John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
FOR THE COUNTY OF SACRAMENTO

Konnor Robison-Williams, individually and on behalf of all others similarly situated, Plaintiff, v. Visionary Integration Professionals, LLC., Defendant.	Case No. 24CV012543 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Konnor Robison-Williams ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Visionary Integration Professionals, LLC. ("Defendant" or "VIP") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a company that offers various business solutions to its clients, including "public sector

agencies and Fortune 500 organizations[.]"[1]

2. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including Plaintiff's and Class Members' names, dates of birth, driver's licenses or state identification numbers, and Social Security numbers, (collectively defined herein as "PII").

3. Upon information and belief, current and former VIP employees are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain employment or certain employment benefits at Defendant. Defendant retains this information for at least many years and even after the employee-employer relationship has ended.

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

5. Defendant's investigation concluded that the PII compromised in the Data Breach included Plaintiff's and approximately 3,000 other individuals' information.[2]

6. Defendant failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect employees' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class

[1] https://trustvip.com/about-us/

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/31f1dd27-1f56-4bf8-9b2b-0fbde408fbb1.shtml

Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

7. In breaching its duties to properly safeguard employees' PII and give employees timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

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

9. Defendant 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 PII 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 PII 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 they should be entitled to injunctive and other equitable relief.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Norton; (ix) Plaintiff experiencing fraudulent charges to his Capital One credit card, for approximately $458, in or about June 2024; (x) nominal damages; and (xi) 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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

11. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

12. Plaintiff Konnor Robison-Williams is a natural resident and citizen of Sacramento, California.

13. Defendant is a limited liability company organized under the state laws of Delaware with its principal place of business located in Folsom, California.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action under California 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.

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

FACTUAL ALLEGATIONS

Background of Defendant.

16. Defendant is a company that offers various business solutions to its clients, including "public sector agencies and Fortune 500 organizations[.]"[3]

17. Plaintiff and Class Members are current and former employees of Defendant.

18. In order to apply to be an employee or obtain certain employment-related benefits at Defendant, Plaintiff and Class Members were required to provide sensitive and confidential PII, including their names, dates of birth, driver's licenses or state identification numbers, and Social Security numbers.

19. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

20. Upon information and belief, Defendant made promises and representations to its employees, including Plaintiff and Class Members, that the PII collected from them as a condition of their employment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

21. Indeed, Defendant provides on its website that: "[w]e have appropriate security measures in place at our physical facilities to protect against the loss, misuse or alteration of

[3] https://trustvip.com/about-us/

information that we have collected from you at our website. VIP will assess our security measures to ensure compliance and suitability as necessary."[4]

22. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

24. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its employees' PII safe and confidential.

25. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

26. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

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

[4] https://trustvip.com/privacy-policy/

The Data Breach.

28. On or about April 15, 2024, Defendant began sending Plaintiff and other victims of the Data Breach a Notice of Data Breach letter (the "Notice Letter"), informing them that:

> **What Happened?**
>
> On September 21, 2023, Visionary Integration Professionals (VIP) received a notification regarding access to select VIP servers by an unauthorized third party. VIP took immediate action to mitigate the incident, including restoring all systems and data using backups and engaging a forensic investigation team to investigate and resolve the incident. As a result of this investigation, recently, VIP learned that personal information may have been accessed.
>
> **What Information Was Involved?**
>
> Based on this investigation, VIP believes the purpose of the unauthorized access was to obtain a payment for potentially copying data from one location to another. No contact was initiated with the bad actors and the systems were all restored. VIP is not aware of any actual misuse of personal information related to this incident. VIP has identified the following information relating to you that may have been accessed by the attacker: Social Security Number, Date of Birth and Driver's License or State Identification Number.[5]

29. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the date(s) of the Data Breach, 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. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

30. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without

[5] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/31f1dd27-1f56-4bf8-9b2b-0fbde408fbb1.shtml

these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

31. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Social Security numbers for download and theft.

32. In the context of notice of data breach letters of this type, Defendant's use of the phrase "may have accessed" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiff and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiff's and Class Members' names, dates of birth, Social Security numbers, and other sensitive information were accessed or acquired by an unknown actor – aka cybercriminals.

33. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the approximate 3,000 Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

34. Defendant 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.

35. The attacker targeted, accessed, and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiff and Class Members, including their names, dates of birth, and Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

36. Plaintiff has been informed by Norton that his PII has been disseminated on the dark web, and Plaintiff further believes the PII of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable.

37. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

38. 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."[6]

39. To prevent and detect cyber-attacks, Defendant 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.

[6] 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

- 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.

- 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.[7]

[7] *Id.* at 3-4.

40. To prevent and detect cyber-attacks or ransomware attacks, Defendant 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
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[8]

[8] *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 Nov. 11, 2021).

41. Given that Defendant were storing the sensitive PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

42. The occurrence of the Data Breach indicates that Defendant 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 approximately 3,000 employees, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores its Employees' PII

43. As a condition of employment with Defendant, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

44. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

Defendant Knew or Should Have Known of the Risk Because Employers in Possession of PII are Particularly Susceptible to Cyber Attacks.

48. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

49. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

50. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).[9] The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).[10]

51. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

52. Additionally, as companies became more dependent on computer systems to run their business,[11] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of

[9] https://www.idtheftcenter.org/publication/2023-data-breach-report/

[10] *Id.*

[11] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[12]

53. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

55. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

56. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to more than three thousand individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient

[12] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

58. Defendant's offering of credit and identity monitoring establishes that Plaintiff and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

59. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

60. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

61. As an employer in possession of its employees' and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the 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. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information.

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or

[13] 17 C.F.R. § 248.201 (2013).

in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

63. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[15] For example, Personal Information can be sold at a price ranging from $40 to $200.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

64. Moreover, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

65. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [18] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[19]

---

[14] *Id.*

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

[18] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[19] *Id.*

66. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

67. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[21] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[22]

68. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

[21] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/

[22] *See* https://www.investopedia.com/terms/s/ssn.asp

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."[23]

70. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

71. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a

[23] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[24]

72. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[25]

73. 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."[26]

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

75. 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."[27] However, this is not the case. As cybersecurity experts point out:

---

[24] *See* https://oag.ca.gov/idtheft/facts/your-ssn

[25] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).

[26] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

[27] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).

> "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."[28]

76. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[29]

77. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

78. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[30]

79. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

80. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[28] *Id.*

[29] *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 visited on Feb. 21, 2023).

[30] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

> [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.[31]

81. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendant Fails to Comply with FTC Guidelines.

82. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[32]

84. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

---

[31] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

[32] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[33]

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

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

87. These FTC enforcement actions include actions against employers, like Defendant.

88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

89. Defendant failed to properly implement basic data security practices.

[33] *Id.*

90. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

91. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its employees, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with Industry Standards.

92. As noted above, experts studying cyber security routinely identify employers in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

93. Several best practices have been identified that, at a minimum, should be implemented by employers in possession of PII, like Defendant, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

94. Other best cybersecurity practices that are standard for employers 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

95. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. These foregoing frameworks are existing and applicable industry standards for employers safeguarding their employees' data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages.

97. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) 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) remains backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk of Identity Theft.

98. As Plaintiff has already experienced, the unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

99. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

100. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

101. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

102. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[34]

[34] *See* N.C. Gen. Stat. § 132-1.10(1).

103. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[35]

104. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[36] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[37]

105. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[38]

---

[35] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers

[36] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/

[37] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[38] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-

106. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

107. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

108. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

109. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

110. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud.

111. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud.

texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

112. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiff and Class Members to take the following measures to protect themselves: "remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports."[39]

113. In addition, Defendant's Notice letter includes two pages devoted to "Additional Resources" that recommend Plaintiff and Class Members to partake in activities such as placing freezes on their accounts, placing fraud alerts on their accounts, and contacting consumer reporting bureaus.[40]

114. Defendant's extensive suggestion of steps that Plaintiff and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiff and Class Members must undertake in response to the Data Breach. Plaintiff's and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

115. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, replacing impacted credit cards, contacting financial institutions to dispute fraudulent charges on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiff and

[39] Notice Letter.

[40] *Id.*

Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

116. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that 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."[41]

117. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach 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 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.[42]

118. And for those Class Members who experience actual identity theft and fraud, 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."[4]

Diminution of Value of PII.

119. PII is a valuable property right.[43] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

[41] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[42] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[43] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

120. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[44]

121. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[45] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[46,47] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[48]

122. As a result of the Data Breach, Plaintiff's and Class Members' PII , which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

123. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable

---

[44] *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).

[45] *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 Sep. 13, 2022).

[46] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[47] https://datacoup.com/

[48] https://digi.me/what-is-digime/

consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

124. The fraudulent activity resulting from the Data Breach may not come to light for years.

125. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

126. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than three thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

127. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary.

128. Given the type of targeted attack, the sophisticated criminal activity, the type of PII involved in this case, and Plaintiff's PII already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

129. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII 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.

130. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

131. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain.

132. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain employment at Defendant under certain terms, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received employment positions of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Robison-Williams's Experience.

133. Plaintiff Robison-Williams is a former employee at VIP who left VIP in or about 2023.

134. As a condition of his employment at VIP, he was required to supply Defendant with his PII, including but not limited to his name, date of birth, driver's license or state identification number, and Social Security number.

135. Plaintiff Robison-Williams is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

136. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

137. Plaintiff Robison-Williams received the Notice Letter, by U.S. mail, directly from Defendant, dated April 15, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his full name, date of birth, driver's license or state identification number, and Social Security number.

138. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports[,]"[49] Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, replacing impacted credit cards, contacting financial institutions to dispute fraudulent charges on his accounts, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff have spent significant on mitigation activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

139. Subsequent to the Data Breach, Plaintiff Robison-Williams has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft

[49] Notice Letter.

of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

140. Plaintiff additionally suffered actual injury in the form of experiencing fraudulent charges to his Capital One credit card, for approximately $458, in or about June 2024, which, upon information and belief, was caused by the Data Breach.

141. Plaintiff further suffered actual injury in the form of his PII being disseminated on the dark web, according to Norton, which, upon information and belief, was caused by the Data Breach.

142. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

143. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

144. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

145. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

146. Plaintiff Robison-Williams has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

147. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to California's Class Action Mechanism (Cal. Civ., § 382).

148. The Classes that Plaintiff seeks to represent is defined as follows:

Nationwide Class
All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "Class").

California Subclass
All individuals residing in the State of California whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "California Subclass").

149. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant 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.

150. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

151. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 3,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney General's Office.[50] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

152. 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 and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

[50] https://apps.web.maine.gov/online/aeviewer/ME/40/31f1dd27-1f56-4bf8-9b2b-0fbde408fbb1.shtml

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant 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 Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

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

k. 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.

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

154. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant 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. Defendant's policies challenged herein apply to and affect Class Members

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

155. 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 he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

156. Superiority and Manageability. The 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 large corporations, like Defendant. 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.

157. 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 Defendant 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.

158. The litigation of the claims brought herein is manageable. Defendant's 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.

159. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

160. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

161. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

162. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard its employees' PII; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

163. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

164. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

165. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its employees, which solicitations and services affect commerce.

166. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

167. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

168. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

169. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

170. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

171. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment at Defendant.

172. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

173. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

174. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

175. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

176. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

177. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations, and;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

178. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

179. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

180. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

181. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

182. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

183. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employers in possession of PII.

184. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

185. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

186. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

187. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

188. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

189. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

190. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

191. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

192. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

193. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Norton; (ix) Plaintiff experiencing fraudulent charges to his Capital One credit card, for approximately $458, in or about June 2024; (x) nominal damages; and (xi) 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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

194. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

195. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

196. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

197. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

199. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

200. Plaintiff and Class Members were required deliver their PII to Defendant as part of the process of obtaining employment at Defendant. Plaintiff and Class Members provided their labor and PII to Defendant with the assumption that a portion of its earnings would be used to adequately safeguard their PII.

201. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

202. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of performing its regular business operations.

203. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

204. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

205. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

206. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

207. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

208. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

209. Plaintiff and Class Members provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

210. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

211. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

212. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

213. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

214. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of

Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

215. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

216. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Norton; (ix) Plaintiff experiencing fraudulent charges to his Capital One credit card, for approximately $458, in or about June 2024; (x) nominal damages; and (xi) 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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

217. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

218. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

219. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

220. This Count is pleaded in the alternative to the breach of implied contract (Count II).

221. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their labor to Defendant and/or its agents and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the employment positions that were the subject of the transactions and should have had their PII protected with adequate data security.

222. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

223. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

224. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

225. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained employment at Defendant.

226. Plaintiff and Class Members have no adequate remedy at law.

227. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

228. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

229. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Norton; (ix) Plaintiff experiencing fraudulent charges to his Capital One credit card, for approximately $458, in or about June 2024; (x) nominal damages; and (xi) 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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

230. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

231. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and All Class Members)

232. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

233. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

234. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

235. Defendant's "unfair" acts and practices include:

a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information.

236. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

237. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

238. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

239. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

240. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

241. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

242. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and Class Members.

243. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

244. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT V
Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

245. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count).

246. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

247. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

248. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

249. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

250. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable

security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

251. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

252. As a direct and proximate result of Defendant's acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

253. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

254. On June 21, 2024, Plaintiff's counsel sent a CCPA notice letter to Defendant's registered service agents via certified mail. If Defendant does not cure the effects of the Data Breach, which would require retrieving the PII and securing the PII from continuing and future use, within 30 days of delivery of such CCPA notice letter (which Plaintiff believes any such cure is not possible under these facts and circumstances), Plaintiff shall seek actual damages and

statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

255. Accordingly, Plaintiff and the Class Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT VI
Violation of the California Customer Records Act,
Cal. Civ. Code § 1798.80 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

256. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count).

257. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

258. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

259. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

260. Plaintiff and the Class Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining employment services from Defendant.

261. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

262. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the Class Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's

violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

263. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the Class Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the Class Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

264. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the Class Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the Class Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

265. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

266. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

267. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the Class. On information and belief, to date, Defendant has not sent

written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all Class Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

268. On information and belief, many Class Members affected by the breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

269. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

270. As a direct consequence of the actions as identified above, Plaintiff and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

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

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

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 Class Members, including but not limited to an order:

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

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of

Plaintiff and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, 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 Defendant 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 Defendant's policies, programs, and systems for protecting personal identifying information;

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

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's 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

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

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

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

Dated: June 24, 2024

By: /s/ *John J. Nelson*

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Putative Class