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

Matthew Righetti
RIGHETTI GLUGOSKI, P.C.
2001 Union Street, Ste. 400
San Francisco, California 94123
Office: 415-983-0900
Cell: 415-264-9990

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

JONATHAN CUMMINGS and MISTY CALDERON on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

TELEFLORA LLC,

Defendant.

Case No.: 2:24-CV-02474-PA-SK

CLASS ACTION

DEMAND FOR A JURY TRIAL

FIRST AMENDED COMPLAINT

Plaintiffs Jonathan Cummings, and Misty Calderon ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Teleflora LLC ("Defendant" or "Teleflora") on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a company that operates "over 10,000 member florists throughout the U.S. and Canada[.]"[1]

2. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised and unlawfully accessed due to the Data Breach.

3. Plaintiffs bring this First Amended Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: names, TINs and Social Security numbers, (collectively defined herein as "PII").

[1] https://www.teleflora.com/info/about

4. Upon information and belief, former and current customers of Defendant are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain services from Defendant. Defendant retains this information for at least many years and even after the consumer relationship has ended.

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

6. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

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

8. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a company that collects and maintains highly valuable PII on its systems.

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

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

11. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through

disclosure to an unknown and unauthorized third party. Plaintiffs 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.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent charges placed on Plaintiffs' debit cards and credit accounts, totaling more than $1,000, in or about November 2023 through March 2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal

data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

14. Plaintiff Jonathan Cummings is and has been at all relevant times a resident and citizen of Upper Marlboro, Maryland.

15. Plaintiff Misty Calderon is and has been at all relevant times a resident and citizen of Fairfield, California.

16. Plaintiffs' PII was subject to unauthorized access, disclosure, theft, and exfiltration as a result of the Data Breach. This resulted in an invasion of Plaintiffs' privacy interests, loss of value of their PII, and has placed them at imminent, immediate, and continuing risk of further harm from identity theft and other misuse of their PII. Plaintiffs expect that it will be necessary for them to spend time and money on credit monitoring, including the expense of a credit monitoring service as part of a reasonable effort to mitigate against such harm and will continue to incur such expenses on an ongoing basis. Had Plaintiffs known that Defendant employed substandard data security, they would not have provided their PII to Defendant or used Defendant's services.

17. Defendant Teleflora LLC is a limited liability company with its principal office located in Los Angeles, California.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Cummings, is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because it maintains its principal place of business is in this District, the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District, regularly conducts business in California, and has sufficient minimum contacts in California.

20. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Defendant's Business

21. Defendant is a company that operates "over 10,000 member florists throughout the U.S. and Canada[.]"[2]

22. Plaintiffs and Class Members are current and former customers that obtained services from Defendant.

[2] https://www.teleflora.com/info/about

23. In order to obtain services from Defendant, Plaintiffs and Class Members were required to provide sensitive and confidential PII, including their names, TINs and Social Security numbers.

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

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

26. Indeed, Defendant provides on its website that:

> Information will be retained only for so long as reasonably necessary for the purposes set out above, in accordance with applicable laws.
>
> We maintain reasonable security measures to safeguard information from loss, theft interference, misuse, unauthorized access, disclosure, alteration, or destruction. We also maintain reasonable procedures to help ensure that such data is reliable for its intended use and is accurate, complete, and current.[3]

27. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would

[3] https://www.teleflora.com/info/privacy-policy

comply with its obligations to keep such information confidential and secure from unauthorized access.

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

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

30. Defendant had obligations created by FTC Act, Cal. Civ. Code § 1798.150, *et seq*, Cal. Civ. Code § 1798.82, *et seq*., Cal. Bus. & Prof. Code § 17200, *et seq*. contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

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

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or

should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

33. On or about March 13, 2024, Defendant began sending Plaintiffs and other victims of the Data Breach an untitled letter, informing them that:

> **What Happened?**
> On November 9, 2023, we identified unusual activity in our network related to a third-party software provider. We immediately took steps to contain the activity and launched a full investigation of the incident. On November 29, 2023, that investigation determined an unauthorized person accessed or acquired certain files from our network.
>
> **What Information Was Involved?**
> On February 23, 2024, we completed a manual review of the files that were involved, and determined that a file contained your name and Social Security number.[4]

34. Omitted from the Notice Letter were the date(s) of the Data Breach, the identity of the cybercriminals who perpetrated the cyber-attack, the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took nearly an entire year from the day of the Data Breach to inform impacted individuals that their information was involved, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

[4] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/0e58cbaf-cc13-4651-9595-3f508d6e7260.shtml

35. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

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

37. Notably, companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. By sending notice letters to Plaintiffs and Class Members, it admits that Defendant itself has a "reasonable belief" that Plaintiffs' and Class Members' names, TINs and Social Security numbers were accessed or acquired by an "unknown actor" – aka cybercriminals.

38. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the approximate 12,000 Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data or whether Defendant was interested in hearing about misuse of their data or set up a mechanism for Class Members to report misuse of their data.

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

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

41. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- 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.[5]

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

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

- Monitor for adversarial activities

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

- 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].[6]

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

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over 12,000 customers,[7] including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Its Customers' PII

46. As a condition to obtain services from Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

[6] *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).

[7] According to the breach report submitted to the Office of the Maine Attorney General, 12,635 persons were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/0e58cbaf-cc13-4651-9595-3f508d6e7260.shtml

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

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

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

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

51. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

52. Indeed, Defendant provides on its website that:

> Information will be retained only for so long as reasonably necessary for the purposes set out above, in accordance with applicable laws.
>
> We maintain reasonable security measures to safeguard information from loss, theft interference, misuse, unauthorized access, disclosure, alteration, or

destruction. We also maintain reasonable procedures to help ensure that such data is reliable for its intended use and is accurate, complete, and current.[8]

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

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

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

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

56. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4

---

[8] https://www.teleflora.com/info/privacy-policy

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

[10] *Id.*

million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

57. Indeed, cyber-attacks, such as the one experienced by Defendant, 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."[11]

58. Additionally, as companies became more dependent on computer systems to run their business,[12] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[13]

59. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached,

[11] 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).

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

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

including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

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

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

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

63. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PII. Moreover,

once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

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

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

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

67. As a floral company in possession of its customers' and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] 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."[15]

69. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16] For example, Personal Information can be sold at a price ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[17] *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).
[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

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

71. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[19] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[20]

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

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

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

[20] *Id.*

illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

74. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[22] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[23]

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

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

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

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

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

all of that old bad information is quickly inherited into the new Social Security number."[24]

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

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

78. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[25]

79. 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 credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

80. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

81. 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.

---

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

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

82. 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.[27]

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

Defendant Fails to Comply with FTC Guidelines

84. 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.

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for

[27] *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).

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.[28]

86. 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 large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

87. 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.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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

[28] *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).
[29] *Id.*

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.

89. These FTC enforcement actions include actions against floral companies, like Defendant.

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

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

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

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

Defendant Fails to Comply with Industry Standards

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

95. Several best practices have been identified that, at a minimum, should be implemented by floral companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

97. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (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.

98. These foregoing frameworks are existing and applicable industry standards in the floral industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

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

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk of Identity Theft

100. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

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

102. 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.

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

104. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive

personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[30]

105. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[31]

106. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[32] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[33]

---

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

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

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

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

107. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[34]

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

109. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create

[34] "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/

a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

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

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

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

113. 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.

114. Thus, due to the actual and continuing risk of identity theft, Defendant, in its Notice Letter, encourages Plaintiffs and Class Members to take the following

measures to protect themselves: "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."[35]

115. In addition, Defendant's Notice letter includes a full-page detailing how to sign up for the credit monitoring services offered by Defendant as well as two full pages devoted to "Additional Steps You Can Take" that recommend Plaintiffs and Class Members to partake in activities such as placing fraud alerts on their accounts, putting a freeze on their credit, and contacting government agencies for more information.[36]

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

117. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the

[35] Notice Letter.

[36] *Id.*

legitimacy of the Data Breach upon receiving the Notice Letter and monitoring their financial accounts for fraudulent activity, which may take years to detect.

118. Plaintiffs' 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."[37]

119. Plaintiffs' 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.[38]

120. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

---

[37] *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.

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

Diminution Of Value Of PII

121. PII is a valuable property right.[39] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

122. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[40]

123. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[41] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[42,43] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[44]

---

[39] *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").

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

[41] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

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

[43] https://datacoup.com/

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

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

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

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

127. Plaintiffs 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.

128. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than

twelve thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

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

131. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

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

Loss of Benefit of the Bargain

134. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCE

135. Plaintiffs own and operate companies that contract with Defendant for services.

136. As a condition of receiving services at Defendant, Plaintiffs were required to provide Defendant with his sensitive PII.

137. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

138. Plaintiffs are very careful about sharing their sensitive PII. Plaintiffs store any documents containing PII in a safe and secure location. Plaintiffs have never

knowingly transmitted their unencrypted sensitive PII over the internet or any other unsecured source.

139. Plaintiffs received the Notice Letter, by U.S. mail, directly from Defendant, dated March 14, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including their names and Social Security numbers.

140. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiffs to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity[,]"[45] Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiffs have spent significant time dealing with the Data Breach, valuable time Plaintiffs 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.

141. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach 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

[45] Notice Letter.

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 his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

142. Plaintiffs further suffered actual injury in the form of fraudulent charges and exposure to fraudulent charges. For example, Plaintiff Cummings was exposed to fraudulent charges placed on his M&T Bank debit card, totaling more than $1,000, in or about November 2023 through March 2024, which, upon information and belief, was caused by the Data Breach.

143. Plaintiffs additionally 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.

144. These misuses of Plaintiffs' PII were caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including

websites that aggregate and associate personal information with the owner of such information.

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

146. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

147. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

148. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

149. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**
> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in March 2024, including all those who were sent Notice (the "Class")

California Sub-Class
All individuals residing in California whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in March 2024, including all those who were sent Notice (the "California Sub-Class").

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

151. Plaintiffs reserve the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

152. **Numerosity**: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 12,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney General's Office.[46] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

[46] https://apps.web.maine.gov/online/aeviewer/ME/40/0e58cbaf-cc13-4651-9595-3f508d6e7260.shtml

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

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

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

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

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

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

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

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

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

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

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

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

154. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, 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.

155. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

156. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

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

158. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs

alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were 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.

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

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

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

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

163. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

164. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

165. Defendant requires its customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

166. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

167. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

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

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

170. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits

"unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

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

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

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

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

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

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

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

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

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

c. Allowing unauthorized access to Class Members' PII;

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

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

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

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

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

181. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

182. 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 Plaintiffs and the Class.

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

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

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

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

187. 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.

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

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

190. Defendant's duty extended to protecting Plaintiffs 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.

191. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

192. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

194. As a direct and proximate result of Defendant's negligence, Plaintiffs 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) statutory damages; (viii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent charges placed on Plaintiff's M&T Bank debit card, totaling more than $1,000, in or about November 2023 through March 2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

197. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring

procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

198. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

199. Plaintiffs and Class Members were required to deliver their PII to Defendant as part of the process of obtaining services from Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

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

201. Defendant accepted possession of Plaintiffs' and Class Members' PII for the purpose of providing services to Plaintiffs and Class Members.

202. Plaintiffs and the Class entrusted their PII to Defendant. In so doing, Plaintiffs 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 Plaintiffs and the Class if their data had been breached and compromised or stolen.

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

204. Implicit in the agreement between Plaintiffs 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 Plaintiffs 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 information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

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

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

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

208. Plaintiffs 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.

209. Plaintiffs 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.

210. Plaintiffs 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.

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

212. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

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

215. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent charges placed on Plaintiff's M&T Bank debit card, totaling more than $1,000, in or about November 2023 through March 2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is

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

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

217. Plaintiffs 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
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

218. Plaintiffs incorporates the foregoing allegations as though fully set forth herein.

219. Defendant invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' PII, as set forth above. Defendant further invaded Plaintiffs' and Class Member's privacy by giving publicity to Plaintiffs' and Class Members sensitive and confidential PII.

220. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and

Class Members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

221. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class Members provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

222. As a direct and proximate result of Defendant's above acts, Plaintiffs' and the Class Members' PII was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages as described herein.

223. Defendant has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

224. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Defendant may freely treat Plaintiffs' and Class Members' PII with sub-standard and insufficient protections.

225. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs and the Class

Members great and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

226. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

227. Plaintiffs bring this Count in the alternative to the breach of implied contract count above.

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

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

230. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PIIprovided.

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

232. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII to Defendant or obtained services offered by Defendant.

233. Plaintiffs and Class Members have no adequate remedy at law.

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

235. As a direct and proximate result of Defendant's conduct, Plaintiffs 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) statutory damages; (viii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent charges placed on Plaintiff's M&T Bank debit card, totaling more than $1,000, in or about November 2023 through March

2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

COUNT V
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
(On Behalf of Plaintiff and the Class)

238. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

239. Defendant violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair

competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

240. The acts and omissions identified herein were conceived of, directed from, and emanated from Defendant's California headquarters and harmed consumers nationwide.

241. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII of Plaintiffs and the Class Members.

242. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

243. Defendant also violated its posted privacy policy, knowingly and willfully or negligently and materially, in violation of Cal. Bus. & Prof. Code § 22576.

244. Defendant also violated Section 5 of the FTC Act by failing to employ reasonable and adequate data security safeguards.

245. Defendant further committed unfair acts by failing to employ adequate and reasonable safeguards.

246. Defendant's conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiffs and Class Members. Further, Defendant's conduct narrowly benefited its own business interests at the expense of Plaintiffs' and Class Members' fundamental property and privacy interests protected by the California Constitution and the common law.

247. As a direct and proximate result of Defendant's unlawful and unfair practices and acts, Plaintiffs and Class Members were injured and lost money or property, 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) statutory damages; (viii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent charges placed on Plaintiff's M&T Bank debit card, totaling more than $1,000, in or about November 2023 through March 2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

248. Plaintiffs and Class Members have suffered harm in the form of lost property value, specifically the diminution of the value of their private and personally identifiable data.

249. Defendant's actions caused damage to and loss of Plaintiffs' and Class Members' property right to control the dissemination and use of their personal information and communications.

250. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful and unfair practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

251. Plaintiffs, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.,* including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VI
Violations of the California Consumer Privacy Act
(Cal. Civ. Code § 1798.150)

(On Behalf of Plaintiff Misty Calderon and the California Sub-Class)

252. Plaintiff Misty Calderon ("Plaintiff for the purposes of this Count) incorporates the foregoing allegations as though fully set forth herein.

253. At all relevant times, Defendant was a "business," within the meaning of the California Consumer Privacy Act ("CCPA"). Defendant operates in the State of California and collects consumers' personal information. Plaintiffs are informed and believe that each Defendant either has an annual operating revenue above $25 million or has collected the personal information of 50,000 or more California residents annually or derives at least 50 percent of its annual revenue from the sale of personal information of California residents.

254. At all relevant times, Plaintiff was a "consumer" under the terms of the CCPA as natural persons as defined in Section 17014 of Title 18 of the California Code of Regulations.

255. By the acts described above, Defendant violated the CCPA by negligently, carelessly, and recklessly collecting, maintaining, and controlling their customers' sensitive personal information and by engineering, designing, maintaining, and controlling digital infrastructure that exposed their customers' sensitive personal information of which Defendant had control and possession to the risk of exposure to unauthorized persons, thereby violating its duty to implement and

maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII. Defendant allowed unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted PII of Plaintiff and other members of the sub-class.

256. Plaintiff has complied with the requirements of California Civil Code section 1798.150(b) and provided Defendant with written notice of the specific provisions of the CCPA that Plaintiff alleges have been violated via certified mail. Thirty days after its receipt of Plaintiff's CCPA notice letter, Defendant made no response and has and cannot cure the violations alleged therein.

257. As a result of Defendants' violations, Plaintiff and the sub-class are entitled to actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA, and to such other and further relief as this Court may deem just and proper.

COUNT VII
Violation of the Customer Records Act
(Cal. Civ. Code § 1798.82 ("CRA"))

(On Behalf of Plaintiff Misty Calderon and the California Sub-Class)

258. Plaintiff Misty Calderon ("Plaintiff for the purposes of this Count) incorporates the foregoing allegations as though fully set forth herein.

259. At all relevant times, Defendant was a "business" under the terms of the CRA as sole proprietorships, partnerships, corporations, associations, financial

institutions, or other groups, operating in the State of California that owned or licensed computerized data that included the personal information of Plaintiffs.

260. At all relevant times, Plaintiff was a "customer" under the terms of the CRA as a natural person who provided personal information to Defendant for the purpose of purchasing or leasing a product or obtaining a service.

261. By the acts described above, Defendant violated the CRA by allowing unauthorized access to customers' personal information and then failing to inform them when the unauthorized use occurred for weeks or months, thereby failing in their duty to inform their customers of unauthorized access expeditiously and without delay.

262. As a direct consequence of the actions as identified above, Plaintiff and sub-class members incurred additional losses and suffered further harm to their privacy, including but not limited to the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal information disclosed, that they would not have otherwise lost had Defendant immediately informed them of the unauthorized use.

263. As a result of Defendants' violations, Plaintiff and sub-class members are entitled to all actual and compensatory damages according to proof, to non-

economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class and sub-class;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

xiii. requiring Defendant to implement a system of tests to assess its

employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

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

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

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 Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and

to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

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

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

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class and sub-class, demand a trial by jury for all issues so triable.

Respectfully submitted,

Date: May 31, 2024

By: *s/ John J. Nelson*

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

MATTHEW RIGHETTI (SBN 121012)
RIGHETTI GLUGOSKI, P.C.
2001 Union Street, Suite 400
San Francisco, CA 94129
Telephone: (415) 983-0900
matt@righettilaw.com

Attorneys for Plaintiffs and the Putative Class