

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

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

*Attorney for Plaintiff*

**UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

JONATHAN CUMMINGS, on behalf  
of himself and all others similarly  
situated,  
  
Plaintiff,  
  
v.  
  
TELEFLORA LLC,  
  
Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION**

**DEMAND FOR A JURY TRIAL**

Plaintiff Jonathan Cummings (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant Teleflora LLC (“Defendant” or “Teleflora”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

1 **NATURE OF THE ACTION**

2 1. This class action arises out of the recent data breach (“Data Breach”)  
3 involving Defendant, a company that operates “over 10,000 member florists  
4 throughout the U.S. and Canada[.]”<sup>1</sup>

5  
6 2. Plaintiff’s and Class Members’ sensitive personal information—which  
7 they entrusted to Defendant on the mutual understanding that Defendant would  
8 protect it against disclosure—was targeted, compromised and unlawfully accessed  
9 due to the Data Breach.  
10

11  
12 3. Plaintiff brings this Complaint against Defendant for its failure to  
13 properly secure and safeguard the personally identifiable information that it collected  
14 and maintained as part of its regular business practices, including, but not limited to:  
15 names and Social Security numbers, (collectively defined herein as “PII”).  
16

17 4. Upon information and belief, former and current customers of Defendant  
18 are required to entrust Defendant with sensitive, non-public PII, without which  
19 Defendant could not perform its regular business activities, in order to obtain services  
20 from Defendant. Defendant retains this information for at least many years and even  
21 after the consumer relationship has ended.  
22

23  
24 5. By obtaining, collecting, using, and deriving a benefit from the PII of  
25 Plaintiff and Class Members, Defendant assumed legal and equitable duties to those  
26  
27

28 \_\_\_\_\_  
<sup>1</sup> <https://www.teleflora.com/info/about>

1 individuals to protect and safeguard that information from unauthorized access and  
2 intrusion.

3  
4 6. Defendant failed to adequately protect Plaintiff's and Class Members  
5 PII—and failed to even encrypt or redact this highly sensitive information. This  
6 unencrypted, unredacted PII was compromised due to Defendant's negligent and/or  
7  
8 careless acts and omissions and its utter failure to protect customers' sensitive data.  
9 Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value  
10 in exploiting and stealing the identities of Plaintiff and Class Members. The present  
11 and continuing risk of identity theft and fraud to victims of the Data Breach will  
12 remain for their respective lifetimes.  
13

14 7. The Data Breach was a direct result of Defendant's failure to implement  
15 adequate and reasonable cyber-security procedures and protocols necessary to protect  
16 consumers' Private Information from a foreseeable and preventable cyber-attack.  
17

18 8. Moreover, upon information and belief, Defendant was targeted for a  
19 cyber-attack due to its status as a company that collects and maintains highly valuable  
20 PII on its systems.  
21

22 9. In breaching its duties to properly safeguard customers' PII and give  
23 customers timely, adequate notice of the Data Breach's occurrence, Defendant's  
24 conduct amounts to negligence and/or recklessness and violates federal and state  
25 statutes.  
26  
27  
28

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

9  
10           11. Defendant disregarded the rights of Plaintiff and Class Members by  
11 intentionally, willfully, recklessly, or negligently failing to implement and maintain  
12 adequate and reasonable measures to ensure that the PII of Plaintiff and Class  
13 Members was safeguarded, failing to take available steps to prevent an unauthorized  
14 disclosure of data, and failing to follow applicable, required, and appropriate  
15 protocols, policies, and procedures regarding the encryption of data, even for internal  
16 use. As a result, the PII of Plaintiff and Class Members was compromised through  
17 disclosure to an unknown and unauthorized third party. Plaintiff and Class Members  
18 have a continuing interest in ensuring that their information is and remains safe, and  
19 they should be entitled to injunctive and other equitable relief.  
20  
21  
22  
23

24           12. Plaintiff and Class Members have suffered injury as a result of  
25 Defendant’s conduct. These injuries include: (i) invasion of privacy; (ii) theft of their  
26 PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated  
27 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of  
28

1 benefit of the bargain; (vi) lost opportunity costs associated with attempting to  
2 mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii)  
3 actual misuse of the compromised data consisting of an increase in spam calls, texts,  
4 and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent  
5 charges placed on Plaintiff's M&T Bank debit card, totaling more than \$1,000, in or  
6 about November 2023 through March 2024; (xi) nominal damages; and (xii) the  
7 continued and certainly increased risk to their PII, which: (a) remains unencrypted  
8 and available for unauthorized third parties to access and abuse; and (b) remains  
9 backed up in Defendant's possession and is subject to further unauthorized  
10 disclosures so long as Defendant fails to undertake appropriate and adequate measures  
11 to protect the PII.

12  
13  
14  
15  
16 13. Plaintiff seeks to remedy these harms and prevent any future data  
17 compromise on behalf of himself and all similarly situated persons whose personal  
18 data was compromised and stolen as a result of the Data Breach and who remain at  
19 risk due to Defendant's inadequate data security practices.

20  
21 **PARTIES**

22  
23 14. Plaintiff Jonathan Cummings is and has been at all relevant times a  
24 resident and citizen of Upper Marlboro, Maryland.

25  
26 15. Defendant Teleflora LLC is a limited liability company with its principal  
27 office located in Los Angeles, California.

1 **JURISDICTION AND VENUE**

2 16. This Court has subject matter jurisdiction over this action under 28  
3 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy  
4 exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more  
5 than 100 members in the proposed class, and at least one member of the class,  
6 including Plaintiff, is a citizen of a state different from Defendant.  
7

8  
9 17. This Court has personal jurisdiction over Defendant because it  
10 maintains its principal place of business is in this District, the acts and omissions  
11 giving rise to Plaintiff’s claims occurred in and emanated from this District, regularly  
12 conducts business in California, and has sufficient minimum contacts in California.  
13

14 18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's  
15 principal place of business is in this District.  
16

17 **FACTUAL ALLEGATIONS**

18 ***Defendant's Business***

19  
20 19. Defendant is a company that operates “over 10,000 member florists  
21 throughout the U.S. and Canada[.]”<sup>2</sup>  
22

23 20. Plaintiff and Class Members are current and former customers that  
24 obtained services from Defendant.  
25  
26  
27

28 \_\_\_\_\_  
<sup>2</sup> <https://www.teleflora.com/info/about>

1           21. In order to obtain services from Defendant, Plaintiff and Class Members  
2 were required to provide sensitive and confidential PII, including their names and  
3 Social Security numbers.  
4

5           22. The information held by Defendant in its computer systems at the time  
6 of the Data Breach included the unencrypted PII of Plaintiff and Class Members.  
7

8           23. Upon information and belief, Defendant made promises and  
9 representations to its customers, including Plaintiff and Class Members, that the PII  
10 collected from them as a condition of receiving services would be kept safe,  
11 confidential, that the privacy of that information would be maintained, and that  
12 Defendant would delete any sensitive information after it was no longer required to  
13 maintain it.  
14

15           24. Indeed, Defendant provides on its website that:  
16

17 Information will be retained only for so long as reasonably necessary for the  
18 purposes set out above, in accordance with applicable laws.

19 We maintain reasonable security measures to safeguard information from loss,  
20 theft interference, misuse, unauthorized access, disclosure, alteration, or  
21 data is reliable for its intended use and is accurate, complete, and current.<sup>3</sup>  
22

23           25. Plaintiff and Class Members provided their PII to Defendant with the  
24 reasonable expectation and on the mutual understanding that Defendant would  
25  
26  
27

28 

---

<sup>3</sup> <https://www.teleflora.com/info/privacy-policy>

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

3  
4 26. Plaintiff and the Class Members have taken reasonable steps to maintain  
5 the confidentiality of their PII. Plaintiff and Class Members relied on the  
6 sophistication of Defendant to keep their PII confidential and securely maintained, to  
7 use this information for necessary purposes only, and to make only authorized  
8 disclosures of this information. Plaintiff and Class Members value the confidentiality  
9 of their PII and demand security to safeguard their PII.  
10

11  
12 27. Defendant had a duty to adopt reasonable measures to protect the PII of  
13 Plaintiff and Class Members from involuntary disclosure to third parties. Defendant  
14 has a legal duty to keep consumer's PII safe and confidential.  
15

16 28. Defendant had obligations created by FTC Act, contract, industry  
17 standards, and representations made to Plaintiff and Class Members, to keep their PII  
18 confidential and to protect it from unauthorized access and disclosure.  
19

20 29. Defendant derived a substantial economic benefit from collecting  
21 Plaintiff's and Class Members' PII. Without the required submission of PII,  
22 Defendant could not perform the services it provides.  
23

24 30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's  
25 and Class Members' PII, Defendant assumed legal and equitable duties and knew or  
26 should have known that it was responsible for protecting Plaintiff's and Class  
27 Members' PII from disclosure.  
28



1           ***The Data Breach***

2           31. On or about March 13, 2024, Defendant began sending Plaintiff and  
3 other victims of the Data Breach an untitled letter, informing them that:  
4

5           **What Happened?**

6           On November 9, 2023, we identified unusual activity in our network related to  
7 a third-party software provider. We immediately took steps to contain the  
8 activity and launched a full investigation of the incident. On November 29,  
9 2023, that investigation determined an unauthorized person accessed or  
acquired certain files from our network.

10           **What Information Was Involved?**

11           On February 23, 2024, we completed a manual review of the files that were  
12 involved, and determined that a file contained your name and Social Security  
number.<sup>4</sup>

13           32. Omitted from the Notice Letter were the date(s) of the Data Breach, the  
14 identity of the cybercriminals who perpetrated the cyber-attack, the details of the root  
15 cause of the Data Breach, the vulnerabilities exploited, why it took nearly an entire  
16 year from the day of the Data Breach to inform impacted individuals that their  
17 information was involved, and the remedial measures undertaken to ensure such a  
18 breach does not occur again. To date, these critical facts have not been explained or  
19 clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that  
20 their PII remains protected.  
21  
22  
23

24           33. This “disclosure” amounts to no real disclosure at all, as it fails to inform,  
25 with any degree of specificity, Plaintiff and Class Members of the Data Breach’s  
26

---

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

1 critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate  
2 the harms resulting from the Data Breach is severely diminished.

3  
4 34. Despite Defendant’s intentional opacity about the root cause of this  
5 incident, several facts may be gleaned from the Notice Letter, including: (a) that this  
6 Data Breach was the work of cybercriminals; (b) that the cybercriminals first  
7 infiltrated Defendant’s networks and systems, and downloaded data from the  
8 networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and  
9 (c) that once inside Defendant’s networks and systems, the cybercriminals targeted  
10 information including Plaintiff’s and Class Members’ Social Security numbers for  
11 download and theft.  
12  
13

14 35. Notably, companies only send notice letters because data breach  
15 notification laws require them to do so. And such letters are only sent to those persons  
16 who Defendant itself has a reasonable belief that such personal information was  
17 accessed or acquired by an unauthorized individual or entity. By sending notice  
18 letters to Plaintiff and Class Members, it admits that Defendant itself has a  
19 “reasonable belief” that Plaintiff’s and Class Members’ names and Social Security  
20 numbers were accessed or acquired by an “unknown actor” – aka cybercriminals.  
21  
22  
23

24 36. Moreover, in its Notice Letter, Defendant failed to specify whether it  
25 undertook any efforts to contact the approximate 12,000 Class Members whose data  
26 was accessed and acquired in the Data Breach to inquire whether any of the Class  
27 Members suffered misuse of their data or whether Defendant was interested in hearing  
28

1 about misuse of their data or set up a mechanism for Class Members to report misuse  
2 of their data.

3  
4 37. Defendant did not use reasonable security procedures and practices  
5 appropriate to the nature of the sensitive information they were maintaining for  
6 Plaintiff and Class Members, causing the exposure of PII, such as encrypting the  
7 information or deleting it when it is no longer needed.  
8

9 38. The attacker accessed and acquired files in Defendant's computer  
10 systems containing unencrypted PII of Plaintiff and Class Members, including their  
11 names and Social Security numbers. Plaintiff's and Class Members' PII was accessed  
12 and stolen in the Data Breach.  
13

14 39. Plaintiff further believes his PII, and that of Class Members, was  
15 subsequently sold on the dark web following the Data Breach, as that is the *modus*  
16 *operandi* of cybercriminals that commit cyber-attacks of this type.  
17

18 ***Data Breaches Are Preventable***

19  
20 40. To prevent and detect cyber-attacks and/or ransomware attacks,  
21 Defendant could and should have implemented, as recommended by the United States  
22 Government, the following measures:  
23

- 24 ● Implement an awareness and training program. Because end users are  
25 targets, employees and individuals should be aware of the threat of  
26 ransomware and how it is delivered.
- 27 ● Enable strong spam filters to prevent phishing emails from reaching the end  
28 users and authenticate inbound email using technologies like Sender Policy  
Framework (SPF), Domain Message Authentication Reporting and

1 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to  
2 prevent email spoofing.

- 3 ● Scan all incoming and outgoing emails to detect threats and filter executable  
4 files from reaching end users.
- 5 ● Configure firewalls to block access to known malicious IP addresses.
- 6 ● Patch operating systems, software, and firmware on devices. Consider using  
7 a centralized patch management system.
- 8 ● Set anti-virus and anti-malware programs to conduct regular scans  
9 automatically.
- 10 ● Manage the use of privileged accounts based on the principle of least  
11 privilege: no users should be assigned administrative access unless  
12 absolutely needed; and those with a need for administrator accounts should  
13 only use them when necessary.
- 14 ● Configure access controls—including file, directory, and network share  
15 permissions—with least privilege in mind. If a user only needs to read  
16 specific files, the user should not have write access to those files, directories,  
17 or shares.
- 18 ● Disable macro scripts from office files transmitted via email. Consider using  
19 Office Viewer software to open Microsoft Office files transmitted via email  
20 instead of full office suite applications.
- 21 ● Implement Software Restriction Policies (SRP) or other controls to prevent  
22 programs from executing from common ransomware locations, such as  
23 temporary folders supporting popular Internet browsers or  
24 compression/decompression programs, including the  
25 AppData/LocalAppData folder.
- 26 ● Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 27 ● Use application whitelisting, which only allows systems to execute programs  
28 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.<sup>5</sup>

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

**Secure internet-facing assets**

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

**Thoroughly investigate and remediate alerts**

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

**Include IT Pros in security discussions**

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

**Build credential hygiene**

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

**Apply principle of least-privilege**

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

---

<sup>5</sup> *Id.* at 3-4.

1           **Harden infrastructure**

- 2           - Use Windows Defender Firewall  
3           - Enable tamper protection  
4           - Enable cloud-delivered protection  
5           - Turn on attack surface reduction rules and [Antimalware Scan Interface]  
6           for Office[Visual Basic for Applications].<sup>6</sup>

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

10           43. The occurrence of the Data Breach indicates that Defendant failed to  
11 adequately implement one or more of the above measures to prevent cyberattacks,  
12 resulting in the Data Breach and the exposure of the PII of over 12,000 customers,<sup>7</sup>  
13 including that of Plaintiff and Class Members.  
14

15           ***Defendant Acquires, Collects, and Stores Its Customers' PII***

16           44. As a condition to obtain services from Defendant, Plaintiff and Class  
17 Members were required to give their sensitive and confidential PII to Defendant.  
18

19           45. Defendant retains and stores this information and derives a substantial  
20 economic benefit from the PII that it collects. But for the collection of Plaintiff's and  
21

22  
23  
24  
25           <sup>6</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*:  
26           <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

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

1 Class Members' PII, Defendant would be unable to perform its communication  
2 services.

3  
4 46. By obtaining, collecting, and storing the PII of Plaintiff and Class  
5 Members, Defendant assumed legal and equitable duties and knew or should have  
6 known that they were responsible for protecting the PII from disclosure.

7  
8 47. Plaintiff and Class Members have taken reasonable steps to maintain the  
9 confidentiality of their PII and relied on Defendant to keep their PII confidential and  
10 maintained securely, to use this information for business purposes only, and to make  
11 only authorized disclosures of this information.

12  
13 48. Defendant could have prevented this Data Breach by properly securing  
14 and encrypting the files and file servers containing the PII of Plaintiff and Class  
15 Members.

16  
17 49. Upon information and belief, Defendant made promises to Plaintiff and  
18 Class Members to maintain and protect their PII, demonstrating an understanding of  
19 the importance of securing PII.

20  
21 50. Indeed, Defendant provides on its website that:

22  
23 Information will be retained only for so long as reasonably necessary for the  
24 purposes set out above, in accordance with applicable laws.

25  
26 We maintain reasonable security measures to safeguard information from loss,  
27 theft interference, misuse, unauthorized access, disclosure, alteration, or  
28 data is reliable for its intended use and is accurate, complete, and current.<sup>8</sup>

---

<sup>8</sup> <https://www.teleflora.com/info/privacy-policy>

1  
2 ***Defendant Knew or Should Have Known of the Risk Because Floral***  
3 ***Companies in Possession of PII are Particularly Susceptible to Cyber***  
4 ***Attacks***

5 51. Data thieves regularly target companies like Defendant's due to the  
6 highly sensitive information that they custody. Defendant knew and understood that  
7 unprotected PII is valuable and highly sought after by criminal parties who seek to  
8 illegally monetize that PII through unauthorized access.  
9

10 52. Defendant's data security obligations were particularly important given  
11 the substantial increase in cyber-attacks and/or data breaches targeting floral  
12 companies that collect and store PII and other sensitive information, like Defendant,  
13 preceding the date of the breach.  
14

15 53. According to the *2023 Annual Data Breach Report*, the number of data  
16 compromises in 2023 (3,205) increased by 78 percentage points compared to 2022  
17 (1,801).<sup>9</sup> The ITRC set a new record for the number of data compromises tracked in  
18 a year, up 72 percentage points from the previous all-time high in 2021 (1,860).<sup>10</sup>  
19

20 54. In light of recent high profile data breaches at other industry leading  
21 companies, including T-Mobile, USA (37 million records, February-March 2023),  
22 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4  
23 million records, June 2023), NCB Management Services, Inc. (1 million records,  
24  
25  
26

27 \_\_\_\_\_  
28 <sup>9</sup> <https://www.idtheftcenter.org/publication/2023-data-breach-report/>

<sup>10</sup> *Id.*



1 February 2023), Defendant knew or should have known that the PII that it collected  
2 and maintained would be targeted by cybercriminals.

3  
4 55. Indeed, cyber-attacks, such as the one experienced by Defendant, have  
5 become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret  
6 Service have issued a warning to potential targets so they are aware of, and prepared  
7 for, a potential attack. As one report explained, smaller entities that store PII are  
8 “attractive to ransomware criminals...because they often have lesser IT defenses and  
9 a high incentive to regain access to their data quickly.”<sup>11</sup>

10  
11  
12 56. Additionally, as companies became more dependent on computer  
13 systems to run their business,<sup>12</sup> *e.g.*, working remotely as a result of the Covid-19  
14 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is  
15 magnified, thereby highlighting the need for adequate administrative, physical, and  
16 technical safeguards.<sup>13</sup>

17  
18 57. As a custodian of PII, Defendant knew, or should have known, the  
19 importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and  
20 of the foreseeable consequences if its data security systems were breached, including  
21 the significant costs imposed on Plaintiff and Class Members as a result of a breach.  
22  
23

24  
25 <sup>11</sup>[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](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)  
26 [n](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).

27 <sup>12</sup><https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

28 <sup>13</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

1           58. Despite the prevalence of public announcements of data breach and data  
2 security compromises, Defendant failed to take appropriate steps to protect the PII of  
3 Plaintiff and Class Members from being compromised.  
4

5           59. At all relevant times, Defendant knew, or reasonably should have known,  
6 of the importance of safeguarding the PII of Plaintiff and Class Members and of the  
7 foreseeable consequences that would occur if Defendant's data security system was  
8 breached, including, specifically, the significant costs that would be imposed on  
9 Plaintiff and Class Members as a result of a breach.  
10

11           60. Defendant was, or should have been, fully aware of the unique type and  
12 the significant volume of data on Defendant's server(s), amounting to more than  
13 twelve thousand individuals' detailed, PII, and, thus, the significant number of  
14 individuals who would be harmed by the exposure of the unencrypted data.  
15  
16

17           61. In the Notice Letter, Defendant makes an offer of 12 months of identity  
18 monitoring services. This is wholly inadequate to compensate Plaintiff and Class  
19 Members as it fails to provide for the fact victims of data breaches and other  
20 unauthorized disclosures commonly face multiple years of ongoing identity theft,  
21 financial fraud, and it entirely fails to provide sufficient compensation for the  
22 unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover,  
23 once this service expires, Plaintiff and Class Members will be forced to pay out of  
24 pocket for necessary identity monitoring services.  
25  
26  
27  
28

1           62. Defendant’s offering of credit and identity monitoring establishes that  
2 Plaintiff and Class Members’ sensitive PII *was* in fact affected, accessed,  
3 compromised, and exfiltrated from Defendant's computer systems.  
4

5           63. The injuries to Plaintiff and Class Members were directly and  
6 proximately caused by Defendant's failure to implement or maintain adequate data  
7 security measures for the PII of Plaintiff and Class Members.  
8

9           64. The ramifications of Defendant's failure to keep secure the PII of  
10 Plaintiff and Class Members are long lasting and severe. Once PII is stolen—  
11 particularly Social Security numbers—fraudulent use of that information and damage  
12 to victims may continue for years.  
13

14           65. As a floral company in possession of its customers’ and former  
15 customers’ PII, Defendant knew, or should have known, the importance of  
16 safeguarding the PII entrusted to them by Plaintiff and Class Members and of the  
17 foreseeable consequences if its data security systems were breached. This includes  
18 the significant costs imposed on Plaintiff and Class Members as a result of a breach.  
19 Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the  
20 Data Breach.  
21  
22  
23

24           ***Value of Personally Identifying Information***

25           66. The Federal Trade Commission (“FTC”) defines identity theft as “a  
26 fraud committed or attempted using the identifying information of another person  
27  
28

1 without authority.”<sup>14</sup> The FTC describes “identifying information” as “any name or  
2 number that may be used, alone or in conjunction with any other information, to  
3 identify a specific person,” including, among other things, “[n]ame, Social Security  
4 number, date of birth, official State or government issued driver’s license or  
5 identification number, alien registration number, government passport number,  
6 employer or taxpayer identification number.”<sup>15</sup>

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

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

20       69. According to the Social Security Administration, each time an  
21 individual’s Social Security number is compromised, “the potential for a thief to  
22

---

23 <sup>14</sup> 17 C.F.R. § 248.201 (2013).

24 <sup>15</sup> *Id.*

25 <sup>16</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.  
26 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).

27 <sup>17</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,  
28 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).

<sup>18</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

1 illegitimately gain access to bank accounts, credit cards, driving records, tax and  
2 employment histories and other private information increases.”<sup>19</sup> Moreover,  
3  
4 “[b]ecause many organizations still use SSNs as the primary identifier, exposure to  
5 identity theft and fraud remains.”<sup>20</sup>

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

9  
10         71. A dishonest person who has your Social Security number can use it to  
11 get other personal information about you. Identity thieves can use your number and  
12 your good credit to apply for more credit in your name. Then, they use the credit cards  
13 and don’t pay the bills, it damages your credit. You may not find out that someone is  
14 using your number until you’re turned down for credit, or you begin to get calls from  
15 unknown creditors demanding payment for items you never bought. Someone  
16 illegally using your Social Security number and assuming your identity can cause a  
17 lot of problems.<sup>21</sup>  
18  
19  
20  
21  
22  
23  
24

---

25 <sup>19</sup> See

26 <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

27 <sup>20</sup> *Id.*

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

1           72. In fact, “[a] stolen Social Security number is one of the leading causes  
2 of identity theft and can threaten your financial health.”<sup>22</sup> “Someone who has your  
3 SSN can use it to impersonate you, obtain credit and open bank accounts, apply for  
4 jobs, steal your tax refunds, get medical treatment, and steal your government  
5 benefits.”<sup>23</sup>  
6

7  
8           73. What’s more, it is no easy task to change or cancel a stolen Social  
9 Security number. An individual cannot obtain a new Social Security number without  
10 significant paperwork and evidence of actual misuse. In other words, preventive  
11 action to defend against the possibility of misuse of a Social Security number is not  
12 permitted; an individual must show evidence of actual, ongoing fraud activity to  
13 obtain a new number.  
14

15  
16           74. Even then, a new Social Security number may not be effective.  
17 According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit  
18 bureaus and banks are able to link the new number very quickly to the old number, so  
19 all of that old bad information is quickly inherited into the new Social Security  
20 number.”<sup>24</sup>  
21  
22  
23  
24

---

25 <sup>22</sup> See [https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)  
26 [number-identity-theft/](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)

27 <sup>23</sup> See <https://www.investopedia.com/terms/s/ssn.asp>

28 <sup>24</sup> 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>

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

17  
18  
19  
20  
21  
22           76. Similarly, the California state government warns consumers that:  
23 “[o]riginally, your Social Security number (SSN) was a way for the government to  
24 track your earnings and pay you retirement benefits. But over the years, it has become  
25 much more than that. It is the key to a lot of your personal information. With your  
26  
27  
28

1 name and SSN, an identity thief could open new credit and bank accounts, rent an  
2 apartment, or even get a job.”<sup>25</sup>

3  
4 77. Based on the foregoing, the information compromised in the Data Breach  
5 is significantly more valuable than the loss of, for example, credit card information in  
6 a retailer data breach because, there, victims can cancel or close credit and debit card  
7 accounts. The information compromised in this Data Breach is impossible to “close”  
8 and difficult, if not impossible, to change—Social Security number and name.

9  
10 78. This data demands a much higher price on the black market. Martin  
11 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit  
12 card information, personally identifiable information and Social Security numbers are  
13 worth more than 10x on the black market.”<sup>26</sup>

14  
15  
16 79. Among other forms of fraud, identity thieves may obtain driver’s  
17 licenses, government benefits, medical services, and housing or even give false  
18 information to police.

19  
20 80. The fraudulent activity resulting from the Data Breach may not come to  
21 light for years. There may be a time lag between when harm occurs versus when it is  
22 discovered, and also between when PII is stolen and when it is used. According to the  
23

24  
25  
26 <sup>25</sup> See <https://oag.ca.gov/idtheft/facts/your-ssn>

27 <sup>26</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
28 *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).



1 U.S. Government Accountability Office (“GAO”), which conducted a study regarding  
2 data breaches:

3  
4 [L]aw enforcement officials told us that in some cases, stolen data may be held  
5 for up to a year or more before being used to commit identity theft. Further,  
6 once stolen data have been sold or posted on the Web, fraudulent use of that  
7 information may continue for years. As a result, studies that attempt to measure  
8 the harm resulting from data breaches cannot necessarily rule out all future  
9 harm.<sup>27</sup>

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

14 ***Defendant Fails to Comply with FTC Guidelines***

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

19 83. In 2016, the FTC updated its publication, Protecting Personal  
20 Information: A Guide for Business, which established cyber-security guidelines for  
21 businesses. These guidelines note that businesses should protect the personal  
22 customer information that they keep; properly dispose of personal information that is  
23  
24  
25  
26  
27

28 <sup>27</sup> *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).

1 no longer needed; encrypt information stored on computer networks; understand their  
2 network's vulnerabilities; and implement policies to correct any security problems.<sup>28</sup>  
3

4 84. The guidelines also recommend that businesses use an intrusion  
5 detection system to expose a breach as soon as it occurs; monitor all incoming traffic  
6 for activity indicating someone is attempting to hack the system; watch for large  
7 amounts of data being transmitted from the system; and have a response plan ready  
8 in the event of a breach.<sup>29</sup>  
9

10 85. The FTC further recommends that companies not maintain PII longer  
11 than is needed for authorization of a transaction; limit access to sensitive data; require  
12 complex passwords to be used on networks; use industry-tested methods for security;  
13 monitor for suspicious activity on the network; and verify that third-party service  
14 providers have implemented reasonable security measures.  
15  
16

17 86. The FTC has brought enforcement actions against businesses for failing  
18 to adequately and reasonably protect customer data, treating the failure to employ  
19 reasonable and appropriate measures to protect against unauthorized access to  
20 confidential consumer data as an unfair act or practice prohibited by Section 5 of the  
21 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from  
22  
23  
24  
25  
26

---

27 <sup>28</sup> *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-  
28 personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

<sup>29</sup> *Id.*

1 these actions further clarify the measures businesses must take to meet their data  
2 security obligations.

3  
4 87. These FTC enforcement actions include actions against floral  
5 companies, like Defendant.

6  
7 88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices  
8 in or affecting commerce,” including, as interpreted and enforced by the FTC, the  
9 unfair act or practice by businesses, such as Defendant, of failing to use reasonable  
10 measures to protect PII. The FTC publications and orders described above also form  
11 part of the basis of Defendant’s duty in this regard.

12  
13 89. Defendant failed to properly implement basic data security practices.

14  
15 90. Defendant’s failure to employ reasonable and appropriate measures to  
16 protect against unauthorized access to customers’ PII or to comply with applicable  
17 industry standards constitutes an unfair act or practice prohibited by Section 5 of the  
18 FTC Act, 15 U.S.C. § 45.

19  
20 91. Upon information and belief, Defendant was at all times fully aware of  
21 its obligation to protect the PII of its customers, Defendant was also aware of the  
22 significant repercussions that would result from its failure to do so. Accordingly,  
23 Defendant’s conduct was particularly unreasonable given the nature and amount of  
24 PII it obtained and stored and the foreseeable consequences of the immense damages  
25 that would result to Plaintiff and the Class.  
26  
27  
28

1           ***Defendant Fails to Comply with Industry Standards***

2           92. As noted above, experts studying cyber security routinely identify  
3 entities in possession of PII as being particularly vulnerable to cyberattacks because  
4 of the value of the PII which they collect and maintain.  
5

6           93. Several best practices have been identified that, at a minimum, should be  
7 implemented by floral companies in possession of PII, like Defendant, including but  
8 not limited to: educating all employees; strong passwords; multi-layer security,  
9 including firewalls, anti-virus, and anti-malware software; encryption, making data  
10 unreadable without a key; multi-factor authentication; backup data and limiting which  
11 employees can access sensitive data. Defendant failed to follow these industry best  
12 practices, including a failure to implement multi-factor authentication.  
13  
14

15           94. Other best cybersecurity practices that are standard in the floral industry  
16 include installing appropriate malware detection software; monitoring and limiting  
17 the network ports; protecting web browsers and email management systems; setting  
18 up network systems such as firewalls, switches and routers; monitoring and protection  
19 of physical security systems; protection against any possible communication system;  
20 training staff regarding critical points. Defendant failed to follow these cybersecurity  
21 best practices, including failure to train staff.  
22  
23

24           95. Defendant failed to meet the minimum standards of any of the following  
25 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
26 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,  
27  
28

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,  
2 and RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS  
3 CSC), which are all established standards in reasonable cybersecurity readiness.  
4

5 96. These foregoing frameworks are existing and applicable industry  
6 standards in the floral industry, and upon information and belief, Defendant failed to  
7 comply with at least one—or all—of these accepted standards, thereby opening the  
8 door to the threat actor and causing the Data Breach.  
9

10 ***Common Injuries & Damages***  
11

12 97. As a result of Defendant’s ineffective and inadequate data security  
13 practices, the Data Breach, and the foreseeable consequences of PII ending up in the  
14 possession of criminals, the risk of identity theft to the Plaintiff and Class Members  
15 has materialized and is imminent, and Plaintiff and Class Members have all sustained  
16 actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII;  
17 (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated  
18 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of  
19 benefit of the bargain; (vi) lost opportunity costs associated with attempting to  
20 mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii)  
21 nominal damages; and (ix) the continued and certainly increased risk to their PII,  
22 which: (a) remains unencrypted and available for unauthorized third parties to access  
23 and abuse; and (b) remains backed up in Defendant’s possession and is subject to  
24  
25  
26  
27  
28

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

3  
4 ***The Data Breach Increases Victims' Risk of Identity Theft***

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

7  
8 99. Unencrypted PII may also fall into the hands of companies that will use  
9 the detailed PII for targeted marketing without the approval of Plaintiff and Class  
10 Members. Simply, unauthorized individuals can easily access the PII of Plaintiff and  
11 Class Members.

12  
13 100. The link between a data breach and the risk of identity theft is simple and  
14 well established. Criminals acquire and steal PII to monetize the information.  
15 Criminals monetize the data by selling the stolen information on the black market to  
16 other criminals who then utilize the information to commit a variety of identity theft  
17 related crimes discussed below.

18  
19  
20 101. Plaintiff's and Class Members' PII is of great value to hackers and cyber  
21 criminals, and the data stolen in the Data Breach has been used and will continue to  
22 be used in a variety of sordid ways for criminals to exploit Plaintiff and Class  
23 Members and to profit off their misfortune.

24  
25 102. Due to the risk of one's Social Security number being exposed, state  
26 legislatures have passed laws in recognition of the risk: "[t]he social security number  
27 can be used as a tool to perpetuate fraud against a person and to acquire sensitive  
28

1 personal, financial, medical, and familial information, the release of which could  
2 cause great financial or personal harm to an individual. While the social security  
3 number was intended to be used solely for the administration of the federal Social  
4 Security System, over time this unique numeric identifier has been used extensively  
5 for identity verification purposes[.]”<sup>30</sup>  
6

7  
8 103. Moreover, “SSNs have been central to the American identity  
9 infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes  
10 have also had SSNs baked into their identification process for years. In fact, SSNs  
11 have been the gold standard for identifying and verifying the credit history of  
12 prospective customers.”<sup>31</sup>  
13

14 104. “Despite the risk of fraud associated with the theft of Social Security  
15 numbers, just five of the nation’s largest 25 banks have stopped using the numbers to  
16 verify a customer’s identity after the initial account setup[.]”<sup>32</sup> Accordingly, since  
17 Social Security numbers are frequently used to verify an individual’s identity after  
18 logging onto an account or attempting a transaction, “[h]aving access to your Social  
19 Security number may be enough to help a thief steal money from your bank account”<sup>33</sup>  
20  
21  
22  
23

---

24 <sup>30</sup> See N.C. Gen. Stat. § 132-1.10(1).

25 <sup>31</sup> See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

26 <sup>32</sup> See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

27 <sup>33</sup> See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>  
28

1           105. One such example of criminals piecing together bits and pieces of  
2 compromised Private Information for profit is the development of “Fullz” packages.<sup>34</sup>  
3

4           106. With “Fullz” packages, cyber-criminals can cross-reference two sources  
5 of Private Information to marry unregulated data available elsewhere to criminally  
6 stolen data with an astonishingly complete scope and degree of accuracy in order to  
7 assemble complete dossiers on individuals.  
8

9           107. The development of “Fullz” packages means here that the stolen Private  
10 Information from the Data Breach can easily be used to link and identify it to  
11 Plaintiff’s and Class Members’ phone numbers, email addresses, and other  
12 unregulated sources and identifiers. In other words, even if certain information such  
13 as emails, phone numbers, or credit card numbers may not be included in the Private  
14 Information that was exfiltrated in the Data Breach, criminals may still easily create  
15  
16  
17  
18  
19

---

20 <sup>34</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not  
21 limited to, the name, address, credit card information, social security number, date of birth, and  
22 more. As a rule of thumb, the more information you have on a victim, the more money that can be  
23 made off of those credentials. Fullz are usually pricier than standard credit card credentials,  
24 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning  
25 credentials into money) in various ways, including performing bank transactions over the phone  
26 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials  
27 associated with credit cards that are no longer valid, can still be used for numerous purposes,  
28 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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-  
life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-  
stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)



1 a Fullz package and sell it at a higher price to unscrupulous operators and criminals  
2 (such as illegal and scam telemarketers) over and over.  
3

4 108. The existence and prevalence of “Fullz” packages means that the Private  
5 Information stolen from the data breach can easily be linked to the unregulated data  
6 (like insurance information) of Plaintiff and the other Class Members.  
7

8 109. Thus, even if certain information (such as insurance information) was  
9 not stolen in the data breach, criminals can still easily create a comprehensive “Fullz”  
10 package.  
11

12 110. Then, this comprehensive dossier can be sold—and then resold in  
13 perpetuity—to crooked operators and other criminals (like illegal and scam  
14 telemarketers).  
15

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

17 111. As a result of the recognized risk of identity theft, when a Data Breach  
18 occurs, and an individual is notified by a company that their PII was compromised,  
19 as in this Data Breach, the reasonable person is expected to take steps and spend time  
20 to address the dangerous situation, learn about the breach, and otherwise mitigate the  
21 risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps  
22 to review accounts or credit reports could expose the individual to greater financial  
23 harm – yet, the resource and asset of time has been lost.  
24  
25

26 112. Thus, due to the actual and continuing risk of identity theft, Defendant,  
27 in its Notice Letter, encourages Plaintiff and Class Members to take the following  
28

1 measures to protect themselves: “be vigilant for incidents of fraud or identity theft by  
2 reviewing your account statements and free credit reports for any unauthorized  
3 activity.”<sup>35</sup>  
4

5 113. In addition, Defendant’s Notice letter includes a full page detailing how  
6 to sign up for the credit monitoring services offered by Defendant as well as two full  
7 pages devoted to “Additional Steps You Can Take” that recommend Plaintiff and  
8 Class Members to partake in activities such as placing fraud alerts on their accounts,  
9 putting a freeze on their credit, and contacting government agencies for more  
10 information.<sup>36</sup>  
11  
12

13 114. Defendant’s extensive suggestion of steps that Plaintiff and Class  
14 Members must take in order to protect themselves from identity theft and/or fraud  
15 demonstrates the significant time that Plaintiffs and Class Members must undertake  
16 in response to the Data Breach. Plaintiff’s and Class Members’ time is highly valuable  
17 and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury  
18 and damages in the form of lost time that they spent on mitigation activities in  
19 response to the Data Breach and at the direction of Defendant’s Notice Letter.  
20  
21

22 115. Plaintiff and Class Members have spent, and will spend additional time  
23 in the future, on a variety of prudent actions, such as researching and verifying the  
24  
25  
26

---

27 <sup>35</sup> Notice Etter.

28 <sup>36</sup> *Id.*

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

3  
4 116. Plaintiff’s mitigation efforts are consistent with the U.S. Government  
5 Accountability Office that released a report in 2007 regarding data breaches (“GAO  
6 Report”) in which it noted that victims of identity theft will face “substantial costs  
7 and time to repair the damage to their good name and credit record.”<sup>37</sup>  
8

9 117. Plaintiff’s mitigation efforts are also consistent with the steps that FTC  
10 recommends that data breach victims take several steps to protect their personal and  
11 financial information after a data breach, including: contacting one of the credit  
12 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven  
13 years if someone steals their identity), reviewing their credit reports, contacting  
14 companies to remove fraudulent charges from their accounts, placing a credit freeze  
15 on their credit, and correcting their credit reports.<sup>38</sup>  
16  
17

18 118. And for those Class Members who experience actual identity theft and  
19 fraud, the United States Government Accountability Office released a report in 2007  
20 regarding data breaches (“GAO Report”) in which it noted that victims of identity  
21 theft will face “substantial costs and time to repair the damage to their good name and  
22 credit record.”<sup>[4]</sup>  
23  
24

25  
26 <sup>37</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data  
27 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full  
Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

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

### *Diminution Of Value Of PII*

119. PII is a valuable property right.<sup>39</sup> 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.

120. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>40</sup>

121. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>41</sup> 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.<sup>42,43</sup> Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>44</sup>

---

<sup>39</sup> 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”).

<sup>40</sup> 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).

<sup>41</sup> 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).

<sup>42</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>43</sup> <https://datacoup.com/>

<sup>44</sup> <https://digi.me/what-is-digime/>

1           122. As a result of the Data Breach, Plaintiff's and Class Members' PII, which  
2 has an inherent market value in both legitimate and dark markets, has been damaged  
3 and diminished by its compromise and unauthorized release. However, this transfer  
4 of value occurred without any consideration paid to Plaintiff or Class Members for  
5 their property, resulting in an economic loss. Moreover, the PII is now readily  
6 available, and the rarity of the Data has been lost, thereby causing additional loss of  
7 value.  
8

9  
10           123. At all relevant times, Defendant knew, or reasonably should have known,  
11 of the importance of safeguarding the PII of Plaintiff and Class Members, and of the  
12 foreseeable consequences that would occur if Defendant's data security system was  
13 breached, including, specifically, the significant costs that would be imposed on  
14 Plaintiff and Class Members as a result of a breach.  
15

16  
17           124. The fraudulent activity resulting from the Data Breach may not come to  
18 light for years.  
19

20           125. Plaintiff and Class Members now face years of constant surveillance of  
21 their financial and personal records, monitoring, and loss of rights. The Class is  
22 incurring and will continue to incur such damages in addition to any fraudulent use  
23 of their PII .  
24

25           126. Defendant was, or should have been, fully aware of the unique type and  
26 the significant volume of data on Defendant's network, amounting to more than  
27  
28

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

3  
4 127. The injuries to Plaintiff and Class Members were directly and  
5 proximately caused by Defendant's failure to implement or maintain adequate data  
6 security measures for the PII of Plaintiff and Class Members.

7  
8 ***Future Costs of Credit and Identity Theft Monitoring***  
9 ***is Reasonable and Necessary***

10 128. Given the type of targeted attack, the sophisticated criminal activity, and  
11 the type of PII involved in this case, there is a strong probability that entire batches of  
12 stolen information have been placed, or will be placed, on the black market/dark web  
13 for sale and purchase by criminals intending to utilize the PII for identity theft crimes  
14 –e.g., opening bank accounts in the victims' names to make purchases or to launder  
15 money; file false tax returns; take out loans or lines of credit; or file false  
16 unemployment claims.  
17

18  
19 129. Such fraud may go undetected until debt collection calls commence  
20 months, or even years, later. An individual may not know that his or her PII was used  
21 to file for unemployment benefits until law enforcement notifies the individual's  
22 employer of the suspected fraud. Fraudulent tax returns are typically discovered only  
23 when an individual's authentic tax return is rejected.  
24

25  
26 130. Consequently, Plaintiff and Class Members are at an increased risk of  
27 fraud and identity theft for many years into the future.  
28

1 131. The retail cost of credit monitoring and identity theft monitoring can cost  
2 around \$200 a year per Class Member. This is reasonable and necessary cost to  
3 monitor to protect Class Members from the risk of identity theft that arose from  
4 Defendant's Data Breach.  
5

6 ***Loss of Benefit of the Bargain***  
7

8 132. Furthermore, Defendant's poor data security deprived Plaintiff and  
9 Class Members of the benefit of their bargain. When agreeing to pay Defendant for  
10 services, Plaintiff and other reasonable consumers understood and expected that  
11 they were, in part, paying for the service and necessary data security to protect the  
12 PII, when in fact, Defendant did not provide the expected data security.  
13 Accordingly, Plaintiff and Class Members received services that were of a lesser  
14 value than what they reasonably expected to receive under the bargains they struck  
15 with Defendant.  
16  
17

18 **PLAINTIFF CUMMINGS' EXPERIENCE**  
19

20 133. Plaintiff Cummings owns and operates a company that contracts with  
21 Defendant for services.  
22

23 134. As a condition of receiving services at Defendant, he was required to  
24 provide Defendant with his sensitive PII, including his name and Social Security  
25 number.  
26

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

1           136. Plaintiff Cummings is very careful about sharing his sensitive PII.  
2 Plaintiff stores any documents containing his PII in a safe and secure location. He has  
3 never knowingly transmitted unencrypted sensitive PII over the internet or any other  
4 unsecured source.  
5

6           137. Plaintiff Cummings received the Notice Letter, by U.S. mail, directly  
7 from Defendant, dated March 14, 2024. According to the Notice Letter, Plaintiff’s PII  
8 was improperly accessed and obtained by unauthorized third parties, including his  
9 name and Social Security number.  
10

11           138. As a result of the Data Breach, and at the direction of Defendant’s Notice  
12 Letter, which instructs Plaintiff to “be vigilant for incidents of fraud or identity theft  
13 by reviewing your account statements and free credit reports for any unauthorized  
14 activity[,]”<sup>45</sup> Plaintiff made reasonable efforts to mitigate the impact of the Data  
15 Breach, including researching and verifying the legitimacy of the Data Breach and  
16 monitoring his financial accounts for any indication of fraudulent activity, which may  
17 take years to detect. Plaintiff has spent significant time dealing with the Data Breach,  
18 valuable time Plaintiff otherwise would have spent on other activities, including but  
19 not limited to work and/or recreation. This time has been lost forever and cannot be  
20 recaptured.  
21  
22  
23  
24  
25  
26  
27

---

28 <sup>45</sup> Notice Letter.



1           139. Plaintiff suffered actual injury from having his PII compromised as a  
2 result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii)  
3 theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity  
4 costs associated with attempting to mitigate the actual consequences of the Data  
5 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with  
6 attempting to mitigate the actual consequences of the Data Breach; (vii) statutory  
7 damages; (viii) nominal damages; and (ix) the continued and certainly increased risk  
8 to his PII, which: (a) remains unencrypted and available for unauthorized third parties  
9 to access and abuse; and (b) remains backed up in Defendant's possession and is  
10 subject to further unauthorized disclosures so long as Defendant fails to undertake  
11 appropriate and adequate measures to protect the PII.  
12

13  
14  
15           140. Plaintiff further suffered actual injury in the form of fraudulent charges  
16 placed on his M&T Bank debit card, totaling more than \$1,000, in or about November  
17 2023 through March 2024, which, upon information and belief, was caused by the  
18 Data Breach.  
19  
20

21           141. Plaintiff additionally suffered actual injury in the form of experiencing  
22 an increase in spam calls, texts, and/or emails, which, upon information and belief,  
23 was caused by the Data Breach.  
24

25           142. These misuses of his PII was caused, upon information and belief, by the  
26 fact that cybercriminals are able to easily use the information compromised in the  
27 Data Breach to find more information about an individual, such as their phone number  
28

1 or email address, from publicly available sources, including websites that aggregate  
2 and associate personal information with the owner of such information.

3  
4 143. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress,  
5 which has been compounded by the fact that Defendant has still not fully informed  
6 him of key details about the Data Breach's occurrence.

7  
8 144. As a result of the Data Breach, Plaintiff anticipates spending  
9 considerable time and money on an ongoing basis to try to mitigate and address harms  
10 caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk  
11 and will continue to be at increased risk of identity theft and fraud for years to come.

12  
13 145. Plaintiff Cummings has a continuing interest in ensuring that his PII,  
14 which, upon information and belief, remain backed up in Defendant's possession, is  
15 protected and safeguarded from future breaches.

16  
17 **CLASS ACTION ALLEGATIONS**

18  
19 146. Plaintiff brings this nationwide class action on behalf of himself and on  
20 behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4)  
21 of the Federal Rules of Civil Procedure.

22  
23 147. The Class that Plaintiff seeks to represent is defined as follows:

24 **Nationwide Class**

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

1 148. Excluded from the Class are the following individuals and/or entities:  
2 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and  
3 any entity in which Defendant have a controlling interest; all individuals who make a  
4 timely election to be excluded from this proceeding using the correct protocol for  
5 opting out; and all judges assigned to hear any aspect of this litigation, as well as their  
6 immediate family members.  
7  
8

9 149. Plaintiff reserves the right to amend the definition of the Class or add a  
10 Class or Subclass if further information and discovery indicate that the definitions of  
11 the Class should be narrowed, expanded, or otherwise modified.  
12

13 150. **Numerosity:** The members of the Class are so numerous that joinder of  
14 all members is impracticable, if not completely impossible. At least 12,000  
15 individuals were notified by Defendant of the Data Breach, according to the breach  
16 report submitted to Maine Attorney General's Office.<sup>46</sup> The Class is apparently  
17 identifiable within Defendant's records, and Defendant has already identified these  
18 individuals (as evidenced by sending them breach notification letters).  
19  
20

21 151. Common questions of law and fact exist as to all members of the Class  
22 and predominate over any questions affecting solely individual members of the Class.  
23 Among the questions of law and fact common to the Class that predominate over  
24 questions which may affect individual Class members, including the following:  
25  
26  
27

28 <sup>46</sup> <https://apps.web.maine.gov/online/aewiewer/ME/40/0e58cbaf-cc13-4651-9595-3f508d6e7260.shtml>

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

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

1 k. Whether Plaintiff and Class Members are entitled to injunctive relief to  
2 redress the imminent and currently ongoing harm faced as a result of the  
3 Data Breach.  
4

5 152. **Typicality:** Plaintiff's claims are typical of those of the other members  
6 of the Class because Plaintiff, like every other Class Member, was exposed to virtually  
7 identical conduct and now suffers from the same violations of the law as each other  
8 member of the Class.  
9

10 153. **Policies Generally Applicable to the Class:** This class action is also  
11 appropriate for certification because Defendant acted or refused to act on grounds  
12 generally applicable to the Class, thereby requiring the Court's imposition of uniform  
13 relief to ensure compatible standards of conduct toward the Class Members and  
14 making final injunctive relief appropriate with respect to the Class as a whole.  
15 Defendant's policies challenged herein apply to and affect Class Members uniformly  
16 and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect  
17 to the Class as a whole, not on facts or law applicable only to Plaintiff.  
18  
19  
20

21 154. **Adequacy:** Plaintiff will fairly and adequately represent and protect the  
22 interests of the Class Members in that he has no disabling conflicts of interest that  
23 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief  
24 that is antagonistic or adverse to the Class Members and the infringement of the rights  
25 and the damages he has suffered are typical of other Class Members. Plaintiff has  
26  
27  
28

1 retained counsel experienced in complex class action and data breach litigation, and  
2 Plaintiff intends to prosecute this action vigorously.  
3

4       **155. Superiority and Manageability:** The class litigation is an appropriate  
5 method for fair and efficient adjudication of the claims involved. Class action  
6 treatment is superior to all other available methods for the fair and efficient  
7 adjudication of the controversy alleged herein; it will permit a large number of Class  
8 Members to prosecute their common claims in a single forum simultaneously,  
9 efficiently, and without the unnecessary duplication of evidence, effort, and expense  
10 that hundreds of individual actions would require. Class action treatment will permit  
11 the adjudication of relatively modest claims by certain Class Members, who could not  
12 individually afford to litigate a complex claim against large corporations, like  
13 Defendant. Further, even for those Class Members who could afford to litigate such a  
14 claim, it would still be economically impractical and impose a burden on the courts.  
15  
16  
17  
18

19       **156.** The nature of this action and the nature of laws available to Plaintiff and  
20 Class Members make the use of the class action device a particularly efficient and  
21 appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs  
22 alleged because Defendant would necessarily gain an unconscionable advantage since  
23 they would be able to exploit and overwhelm the limited resources of each individual  
24 Class Member with superior financial and legal resources; the costs of individual suits  
25 could unreasonably consume the amounts that would be recovered; proof of a  
26 common course of conduct to which Plaintiff was exposed is representative of that  
27  
28

1 experienced by the Class and will establish the right of each Class Member to recover  
2 on the cause of action alleged; and individual actions would create a risk of  
3 inconsistent results and would be unnecessary and duplicative of this litigation.  
4

5 157. The litigation of the claims brought herein is manageable. Defendant's  
6 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable  
7 identities of Class Members demonstrates that there would be no significant  
8 manageability problems with prosecuting this lawsuit as a class action.  
9

10 158. Adequate notice can be given to Class Members directly using  
11 information maintained in Defendant's records.  
12

13 159. Unless a Class-wide injunction is issued, Defendant may continue in its  
14 failure to properly secure the PII of Class Members, Defendant may continue to refuse  
15 to provide proper notification to Class Members regarding the Data Breach, and  
16 Defendant may continue to act unlawfully as set forth in this Complaint.  
17

18 160. Further, Defendant has acted on grounds that apply generally to the Class  
19 as a whole, so that class certification, injunctive relief, and corresponding declaratory  
20 relief are appropriate on a class- wide basis.  
21

22 161. Likewise, particular issues under Rule 42(d)(1) are appropriate for  
23 certification because such claims present only particular, common issues, the  
24 resolution of which would advance the disposition of this matter and the parties'  
25 interests therein. Such particular issues include, but are not limited to:  
26  
27  
28

- 1 a. Whether Defendant failed to timely notify the Plaintiff and the class of the  
2 Data Breach;
- 3
- 4 b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise  
5 due care in collecting, storing, and safeguarding their PII;
- 6
- 7 c. Whether Defendant's security measures to protect their data systems were  
8 reasonable in light of best practices recommended by data security experts;
- 9
- 10 d. Whether Defendant's failure to institute adequate protective security  
11 measures amounted to negligence;
- 12
- 13 e. Whether Defendant failed to take commercially reasonable steps to  
14 safeguard consumer PII; and Whether adherence to FTC data security  
15 recommendations, and measures recommended by data security experts  
16 would have reasonably prevented the Data Breach.

17 **COUNT I**  
18 **Negligence**  
19 **(On Behalf of Plaintiff and the Class)**

20 162. Plaintiff incorporates the foregoing allegations as though fully set forth  
21 herein.

22 163. Defendant requires its customers, including Plaintiff and Class  
23 Members, to submit non-public Private Information in the ordinary course of  
24 providing its services.  
25  
26  
27  
28



1           164. Defendant gathered and stored the Private Information of Plaintiff and  
2 Class Members as part of its business of soliciting its services to its customers, which  
3 solicitations and services affect commerce.  
4

5           165. Plaintiff and Class Members entrusted Defendant with their Private  
6 Information with the understanding that Defendant would safeguard their  
7 information.  
8

9           166. Defendant had full knowledge of the sensitivity of the Private  
10 Information and the types of harm that Plaintiff and Class Members could and would  
11 suffer if the Private Information were wrongfully disclosed.  
12

13           167. By voluntarily undertaking and assuming the responsibility to collect and  
14 store this data, and in fact doing so, and sharing it and using it for commercial gain,  
15 Defendant had a duty of care to use reasonable means to secure and safeguard their  
16 computer property—and Class Members’ Private Information held within it—to  
17 prevent disclosure of the information, and to safeguard the information from theft.  
18 Defendant’s duty included a responsibility to implement processes by which they  
19 could detect a breach of its security systems in a reasonably expeditious period of  
20 time and to give prompt notice to those affected in the case of a data breach.  
21  
22  
23

24           168. Defendant had a duty to employ reasonable security measures under  
25 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits  
26 “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced  
27  
28

1 by the FTC, the unfair practice of failing to use reasonable measures to protect  
2 confidential data.

3  
4 169. Defendant owed a duty of care to Plaintiff and Class Members to provide  
5 data security consistent with industry standards and other requirements discussed  
6 herein, and to ensure that its systems and networks adequately protected the Private  
7 Information.

8  
9 170. Defendant's duty of care to use reasonable security measures arose as a  
10 result of the special relationship that existed between Defendant and Plaintiff and  
11 Class Members. That special relationship arose because Plaintiff and the Class  
12 entrusted Defendant with their confidential Private Information, a necessary part of  
13 being customers at Defendant.

14  
15 171. Defendant's duty to use reasonable care in protecting confidential data  
16 arose not only as a result of the statutes and regulations described above, but also  
17 because Defendant is bound by industry standards to protect confidential Private  
18 Information.

19  
20 172. Defendant was subject to an "independent duty," untethered to any  
21 contract between Defendant and Plaintiff or the Class.

22  
23 173. Defendant also had a duty to exercise appropriate clearinghouse  
24 practices to remove former customers' Private Information it was no longer required  
25 to retain pursuant to regulations.  
26  
27  
28

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

3  
4 175. Defendant had and continues to have a duty to adequately disclose that  
5 the Private Information of Plaintiff and the Class within Defendant's possession might  
6 have been compromised, how it was compromised, and precisely the types of data  
7 that were compromised and when. Such notice was necessary to allow Plaintiff and  
8 the Class to take steps to prevent, mitigate, and repair any identity theft and the  
9 fraudulent use of their Private Information by third parties.  
10

11  
12 176. Defendant breached its duties, pursuant to the FTC Act and other  
13 applicable standards, and thus was negligent, by failing to use reasonable measures to  
14 protect Class Members' Private Information. The specific negligent acts and  
15 omissions committed by Defendant include, but are not limited to, the following:  
16

- 17 a. Failing to adopt, implement, and maintain adequate security measures to  
18 safeguard Class Members' Private Information;  
19  
20 b. Failing to adequately monitor the security of their networks and systems;  
21  
22 c. Allowing unauthorized access to Class Members' Private Information;  
23  
24 d. Failing to detect in a timely manner that Class Members' Private  
25 Information had been compromised;  
26  
27 e. Failing to remove former customers' Private Information it was no  
28 longer required to retain pursuant to regulations, and

1 f. Failing to timely and adequately notify Class Members about the Data  
2 Breach's occurrence and scope, so that they could take appropriate steps  
3 to mitigate the potential for identity theft and other damages.  
4

5 177. Defendant violated Section 5 of the FTC Act by failing to use reasonable  
6 measures to protect Private Information and not complying with applicable industry  
7 standards, as described in detail herein. Defendant's conduct was particularly  
8 unreasonable given the nature and amount of Private Information it obtained and  
9 stored and the foreseeable consequences of the immense damages that would result  
10 to Plaintiff and the Class.  
11  
12

13 178. Plaintiff and Class Members were within the class of persons the Federal  
14 Trade Commission Act was intended to protect and the type of harm that resulted  
15 from the Data Breach was the type of harm that the statute was intended to guard  
16 against.  
17

18 179. Defendant's violation of Section 5 of the FTC Act constitutes  
19 negligence.  
20

21 180. The FTC has pursued enforcement actions against businesses, which, as  
22 a result of their failure to employ reasonable data security measures and avoid unfair  
23 and deceptive practices, caused the same harm as that suffered by Plaintiff and the  
24 Class.  
25  
26  
27  
28

1 181. A breach of security, unauthorized access, and resulting injury to  
2 Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's  
3 inadequate security practices.  
4

5 182. It was foreseeable that Defendant's failure to use reasonable measures to  
6 protect Class Members' Private Information would result in injury to Class Members.  
7 Further, the breach of security was reasonably foreseeable given the known high  
8 frequency of cyberattacks and data breaches in the floral industry.  
9

10 183. Defendant has full knowledge of the sensitivity of the Private  
11 Information and the types of harm that Plaintiff and the Class could and would suffer  
12 if the Private Information were wrongfully disclosed.  
13

14 184. Plaintiff and the Class were the foreseeable and probable victims of any  
15 inadequate security practices and procedures. Defendant knew or should have known  
16 of the inherent risks in collecting and storing the Private Information of Plaintiff and  
17 the Class, the critical importance of providing adequate security of that Private  
18 Information, and the necessity for encrypting Private Information stored on  
19 Defendant's systems or transmitted through third party systems.  
20  
21

22 185. It was therefore foreseeable that the failure to adequately safeguard Class  
23 Members' Private Information would result in one or more types of injuries to Class  
24 Members.  
25

26 186. Plaintiff and the Class had no ability to protect their Private Information  
27 that was in, and possibly remains in, Defendant's possession.  
28

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

3  
4           188. Defendant's duty extended to protecting Plaintiff and the Class from the  
5 risk of foreseeable criminal conduct of third parties, which has been recognized in  
6 situations where the actor's own conduct or misconduct exposes another to the risk or  
7 defeats protections put in place to guard against the risk, or where the parties are in a  
8 special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and  
9 legislatures have also recognized the existence of a specific duty to reasonably  
10 safeguard personal information.  
11

12  
13           189. Defendant has admitted that the Private Information of Plaintiff and the  
14 Class was wrongfully lost and disclosed to unauthorized third persons as a result of  
15 the Data Breach.  
16

17           190. But for Defendant's wrongful and negligent breach of duties owed to  
18 Plaintiff and the Class, the Private Information of Plaintiff and the Class would not  
19 have been compromised.  
20

21           191. There is a close causal connection between Defendant's failure to  
22 implement security measures to protect the Private Information of Plaintiff and the  
23 Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The  
24 Private Information of Plaintiff and the Class was lost and accessed as the proximate  
25 result of Defendant's failure to exercise reasonable care in safeguarding such Private  
26  
27  
28

1 Information by adopting, implementing, and maintaining appropriate security  
2 measures.

3  
4 192. As a direct and proximate result of Defendant's negligence, Plaintiff and  
5 the Class have suffered and will suffer injury, including but not limited to: (i) invasion  
6 of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and  
7 opportunity costs associated with attempting to mitigate the actual consequences of  
8 the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs  
9 associated with attempting to mitigate the actual consequences of the Data Breach;  
10 (vii) statutory damages; (viii) actual misuse of the compromised data consisting of an  
11 increase in spam calls, texts, and/or emails; (ix) actual misuse of the compromised  
12 data consisting of fraudulent charges placed on Plaintiff's M&T Bank debit card,  
13 totaling more than \$1,000, in or about November 2023 through March 2024; (xi)  
14 nominal damages; and (xii) the continued and certainly increased risk to their PII,  
15 which: (a) remains unencrypted and available for unauthorized third parties to access  
16 and abuse; and (b) remains backed up in Defendant's possession and is subject to  
17 further unauthorized disclosures so long as Defendant fails to undertake appropriate  
18 and adequate measures to protect the PII.

19  
20  
21  
22  
23  
24 193. Additionally, as a direct and proximate result of Defendant's negligence,  
25 Plaintiff and the Class have suffered and will suffer the continued risks of exposure  
26 of their Private Information, which remain in Defendant's possession and is subject  
27  
28

1 to further unauthorized disclosures so long as Defendant fails to undertake appropriate  
2 and adequate measures to protect the Private Information in its continued possession.

3  
4 194. Plaintiff and Class Members are entitled to compensatory and  
5 consequential damages suffered as a result of the Data Breach.

6  
7 195. Plaintiff and Class Members are also entitled to injunctive relief  
8 requiring Defendant to (i) strengthen its data security systems and monitoring  
9 procedures; (ii) submit to future annual audits of those systems and monitoring  
10 procedures; and (iii) continue to provide adequate credit monitoring to all Class  
11 Members.  
12

13  
14 **COUNT II**  
15 **Breach of Implied Contract**  
16 **(On Behalf of Plaintiff and the Class)**

17 196. Plaintiff incorporates the foregoing allegations as though fully set forth  
18 herein.

19 197. Plaintiff and Class Members were required to deliver their Private  
20 Information to Defendant as part of the process of obtaining services from Defendant.  
21 Plaintiff and Class Members paid money, or money was paid on their behalf, to  
22 Defendant in exchange for services.  
23

24 198. Defendant solicited, offered, and invited Class Members to provide their  
25 Private Information as part of Defendant's regular business practices. Plaintiff and  
26 Class Members accepted Defendant's offers and provided their Private Information  
27 to Defendant.  
28



1            199. Defendant accepted possession of Plaintiff’s and Class Members’  
2 Private Information for the purpose of providing services to Plaintiff and Class  
3 Members.  
4

5            200. Plaintiff and the Class entrusted their Private Information to Defendant.  
6 In so doing, Plaintiff and the Class entered into implied contracts with Defendant by  
7 which Defendant agreed to safeguard and protect such information, to keep such  
8 information secure and confidential, and to timely and accurately notify Plaintiff and  
9 the Class if their data had been breached and compromised or stolen.  
10

11            201. In entering into such implied contracts, Plaintiff and Class Members  
12 reasonably believed and expected that Defendant’s data security practices complied  
13 with relevant laws and regulations (including FTC guidelines on data security) and  
14 were consistent with industry standards.  
15  
16

17            202. Implicit in the agreement between Plaintiff and Class Members and the  
18 Defendant to provide Private Information, was the latter’s obligation to: (a) use such  
19 Private Information for business purposes only, (b) take reasonable steps to safeguard  
20 that Private Information, (c) prevent unauthorized disclosures of the Private  
21 Information, (d) provide Plaintiff and Class Members with prompt and sufficient  
22 notice of any and all unauthorized access and/or theft of their Private Information, (e)  
23 reasonably safeguard and protect the Private Information of Plaintiff and Class  
24 Members from unauthorized disclosure or uses, (f) retain the Private Information only  
25 under conditions that kept such information secure and confidential.  
26  
27  
28

1           203. The mutual understanding and intent of Plaintiff and Class Members on  
2 the one hand, and Defendant, on the other, is demonstrated by their conduct and  
3 course of dealing.  
4

5           204. On information and belief, at all relevant times Defendant promulgated,  
6 adopted, and implemented written privacy policies whereby it expressly promised  
7 Plaintiff and Class Members that it would only disclose Private Information under  
8 certain circumstances, none of which relate to the Data Breach.  
9

10           205. On information and belief, Defendant further promised to comply with  
11 industry standards and to make sure that Plaintiff's and Class Members' Private  
12 Information would remain protected.  
13

14           206. Plaintiff and Class Members paid money to Defendant with the  
15 reasonable belief and expectation that Defendant would use part of its earnings to  
16 obtain adequate data security. Defendant failed to do so.  
17

18           207. Plaintiff and Class Members would not have entrusted their Private  
19 Information to Defendant in the absence of the implied contract between them and  
20 Defendant to keep their information reasonably secure.  
21

22           208. Plaintiff and Class Members would not have entrusted their Private  
23 Information to Defendant in the absence of their implied promise to monitor their  
24 computer systems and networks to ensure that it adopted reasonable data security  
25 measures.  
26  
27  
28

1           209. Every contract in this State has an implied covenant of good faith and  
2 fair dealing, which is an independent duty and may be breached even when there is  
3 no breach of a contract's actual and/or express terms.  
4

5           210. Plaintiff and Class Members fully and adequately performed their  
6 obligations under the implied contracts with Defendant.  
7

8           211. Defendant breached the implied contracts it made with Plaintiff and the  
9 Class by failing to safeguard and protect their personal information, by failing to  
10 delete the information of Plaintiff and the Class once the relationship ended, and by  
11 failing to provide accurate notice to them that personal information was compromised  
12 as a result of the Data Breach.  
13

14           212. Defendant breached the implied covenant of good faith and fair dealing  
15 by failing to maintain adequate computer systems and data security practices to  
16 safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff  
17 and Class Members and continued acceptance of PII and storage of other personal  
18 information after Defendant knew, or should have known, of the security  
19 vulnerabilities of the systems that were exploited in the Data Breach.  
20  
21

22           213. As a direct and proximate result of Defendant's breach of the implied  
23 contracts, Plaintiff and Class Members sustained damages, including, but not limited  
24 to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII;  
25 (iv) lost time and opportunity costs associated with attempting to mitigate the actual  
26 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost  
27  
28



1           217. Defendant invaded Plaintiff's and the Class Members' right to privacy  
2 by allowing the unauthorized access to Plaintiff's and Class Members' PII and by  
3 negligently maintaining the confidentiality of Plaintiff's and Class Members' PII, as  
4 set forth above. Defendant further invaded Plaintiff's and Class Member's privacy by  
5 giving publicity to Plaintiff's and Class Members sensitive and confidential PII.  
6

7  
8           218. The intrusion was offensive and objectionable to Plaintiff, the Class  
9 Members, and to a reasonable person of ordinary sensibilities in that Plaintiff's and  
10 Class Members' PII was disclosed without prior written authorization of Plaintiff and  
11 the Class.  
12

13           219. The intrusion was into a place or thing which was private and is entitled  
14 to be private, in that Plaintiff and the Class Members provided and disclosed their PII  
15 to Defendant privately with an intention that the PII would be kept confidential and  
16 protected from unauthorized disclosure. Plaintiff and the Class Members were  
17 reasonable to believe that such information would be kept private and would not be  
18 disclosed without their written authorization.  
19  
20

21           220. As a direct and proximate result of Defendant's above acts, Plaintiff's  
22 and the Class Members' PII was viewed, distributed, and used by persons without  
23 prior written authorization and Plaintiff and the Class Members suffered damages as  
24 described herein.  
25  
26  
27  
28



1 the transaction and should have had their Private Information protected with adequate  
2 data security.

3  
4 227. Defendant knew that Plaintiff and Class Members conferred a benefit  
5 upon it and has accepted and retained that benefit by accepting and retaining the  
6 Private Information entrusted to it. Defendant profited from Plaintiff's retained data  
7 and used Plaintiff's and Class Members' Private Information for business purposes.

8  
9 228. Defendant failed to secure Plaintiff's and Class Members' Private  
10 Information and, therefore, did not fully compensate Plaintiff or Class Members for  
11 the value that their Private Information provided.

12  
13 229. Defendant acquired the Private Information through inequitable record  
14 retention as it failed to investigate and/or disclose the inadequate data security  
15 practices previously alleged.

16  
17 230. If Plaintiff and Class Members had known that Defendant would not use  
18 adequate data security practices, procedures, and protocols to adequately monitor,  
19 supervise, and secure their Private Information, they would have entrusted their  
20 Private Information at Defendant or obtained services at Defendant.

21  
22 231. Plaintiff and Class Members have no adequate remedy at law.

23  
24 232. Under the circumstances, it would be unjust for Defendant to be  
25 permitted to retain any of the benefits that Plaintiff and Class Members conferred  
26 upon it.  
27  
28

1           233. As a direct and proximate result of Defendant’s conduct, Plaintiff and  
2 Class Members have suffered and will suffer injury, including but not limited to: (i)  
3 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost  
4 time and opportunity costs associated with attempting to mitigate the actual  
5 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost  
6 opportunity costs associated with attempting to mitigate the actual consequences of  
7 the Data Breach; (vii) statutory damages; (viii) actual misuse of the compromised data  
8 consisting of an increase in spam calls, texts, and/or emails; (ix) actual misuse of the  
9 compromised data consisting of fraudulent charges placed on Plaintiff’s M&T Bank  
10 debit card, totaling more than \$1,000, in or about November 2023 through March  
11 2024; (xi) nominal damages; and (xii) the continued and certainly increased risk to  
12 their PII, which: (a) remains unencrypted and available for unauthorized third parties  
13 to access and abuse; and (b) remains backed up in Defendant’s possession and is  
14 subject to further unauthorized disclosures so long as Defendant fails to undertake  
15 appropriate and adequate measures to protect the PII.  
16

17           234. Plaintiff and Class Members are entitled to full refunds, restitution,  
18 and/or damages from Defendant and/or an order proportionally disgorging all profits,  
19 benefits, and other compensation obtained by Defendant from its wrongful conduct.  
20 This can be accomplished by establishing a constructive trust from which the Plaintiff  
21 and Class Members may seek restitution or compensation.  
22  
23  
24  
25  
26  
27  
28





1 of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires  
2 Defendant to take reasonable methods of safeguarding the PII of Plaintiff and the  
3  
4 Class Members.

5 240. In addition, Defendant engaged in unlawful acts and practices by failing  
6 to disclose the Data Breach in a timely and accurate manner, contrary to the duties  
7  
8 imposed by Cal. Civ. Code § 1798.82.

9 241. Defendant also violated its posted privacy policy, knowingly and  
10 willfully or negligently and materially, in violation of Cal. Bus. & Prof. Code § 22576.  
11

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

14 243. Defendant further committed unfair acts by failing to employ adequate  
15 and reasonable safeguards.  
16

17 244. Defendant's conduct was immoral, unethical, oppressive, unscrupulous,  
18 and substantially injurious to Plaintiff and Class Members. Further, Defendant's  
19 conduct narrowly benefitted its own business interests at the expense of Plaintiff's  
20 and Class Members' fundamental property and privacy interests protected by the  
21 California Constitution and the common law.  
22

23 245. As a direct and proximate result of Defendant's unlawful and unfair  
24 practices and acts, Plaintiff and Class Members were injured and lost money or  
25 property, including but not limited to: (i) invasion of privacy; (ii) theft of their PII;  
26  
27 (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated  
28

1 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of  
2 benefit of the bargain; (vi) lost opportunity costs associated with attempting to  
3 mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii)  
4 actual misuse of the compromised data consisting of an increase in spam calls, texts,  
5 and/or emails; (ix) actual misuse of the compromised data consisting of fraudulent  
6 charges placed on Plaintiff's M&T Bank debit card, totaling more than \$1,000, in or  
7 about November 2023 through March 2024; (xi) nominal damages; and (xii) the  
8 continued and certainly increased risk to their PII, which: (a) remains unencrypted  
9 and available for unauthorized third parties to access and abuse; and (b) remains  
10 backed up in Defendant's possession and is subject to further unauthorized  
11 disclosures so long as Defendant fails to undertake appropriate and adequate measures  
12 to protect the PII.

13  
14  
15  
16  
17 246. Plaintiff and Class Members have suffered harm in the form of lost  
18 property value, specifically the diminution of the value of their private and personally  
19 identifiable data.  
20

21 247. Defendant's actions caused damage to and loss of Plaintiff's and Class  
22 Members' property right to control the dissemination and use of their personal  
23 information and communications.  
24

25 248. Defendant knew or should have known that Defendant's computer  
26 systems and data security practices were inadequate to safeguard Plaintiff's and Class  
27 Members' PII and that the risk of a data breach or theft was highly likely. Defendant's  
28



1 C. For injunctive relief requested by Plaintiff, including but not limited to,  
2 injunctive and other equitable relief as is necessary to protect the interests of Plaintiff  
3 and Class Members, including but not limited to an order:  
4

- 5 i. prohibiting Defendant from engaging in the wrongful and  
6 unlawful acts described herein;  
7  
8 ii. requiring Defendant to protect, including through encryption, all  
9 data collected through the course of its business in accordance  
10 with all applicable regulations, industry standards, and federal,  
11 state, or local laws.  
12  
13 iii. requiring Defendant to delete, destroy, and purge the personal  
14 identifying information of Plaintiff and Class Members unless  
15 Defendant can provide to the Court reasonable justification for the  
16 retention and use of such information when weighed against the  
17 privacy interests of Plaintiff and Class Members;  
18  
19 iv. requiring Defendant to implement and maintain a comprehensive  
20 Information Security Program designed to protect the  
21 confidentiality and integrity of the PII of Plaintiff and Class  
22 Members;  
23  
24 v. prohibiting Defendant from maintaining the PII of Plaintiff and  
25 Class Members on a cloud-based database;  
26  
27  
28

- 1 i. requiring Defendant to engage independent third-party security  
2 auditors/penetration testers as well as internal security personnel  
3 to conduct testing, including simulated attacks, penetration tests,  
4 and audits on Defendant's systems on a periodic basis, and  
5 ordering Defendant to promptly correct any problems or issues  
6 detected by such third-party security auditors;  
7  
8  
9 vii. requiring Defendant to engage independent third-party security  
10 auditors and internal personnel to run automated security  
11 monitoring;  
12  
13 viii. requiring Defendant to audit, test, and train its security personnel  
14 regarding any new or modified procedures;  
15  
16 ix. requiring Defendant to segment data by, among other things,  
17 creating firewalls and access controls so that if one area of  
18 Defendant's network is compromised, hackers cannot gain access  
19 to other portions of Defendant's systems;  
20  
21 x. requiring Defendant to conduct regular database scanning and  
22 securing checks;  
23  
24 xi. requiring Defendant to establish an information security training  
25 program that includes at least annual information security training  
26 for all employees, with additional training to be provided as  
27 appropriate based upon the employees' respective responsibilities  
28

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

with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

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

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**

Plaintiff, on behalf of himself and the proposed Class, demands a trial by jury for all issues so triable.



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

Respectfully submitted,

Date: March 26, 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](mailto:jnelson@milberg.com)

*Attorney for Plaintiff and  
the Putative Class*