John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

PRISCILLA WALL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

WESCOM CENTRAL CREDIT UNION and BARRACUDA NETWORKS, INC.,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Priscilla Wall ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Wescom Central Credit Union ("Wescom") and Barracuda Networks, Inc. ("Barracuda") (collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal

knowledge as to her own actions and her 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 cyberattack and data breach ("Data Breach") resulting from Wescom's failure to implement reasonable and industry standard data security practices.

2. Defendant Wescom is a California-based credit union that provides financial services to "more than 200,000 members" across its "24 branches".[1]

3. Defendant Barracuda is a data management corporation that provides IT services including "Email Protection, Application Protection, Network Security, and Data Protection Solutions."[2]

4. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

5. Defendants collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are (or were) customers at Wescom.

[1] https://www.wescom.org/About-Us (last accessed Nov. 6, 2023).

[2] https://www.barracuda.com (last accessed Nov. 7, 2023).

6. The personal information compromised in the Data Breach included Plaintiff's and Class Members' full names and financial account numbers ("personally identifiable information" or "PII").

7. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves.

8. As a result of the Data Breach, Plaintiff and approximately 34,000 Class Members,[3] suffered concrete injuries in fact 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) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff experiencing fraudulent charges, for approximately $11, placed on her Wescom Central Credit Union debit card, in or about November 2023; (ix) statutory damages; (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

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/d55f0583-a6fb-45aa-a46f-adb949f4197b.shtml (last accessed Nov. 6, 2023).

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

9. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Wescom's customers' PII from a foreseeable and preventable cyber-attack.

10. Defendants maintained the PII in a reckless manner. In particular, the PII was maintained on Defendants' computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to ensure those measures were followed by their IT vendors; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' PII; failing to take

standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct because the PII that Defendants collected and maintained is now in the hands of data thieves.

13. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other

protective measures to deter and detect identity theft.

16. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendants' inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. 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.

PARTIES

19. Plaintiff, Priscilla Wall, is a natural person and citizen of Riverside, California.

20. Defendant Wescom is a California corporation with its principal place of business located at 123 South Marengo Avenue, Pasadena, California 91101.

21. Defendant Barracuda is a Delaware corporation with its principal place of business located at 3175 South Winchester Boulevard, Campbell, California 95008.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendants.[4] This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

23. This Court has personal jurisdiction over Defendants because Defendants operate in this District and Defendants are authorized to and regularly conduct business in this District.

24. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District; Defendant Wescom's principal place of business is located in this

[4] According to the breach report submitted to the Office of the Maine Attorney General, 11 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d55f0583-a6fb-45aa-a46f-adb949f4197b.shtml (last accessed Nov. 7, 2023).

district; Defendants maintain Class Members' PII in this District; and Defendants caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendants' Businesses

25. Defendant Wescom is a California-based credit union that provides financial services to "more than 200,000 members" across its "24 branches".[5]

26. Defendant Barracuda is a data management corporation that provides IT services including "Email Protection, Application Protection, Network Security, and Data Protection Solutions."[6]

27. Plaintiff and Class Members are current and former Wescom customers.

28. As a condition of receiving financial services at Wescom, Defendants requires that Wescom's customers, including Plaintiff and Class Members, entrust Defendants with highly sensitive personal information.

29. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

30. Upon information and belief, in the course of collecting PII from its customers, including Plaintiff, Wescom promised to provide confidentiality and

[5] https://www.wescom.org/About-Us (last accessed Nov. 6, 2023).

[6] https://www.barracuda.com (last accessed Nov. 7, 2023).

adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

31. Indeed, the Privacy Policy posted on Wescom's website provides that: "[w]e use reasonable physical, electronic, and procedural safeguards that comply with federal standards to protect and limit access to personal information. This includes device safeguards and secured files and buildings."[7]

32. Plaintiff and the Class Members, as former and current Wescom customers, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers, in general, demand security to safeguard their PII.

The Data Breach

33. In the Notice of Data Breach letters sent to Plaintiff and Class Members on or about October 20, 2023 (the "Notice Letter"), Wescom asserts that:

> **What Happened?** On May 19, 2023, Barracuda announced a wide-spread vulnerability in their ESG appliance which allowed third party access to a subset of their ESG appliances since October 2022. On May 30, 2023, Barracuda confirmed this impacted Wescom. Upon notice, Wescom immediately removed the appliance from the network and began an investigation into the incident with cybersecurity experts.
>
> **What Information Was Involved?** The investigation determined the ESG

[7] https://www.wescom.org/online-privacy-policy#:~:text=We%20use%20reasonable%20physical%2C%20electronic,and%20secured%20files%20and%20buildings. (last accessed Nov. 6, 2023).

> had been accessed and that some emails and attachments stored on the appliances between October 30, 2022 and May 30, 2023, were potentially at risk. We reviewed the contents of the emails and attachments that were potentially accessible to the unauthorized person for personal information. On September 29, 2023, we determined that one or more emails or attachments stored on the ESG appliances included your name and financial account number[.][8]

34. Omitted from the Notice Letter were any explanation as to why Defendants failed to stop the unauthorized access for approximately *seven months* after the cyberattack began, any explanation as to why Defendants failed to inform Plaintiff and Class Members of the Data Breach for *more than five months* after being informed of the cyberattack, 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 omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

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

36. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for

[8] *Id.*

Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Wescom failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

37. Upon information and belief, the cyberattack was targeted at Defendants, due to their statuses as a financial institution and data management company that collects, creates, and maintains PII on their computer networks and/or systems.

38. As Wescom's Notice Letter admits, Plaintiff's and Class Members' PII was, in fact, compromised and acquired in the Data Breach.

39. The files containing Plaintiff's and Class Members' PII, that were targeted and stolen from Defendants, included their names and financial account numbers.[9]

40. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendants that included the PII of Plaintiff and Class Members.

41. As evidenced by the Data Breach's occurrence, the PII contained in Defendants' networks were not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

[9] *Id.*

42. Plaintiff's PII was accessed and stolen in the Data Breach and Plaintiff believes her stolen PII and that of Class Members is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

43. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Wescom, in its Notice Letter, instructs Plaintiff and Class Members to do the following:

> We remind you to remain vigilant to the possibility of fraud by reviewing your financial statements and credit reports for any unauthorized activity. If you see anything you do not recognize, please contact us or the relevant financial institution right away. We have also included information on what you can do to better protect against possible misuse of your information.
>
> Review the enclosed "Additional Steps You Can Take" document to continue to guard your information from fraud or identity theft. If you see anything you do not understand, call the credit agency immediately.
>
> Sign up for free Account Alerts in Online Banking to help you keep track of your Wescom accounts via text message or email notifications.
>
> Visit our Security Center at wescom.org/security-center for more ways on how Wescom can help you keep your accounts safe.[10]

44. In the Notice Letter, Wescom makes an offer of 12 months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing

[10] *Id.*

identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

45. That Wescom is encouraging its current and former customers to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII was acquired, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

46. Defendants had obligations created by the FTC Act, GLBA, contract, common law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure parties. Wescom further had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have legal duties to keep consumer's PII safe and confidential.

Data Breaches Are Preventable

47. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Wescom failed to exercise due diligence in selecting its IT vendors or deciding with whom it would

share sensitive PII.

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

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

- Implement an awareness and training program. Because end users are targets, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- 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.[11]

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

Secure internet-facing assets

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

- 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].[12]

[12] *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).

51. Given that Defendants were storing the PII of Wescom's current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

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

Defendants Acquire, Collect, And Store Customers' PII

53. Defendants acquire, collect, and store a massive amount of PII on their customers, former customers and other personnel.

54. Defendants retain and store this information and derive a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendants would be unable to perform their services.

55. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

56. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants 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.

57. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by Wescom exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

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

Defendants Knew, or Should Have Known, of the Risk Because Financial Institutions and Data Management Companies In Possession Of PII Are Particularly Suspectable To Cyber Attacks

59. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial institutions and data management companies that collect and store PII, like Defendants, preceding the date of the breach.

60. Data breaches, including those perpetrated against financial institutions and data management companies that store PII in their systems, have become widespread.

61. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal

information being compromised.[13]

62. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

63. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

64. Defendants knew and understood unprotected or exposed PII in the custody of financial institutions and data management companies, like Defendants,

---

[13] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

[14] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

65. At all relevant times, Defendants 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 Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

66. 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.

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

68. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

69. As a financial institution and data management company in custody of customers' PII, Defendants knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the

foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of PII

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or 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."[16]

71. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

72. Numerous sources cite dark web pricing for stolen identity credentials.[17]

---

[15] 17 C.F.R. § 248.201 (2013).

[16] *Id.*

[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital

73. For example, PII can be sold at a price ranging from $40 to $200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

74. PII can sell for as much as $363 per record according to the Infosec Institute.[20]

75. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

76. PII use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable

---

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).

[18] *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).

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

[20] *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 May 7, 2023).

information . . . [is] worth more than 10x on the black market."[21]

78. 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.

79. 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:

> [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.[22]

80. 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 retailer data breach because, there, victims can cancel or close

---

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

[22] *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).

credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

Defendants Fail To Comply With FTC Guidelines

81. 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.

82. 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 customer 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.[23]

83. 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 is attempting to hack the system; watch for

[23] *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).

large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

84. 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.

85. The FTC has brought enforcement actions against financial institutions for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer 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.

86. These FTC enforcement actions include actions against financial institutions and data management companies, like Defendants.

87. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and Wescom failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to

[24] *Id.*

employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

88. Upon information and belief, Defendants were at all times fully aware of their obligations to protect the PII of Wescom's customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Wescom Fails To Comply with the Gramm-Leach-Bliley Act

89. Wescom is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

90. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

91. Wescom collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Wescom was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

92. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the

CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

93. Accordingly, Wescom's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

94. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. §

1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Wescom violated the Privacy Rule and Regulation P.

95. Upon information and belief, Wescom failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Wescom' network systems.

96. Wescom failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an unsecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

97. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and

regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

98. As alleged herein, Wescom violated the Safeguard Rule.

99. Wescom failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

100. Wescom violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Fail To Comply With Industry Standards

101. As noted above, experts studying cyber security routinely identify financial institutions and data management companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

102. Several best practices have been identified that, at a minimum, should

be implemented by financial institutions and data management companies in possession of PII, like Defendants, 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. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

103. Other best cybersecurity practices that are standard in the financial services and data management industries 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. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

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

Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

105. These foregoing frameworks are existing and applicable industry standards in the financial services and data management industries, and upon information and belief, Defendants 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.

Defendants Breached Their Duties to Safeguard Customers' PII

106. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members

107. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard their computer systems and data, and Wescom failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants'

unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' PII;

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

d. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

e. Failing to sufficiently train their employees and vendors regarding the proper handling of customers' PII;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to the Gramm-Leach-Bliley Act and industry standards for cybersecurity as discussed above; and,

h. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

108. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their computer networks and systems and/or their vendor's computer networks and systems, which

contained unsecured and unencrypted PII.

109. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

Common Injuries & Damages

110. As a result of Defendants' 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants

fail to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

111. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

112. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

113. 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.

114. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

115. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more

information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

116. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[25]

117. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen

[25] "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-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

118. 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' 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.

119. 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 phone numbers and emails) of Plaintiff and the other Class Members.

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

121. 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 Risk Of Identity Theft And Fraud

122. 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. 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.

123. Thus, due to the actual and imminent risk of identity theft as a result of the Data Breach, Wescom, in its Notice Letter, instructs Plaintiff and Class Members to do the following:

> We remind you to remain vigilant to the possibility of fraud by reviewing your financial statements and credit reports for any unauthorized activity. If you see anything you do not recognize, please contact us or the relevant financial institution right away. We have also included information on what you can do to better protect against possible misuse of your information.
>
> Review the enclosed "Additional Steps You Can Take" document to continue to guard your information from fraud or identity theft. If you see anything you do not understand, call the credit agency immediately.
>
> Sign up for free Account Alerts in Online Banking to help you keep track of your Wescom accounts via text message or email notifications.
>
> Visit our Security Center at wescom.org/security-center for more ways on how Wescom can help you keep your accounts safe.[26]

[26] The Notice Letter.

124. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as replacing debit cards in response to fraudulent charges; contacting banks to sort out fraudulent activity on their accounts and place security measures on their accounts; and researching and verifying the legitimacy of the Data Breach, upon receiving the Notice Letter.

125. 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."[27]

126. 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.[28]

---

[27] *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.

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

127. 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."[29]

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

128. Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

129. 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 Defendants' Data Breach.

Loss Of The Benefit Of The Bargain

130. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Wescom and/or its agents for financial services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and

[29] *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").

necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received financial services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Wescom.

Plaintiff Wall's Experience

131. Plaintiff Priscilla Wall is a current Wescom customer.

132. In order to obtain financial services at Wescom, she was required to provide her PII to Defendants, including her name and financial account information.

133. At the time of the Data Breach—October 30, 2022 through May 30, 2023—Defendants retained Plaintiff's PII in their systems.

134. Plaintiff Wall is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

135. Plaintiff Priscilla Wall received the Notice Letter, by U.S. mail, directly from Wescom, dated October 20, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name and financial account number.

136. As a result of the Data Breach, and at the direction of Wescom's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including replacing debit cards in response to fraudulent charges; contacting banks to sort out fraudulent activity and place security measures on her accounts; and researching and verifying the legitimacy of the Data Breach, upon receiving the Notice Letter. Plaintiff has spent significant time dealing with 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.

137. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her 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 her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

138. Plaintiff also suffered actual injury in the form of experiencing fraudulent charges to Wescom debit card, for approximately $11, in or about November 2023, which, upon information and belief, was caused by the Data Breach.

139. Plaintiff further 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.

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

141. 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.

142. 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.

143. Plaintiff Priscilla Wall has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

144. Plaintiff brings this class action on behalf of herself and others similarly

situated, pursuant to Federal Rule of Civil Procedure 23, for the following Class and Subclass defined as:

> **Nationwide Class**
> **All individuals residing in the United States whose PII was compromised in the data breach announced by Wescom in October 2023 (the "Class").**
>
> **California Subclass**
> **All individuals residing in the United States whose PII was compromised in the data breach announced by Wescom in October 2023 (the "California Subclass").**

145. Excluded from the Class and California Subclass are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has 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.

146. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

147. **Numerosity:** The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 34,000 individuals were notified by Wescom of the Data Breach, according to the breach

report submitted to Office of the Maine Attorney General.[30] The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by Wescom sending them breach notification letters).

148. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendants had duties to protect the PII of Plaintiff and Class Members;

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

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

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

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

[30] https://apps.web.maine.gov/online/aeviewer/ME/40/d55f0583-a6fb-45aa-a46f-adb949f4197b.shtml (last accessed Nov. 6, 2023).

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

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

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

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

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

149. **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.

150. **Policies Generally Applicable to the Class:** This class action is also

appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

151. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she 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 she 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.

152. **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 Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

153. Plaintiff and Class Members are ascertainable because Defendants' records will identify all victims of Defendants' Data Breach.

154. Plaintiff and Class Members are sufficiently numerous as to justify class action. Specifically, the putative Class exceeds 81,000 individuals.

155. Plaintiff and Class Members have a well-defined community of interest in pursuing relief from the harm that resulted from the Data Breach, including (1) predominant common questions of law or fact; (2) a class representative with claims or defenses typical of the class; and (3) a class representative who can adequately represent the class.

156. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources

of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

160. Plaintiff restates and realleges the factual allegations in paragraphs 1

through 159, as if fully set forth herein.

161. Wescom requires its customers, including Plaintiff and Class Members, to submit non-public PII to Defendants in the ordinary course of providing its financial services.

162. Defendants gathered and stored the PII of Plaintiff and Class Members as part of their businesses of soliciting their services to their customers and/or clients, which solicitations and services affect commerce.

163. Plaintiff and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard their information.

164. Defendants 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.

165. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had duties of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. Moreover, Wescom's duty included a responsibility to

exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

166. Defendants had duties 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.

167. Wescom's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

168. Defendants owed duties of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

169. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Wescom and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class

entrusted Wescom with their confidential PII, a necessary part of being customers at Wescom.

170. Defendants' 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 Defendants are bound by industry standards to protect confidential PII.

171. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

172. Defendants also had duties to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

173. Moreover, Defendants had duties to promptly and adequately notify Plaintiff and the Class of the Data Breach.

174. Defendants had and continues to have duties to adequately disclose that the PII of Plaintiff and the Class within Defendants' 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.

175. Defendants breached their duties, pursuant to the FTC Act, and Wescom breached its duties, pursuant to GLBA and other applicable standards, and

thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants 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. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

e. Allowing unauthorized access to Class Members' PII;

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

g. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

h. 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; and

i. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

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

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

178. Defendants' violation of Section 5 of the FTC Act and Wescom's violation of GLBA constitutes negligence.

179. 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.

180. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of

Defendants' inadequate security practices.

181. It was foreseeable that Defendants' 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 in the financial services and data management industries.

182. Defendants have 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.

183. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants 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 Defendants' systems.

184. 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.

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

186. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

187. Defendants' duties 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.

188. Wescom 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.

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

190. There is a close causal connection between Defendants' 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 Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

191. As a direct and proximate result of Defendants' 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) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff experiencing fraudulent charges, for approximately $11, placed on her Wescom Central Credit Union debit card, in or about November 2023; (ix) statutory damages; (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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

192. As a direct and proximate result of Defendants' 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.

193. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to

further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

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

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

196. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their 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 the Class)

197. Plaintiff restates and realleges the factual allegations in paragraphs 1 through 159, as if fully set forth herein, and brings this count against Defendant Wescom ("Defendant" for the purposes of this count).

198. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of obtaining financial services at Defendant.

199. 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.

200. 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 and were consistent with industry standards.

201. 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.

202. 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.

203. Defendant solicited, offered, and invited Plaintiff and 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.

204. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

205. 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.

206. 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.

207. Plaintiff and Class Members paid money 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.

208. 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.

209. 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.

210. Plaintiff and Class Members fully and adequately performed their

obligations under the implied contracts with Defendant.

211. 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.

212. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

214. 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 / Quasi Contract
(On Behalf of Plaintiff and the Class)

215. Plaintiff restates and realleges the factual allegations in paragraphs 1 through 159, as if fully set forth herein.

216. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for financial services from Wescom and/or its agents and in so doing also provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Wescom the services that were the subject of the transaction and should have had their PII protected with adequate data security.

217. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

218. Defendants 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.

219. Defendants acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

220. If Plaintiff and Class Members had known that Defendants 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 Defendants or obtained financial services at Wescom.

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

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

223. As a direct and proximate result of Defendants' 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) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff experiencing fraudulent charges, for approximately $11, placed on her Wescom Central Credit Union debit card, in or about November 2023; (ix) statutory damages; (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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

224. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their

wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

225. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, 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 the California Subclass)

226. Plaintiff restates and realleges the factual allegations in paragraphs 1 through 159, as if fully set forth herein, and brings this claim individually and on behalf of the California Subclass (the "Class" for the purposes of this count).

227. Defendants are "persons" defined by Cal. Bus. & Prof. Code § 17201.

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

229. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendants failed to identify foreseeable security risks, remediate

identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industries;

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused;

d. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices; and,

e. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

230. Defendants have engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, GLBA, and California common law.

231. Defendants' 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;

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

personal information; and

f. 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, including duties imposed by the FTC Act, 15 U.S.C. § 45.

232. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security systems and abilities to protect the confidentiality of consumers' personal information.

233. As a direct and proximate result of Defendants' unfair and unlawful 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

234. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

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

236. By deceptively storing, collecting, and disclosing their personal

information, Defendants have taken money or property from Plaintiff and Class Members.

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

238. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and California Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from

refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

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

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

iii. Requiring Defendants to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of

such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants 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 Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

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

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

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

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

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

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all customers, with additional training to be provided as appropriate based upon the customers' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

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

xiii. Requiring Defendants to implement a system of tests to assess their respective customers' knowledge of the education programs discussed in the preceding subparagraphs, as well as

randomly and periodically testing customers' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

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

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the

terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff Priscilla Wall, individually and on behalf of the putative Classes, demands a trial by jury on all claims so triable.

DATED: November 7, 2023

Respectfully submitted,

s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class