendant County and its employees would safeguard their information.

136. Defendant Shorr and DOE Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach. However, Plaintiff and Class Members had no ability to protect their Private Information in Defendant County's, Defendant Shorr's, or DOE Defendants' possession.

137. Defendant Shorr and DOE Defendants had full knowledge of the sensitivity of the Private Information, and the types of harm Plaintiff and Class Members could, would, and will suffer if the Private Information were wrongfully disclosed.

138. Defendants admitted that certain systems containing Plaintiff's and Class Members' Private Information were wrongfully compromised and accessed by unauthorized third persons, and that the Data Breach occurred due to Defendants' actions and omissions, including Defendant Shorr's failure to encrypt Private Information in motion and at rest, and requiring two-party authentication to access to Private Information; and DOE Defendants failure to ensure that the PII collected by them as part of their employment was kept safe, confidential, and that the privacy of this sensitive information was maintained.

139. Plaintiff and Class Members were the foreseeable and probable victims of Defendant Shorr's and DOE Defendants' negligent and inadequate security practices and procedures that led to the Data Breach. Defendant Shorr and DOE Defendants knew or should have known of the inherent risks in collecting and storing the highly valuable Private Information of Plaintiff and Class Members, the critical

importance of providing adequate security of that Private Information, the current cyber security risks being perpetrated, and that Defendant Shorr and DOE Defendants had inadequate employee training, monitoring and education and IT security protocols in place to secure the Private Information of Plaintiff and Class Members.

140. Defendant Shorr and DOE Defendants negligently, through their actions and/or omissions, and unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information while the data was within Defendant Shorr's and DOE Defendants' possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach, including Defendant Shorr's failure to encrypt Private Information in motion and at rest, and requiring two-party authentication to access Private Information; and DOE Defendants' failure to ensure that the PII collected by them as part of their employment was kept safe, confidential, and that the privacy of this sensitive information was maintained.

141. Defendant Shorr and DOE Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiff's and Class Members' Private Information.

142. Defendant Shorr and DOE Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

143. But for Defendant Shorr's and DOE Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' Private Information would not have been compromised.

144. There is a temporal and close causal connection between Defendant Shorr's and DOE Defendants' failure to implement security measures to protect the Private Information and the harm suffered, and/or risk of imminent harm suffered, by Plaintiff and Class Members.

145. Defendant Shorr's and DOE Defendants' negligence caused Plaintiff and Class Members to lose control over their Private Information, which subjected each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft, in addition to the time and expenses spent mitigating those injuries and preventing further injury. Plaintiff's and Class Members' Private Information remains in Defendant County's, Defendant Shorr's, and DOE Defendants' possession and is subject to further unauthorized disclosures so long as Defendant Shorr and DOE Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

146. As a direct and proximate result of Defendant Shorr's and DOE Defendants' negligence, Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months— if not years— to discover, detect, and remedy.

147. Additionally, as a direct and proximate result of Defendant Shorr's and DOE Defendants' negligence, Plaintiff and Class Members have suffered diminished value of their Private Information. Plaintiff and Class Members would pay at least as much to properly secure their Private Information as cyber criminals would pay to access their Private Information. As a result of Defendant Shorr's and DOE Defendants' negligence, Plaintiff's, and Class Members' ability to use their own Private Information for activities like establishing credit and obtaining medical services is diminished.

148. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendants to institute appropriate data collection and safeguarding methods and policies regarding customer information.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
At Common Law
(On Behalf of Plaintiff and the Class)

149. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

150. Plaintiff brings this Count on her own behalf and on behalf of the Class.

151. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

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

153. Defendants owed a duty to their current and former employees and applicants, including Plaintiff and the Class, to keep their Private Information contained as a part thereof, confidential.

154. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

155. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendants' failure to protect the PII.

156. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Class is highly offensive to a reasonable person.

157. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their Private Information to Defendants privately with the intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

159. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

160. Because Defendants acted with this knowing state of mind, it had noticed and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

161. As a proximate result of the above acts and omissions of Defendants, the Private Information of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

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

163. Plaintiff seeks injunctive relief on behalf of the Class and as indicated above, will seek leave to amend this Complaint to seek restitution and all other damages available under this cause of action.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
Cal. Const. ART. 1 § 1
(On Behalf of Plaintiff and the Class)

164. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

165. Plaintiff brings this Count on her own behalf and on behalf of the Class.

166. California established the right to privacy in Article I, Section 1 of the California Constitution.

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

168. Defendants owed a duty to their current and former employees, including Plaintiff and the Class, to keep their Private Information contained as a part thereof, confidential.

169. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

170. Defendants allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the Class, by way of Defendants' failure to protect the PII.

171. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Class is highly offensive to a reasonable person.

172. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their Private Information to Defendants, but privately with the intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

174. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

175. Because Defendants acted with a knowing state of mind, they had noticed that the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

176. As a proximate result of the above acts and omissions of Defendants, the Private Information of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

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

178. Plaintiff seeks injunctive relief on behalf of the Class and as indicated above, will seek leave to amend this Complaint to seek restitution and all other damages available under this cause of action.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

180. Plaintiff brings this Count on her own behalf and on behalf of the Class.

181. Plaintiff and the Class delivered their Private Information to Defendants.

182. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendants an implied covenant of good faith and fair dealing by which Defendants were required to perform its obligations and manage Plaintiff's and Class Member's data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendants.

///

///

183. In providing their Private Information, Plaintiff and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

184. In delivering their Private Information to Defendants, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard that data.

185. Plaintiff and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

186. Defendants accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing medical services to Plaintiff and Class Members.

187. Had Defendants disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure Private Information, Plaintiff and members of the Class would not have provided their Private Information to Defendants.

188. Defendants recognized that the Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

189. Plaintiff and the Class fully performed their obligations under the implied contract with Defendants.

190. Defendants breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

191. Defendants breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and acquisition of their Private Information.

192. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs

associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed classes entrusted Defendants with their Private Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Private Information, which remains in the Defendants' possession with in-adequate measures to protect Plaintiff's and Class Members' Private Information.

193. Plaintiff seeks injunctive relief on behalf of the Class and as indicated above, will seek leave to amend this Complaint to seek restitution and all other damages available under this cause of action.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

195. Plaintiff brings this Count on her own behalf and on behalf of the Class.

196. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members provided to Defendants.

197. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

198. Plaintiff and Class Members provided their respective Private Information to Defendants with the explicit and implicit understanding that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized parties.

///

199. Plaintiff and Class Members also provided their Private Information to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including Defendants' employees' email accounts.

200. Defendants required and voluntarily received, in confidence, Plaintiff and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

201. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, following best information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

202. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered, and will continue to suffer damages.

203. But for Defendants' disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, Plaintiff's and Class Members' Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

204. The injury and harm Plaintiff and Class Members suffered, and continue to suffer, was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendants knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' Private Information had numerous security and other vulnerabilities placing Plaintiff's and Class Members' Private Information in jeopardy.

205. As a direct and proximate result of the breach of confidence, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class

Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed classes entrusted Defendants with their Private Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Private Information, which remains in the Defendants' possession with in-adequate measures to protect Plaintiff's and Class Members' Private Information.

206. Plaintiff seeks injunctive relief on behalf of the Class and as indicated above, will seek leave to amend this Complaint to seek restitution and all other damages available under this cause of action.

SIXTH CAUSE OF ACTION
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

207. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

208. Plaintiff brings this Count on her own behalf and on behalf of the Class.

209. Defendants' acts and omissions as alleged herein emanated and directed from California.

210. By reason of the conduct alleged herein, Defendants engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

211. Defendants stored the Private Information of Plaintiff and Class Members in their computer systems.

212. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that Private Information.

213. Defendants did not disclose at any time that Plaintiff's and Class Members' Private Information was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only ones in possession of that material information, which Defendants had a duty to disclose.

Unlawful Business Practices

214. As noted above, Defendants violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and California Subclass Members' Private Information.

215. Defendants also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

216. If Defendants had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendants' failure to timely notify Plaintiff and Class Members of the Data Breach.

217. Defendants' acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

218. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiff's and Class Members' Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

219. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and failure to disclose inadequacies of Defendants' data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

220. Defendants engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

221. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harm. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' Private Information to third parties without their consent, diminution in value of their Private Information, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class Members' PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those

that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

222. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. Plaintiff's and Class Members' Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

223. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs. However, at this time the Plaintiff seeks injunctive relief on behalf of the Class and as indicated above, will seek leave to amend this Complaint to seek restitution and all other damages available under this cause of action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the members of the Class, requests judgment against Defendants and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and the members of the Class, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and the members of the Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the members of the Class, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and the members of the Class unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the members of the Class;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and the members of the Class;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and the members of the Class on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all members of the Classes about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation

on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. Ordering Defendants to pay for a lifetime of credit monitoring services for Plaintiff and the Class;

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

F. For prejudgment and/or post-judgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

DATED: August 30, 2023

Respectfully Submitted,

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION

By: */s/ M. Anderson Berry*
M. Anderson Berry, Esq.
Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

May 10, 2023

47 1 14468 ——————AUTO**ALL FOR AADC 956
STAR JOSHUA
[redacted]

NOTICE OF DATA BREACH

Dear Star Joshua,

The County of Contra Costa, California is committed to protecting the confidentiality of the information we maintain. We are writing to inform you of a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken since, and steps you may take in response.

What Happened: The County of Contra Costa recently concluded its investigation of and data analysis for an email phishing incident that may have resulted in unauthorized access to emails and attachments in two County email accounts. Upon learning of the incident, we secured the accounts and launched an investigation. Our investigation determined that an unauthorized party accessed the two email accounts between September 19, 2022 and September 20, 2022. Based on our investigation, the likely purpose of the unauthorized access was to perpetrate an email phishing scheme, not to access personal information. That said, we cannot rule out the possibility that emails and attachments in the email accounts may have been viewed or accessed as a result of this incident.

What Information Was Involved: In order to determine if any emails or attachments contained personal information, we reviewed, both programmatically and manually, the information contained in the emails that may have been involved in the incident. Based on this review, we determined that emails and attachments that may have been subject to unauthorized access contain some of your information, including some or all of the following: your name, Social Security number, driver's license number, and/or government issued identification number.

What We Are Doing: To help prevent a similar incident from occurring in the future, we have implemented enhanced monitoring and alerting software and technical safeguards. In addition, as a precaution, we are offering you a complimentary 12 month membership of Experian's® IdentityWorks℠. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score.

What You Can Do: To date, we have not received any reports of fraud related to this incident. However, out of an abundance of caution, we wanted to let you know this happened and assure you that we take this very seriously. **For more information on IdentityWorks, including instructions on how to activate your complimentary membership and additional steps you can take in response to the incident, please see the pages that follow this letter.**

For More Information: We deeply regret any inconvenience or concern this may cause. If you have any questions about this incident, please call (866) 347-9948, Monday through Friday, between 6:00 a.m. and 3:30 p.m. Pacific Time, excluding major U.S. holidays.

Sincerely,

Karen Caoile

Karen Caoile
Director of Risk Management
Risk Management Department
Contra Costa County

ELN-17845-1