IN THE CIRCUIT COURT FOR THE SEVENTEENTH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

MICHAEL TOIKACH, BEATA TOIKACH, RAVEEN BHATT, PORTIA MARIE SMITHSON, SCOTT HOLLAND, RALPH NGUYEN, and ANDY ANSRYAN, individually, and on behalf of all others similarly situated, Plaintiffs, v. CHRISTIAN DIOR, INC., Defendant.	No. Division: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Michael Toikach, Beata Toikach, Raveen Bhatt, Portia Marie Smithson, Scott Holland, Ralph Nguyen, and Andy Ansryan ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Christian Dior, Inc. ("Dior" or "Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant.

2. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including Plaintiffs' and Class Members' first and last names, contact

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 1 of 64

*** FILED: BROWARD COUNTY, FL BRENDA D. FORMAN, CLERK 12/09/2025 03:48:40 PM.****

I HEREBY ATTEST THAT THIS CERTIFIED DOCUMENT IS A TRUE AND CORRECT COPY AS SAME APPEARS ON RECORD WITH BROWARD COUNTY CLERK OF COURTS.
VERIFY AT: HTTPS://WWW.BROWARDCLERK.ORG/ECERTIFY

Digitally signed by Brenda D Forman
Date: 2026.03.10 12:21:30 -04:00
Reason: Electronic Certified Copy
Location: 201 S.E. 6th Street, Fort Lauderdale, FL 33301

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 2 of 64

information, addresses, dates of birth, and other information provided to Dior, such passport or government ID numbers (collectively defined herein as "Private Information").

3. Upon information and belief, Plaintiffs and Class Members were required to entrust Defendant with sensitive, non-public Private Information as a condition of purchasing goods, without which Defendant could not perform its regular business activities. Defendant retains this information for at least many years and even after the company relationship has ended.

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

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

6. In breaching its duties to properly safeguard Plaintiffs' and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

7. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 3 of 64

information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

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

9. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 4 of 64

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

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

PARTIES

11. Plaintiff Michael Toikach is a natural resident and citizen of Hallandale Beach, Florida.

12. Plaintiff Beata Toikach is a natural resident and citizen of Hallandale Beach, Florida.

13. Plaintiff Raveen Bhatt is a natural resident and citizen of Chicago, Illinois.

14. Plaintiff Portia Marie Smithson is a natural resident and citizen of Pittsburgh, Pennsylvania.

15. Plaintiff Scott Holland is a natural resident and citizen of Glen Allen, Virginia.

16. Plaintiff Ralph Nguyen is a natural resident and citizen of Tamarac, Florida

17. Plaintiff Andy Ansryan is a natural resident and citizen of Los Angeles, California.

18. Defendant Christian Dior, Inc. is a for-profit corporation organized under the state laws of New York with its principal place of business located in New York, New York.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over Plaintiffs' claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of $50,000.00 dollars, exclusive of interest and attorneys' fees.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 5 of 64

20. This Court has personal jurisdiction over Defendant under Florida Stat. § 48.193 because it regularly conducts business in Florida, and has sufficient minimum contacts in Florida.

21. Venus is proper in this forum pursuant to Florida Statute §47.011, *et seq*. because the transactions out of which the causes of action arose occurred in this County, and Plaintiffs M. Toikach and B. Toikach reside in this County.

FACTUAL ALLEGATIONS

Background of Defendant.

22. Defendant Christian Dior, Inc. is the American subsidiary company of Christian Dior Couture SAS, a luxury brand that sells products, including fashion, accessories, fragrances, and beauty products.[1]

23. Plaintiffs and Class Members are current or former customers of Defendant's.

24. In order to purchase products from Defendant, Plaintiffs and Class Members were required to provide Defendant with their sensitive and confidential Private Information, including their first and last names, contact information, address, dates of birth, and other information provided to Dior, such as a passport or government ID number.

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

26. Upon information and belief, Defendant made promises and representations to Plaintiffs and Class Members, that the Private Information collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would

[1] https://www.dior.com/en_us/fashion (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 6 of 64

delete any sensitive information after it was no longer required to maintain it. These representations can be seen in the privacy policy on Dior's website.[2]

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

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

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

30. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[2] See https://www.dior.com/en_us/fashion/personal-data#christian-dior-privacy-policy-who-may-access-your-data ("We have adopted reasonable and appropriate physical, technical and organizational security safeguards to protect your data from loss, misuse, alteration, destruction or access by unauthorized third parties.") (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 7 of 64

31. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not sell its products to Plaintiffs and Class Members.

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

The Data Breach.

33. Starting on or about July 18, 2025, Defendant began sending Plaintiffs and other victims of the Data Breach a letter (the "Notice Letter"), informing them that:

> **What Happened?** On May 7, 2025, we identified a potential cybersecurity incident. We promptly conducted an investigation, supported by leading third-party cybersecurity experts. Our investigation determined that an unauthorized party was able to gain access to a Dior database that contained information about Dior clients on January 26, 2025. Dior promptly took steps to contain the incident, and we have no evidence of subsequent unauthorized access to Dior systems.
>
> **What information was involved**? The Dior database contained personal information such as first and last name, contact information, address, date of birth, and other information you may have provided to Dior, such as a passport or government ID number. Importantly, no payment information, including bank account or payment card information, was contained in the database accessed.[3]

34. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. Critical facts have still not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

---

[3] *See, e.g.*, Plaintiff M. Toikach's "Notice Letter" attached hereto as ***Exhibit A***.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 8 of 64

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

36. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' first and last names, contact information, addresses, dates of birth, and other information provided to Dior, such as passport or government ID numbers, for download and theft.

37. To be clear – there are numerous issues with Defendant's Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1) Defendant fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendant continues to maintain is secure; and (2) Defendant fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

38. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 9 of 64

should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information.

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

Data Breaches Are Preventable.

41. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

42. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

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

- Implement an awareness and training program. Because end users are targets, Plaintiffs and Class Members and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

---

[4] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Dec. 8, 2025).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 10 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 11 of 64

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

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[6]

[6] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed December 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 12 of 64

45. Given that Defendant was storing the sensitive Private Information of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information

47. As a condition of purchasing products, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information to Defendant.

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

49. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 13 of 64

Defendant Knew or Should Have Known of the Risk Because Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

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

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

53. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[7] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[8] The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.[9]

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

---

[7] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last accessed Dec. 8, 2025).

[8] *Id.*

[9] *Id.*

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 14 of 64

known that the Private Information that it collected and maintained would be targeted by cybercriminals.

55. Additionally, as companies became more dependent on computer systems to run their business, *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[10]

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

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

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

59. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), including tens of thousands of individuals'

[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 15 of 64

detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

61. Defendant's offering of credit and identity monitoring establishes that Plaintiffs and Class Members' sensitive Private Information *was* in fact affected, accessed, and compromised.

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

63. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 16 of 64

Value of Personally Identifying Information.

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employee-benefit management company or taxpayer identification number."[12]

66. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[13] For example, the average price for driver's license information on the dark web is $150.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

67. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information

---

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*
[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 8, 2025).
[14] ***Here's What Your Data Sells for on the Dark Web,*** Experian, Jun. 30, 2025, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 8, 2025).
[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 17 of 64

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name and date of birth.

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

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

Defendant Failed to Comply with FTC Guidelines.

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

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

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 18 of 64

that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

73. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

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

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

76. These FTC enforcement actions include actions against companies like Defendant.

---

[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Dec. 8, 2025).

[18] *Id.*

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 19 of 64

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

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

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

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

Defendant Failed to Comply with Industry Standards.

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

82. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendant, including but not limited to: educating all Plaintiffs and Class Members; strong passwords; multi-layer security,

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 20 of 64

including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which Plaintiffs and Class Members can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

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

85. These foregoing frameworks are existing and applicable industry standards in the industry safeguarding Plaintiffs' and Class Members' data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards.

Common Injuries and Damages.

86. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 21 of 64

imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Victims' Risk of Identity Theft.

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 22 of 64

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

91. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[19]

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

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

---

[19] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 23 of 64

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

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

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

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

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

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

98. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to protect themselves by reviewing account statements and monitoring their credit reports, in addition to enrolling in the offered free credit monitoring program.

99. Defendant's extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 24 of 64

time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

100. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, freezing their payment cards, contacting credit bureaus to place freezes on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

101. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

102. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),

[20] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf. (last accessed Dec. 8, 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 25 of 64

reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

Diminution of Value of Private Information.

103. Private Information is a valuable property right. 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 Private Information has considerable market value.

104. Private Information can sell for as much as $363 per record according to the Infosec Institute.[22]

105. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] 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.[24]

106. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an

---

[21] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Dec. 8, 2025).

[22] *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).

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://www.infosecinstitute.com/resources/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/ (last accessed December 8, 2025).

[24] https://datacoup.com/ (last accessed Dec. 8 2025).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 26 of 64

economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

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

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

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

110. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

112. Personal data like Private Information is a valuable property right.[25] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber

[25] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 27 of 64

thefts may include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

113. 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.

114. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the cybercriminals.

115. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

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

Loss of Benefit of the Bargain.

117. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to obtain products from Defendant under certain terms, Plaintiffs and Class Members understood and expected that Defendant would

---

Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, 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).

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 28 of 64

properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security.

118. Accordingly, Plaintiffs and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiffs' Experiences

Plaintiff Michael Toikach's Experiences

119. Plaintiff Michael Toikach is a customer of Defendant's.

120. Upon information and belief, as a condition of buying product(s), Plaintiff Toikach was required to provide his Private Information to Defendant.

121. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Toikach's Private Information in its system.

122. Plaintiff Toikach is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

123. Plaintiff Toikach provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

124. Plaintiff Toikach reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

125. Plaintiff Toikach received the Notice Letter, by U.S. mail, directly from Defendant, dated July 18, 2025. According to the Notice Letter, Plaintiff Toikach's Private

Information was improperly accessed and obtained by unauthorized third parties, including his name, contact information, address, date of birth, and other information he may have provided to Dior, such as a passport or government ID number.

126. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Toikach to monitoring his free credit report for any authorized activity, Plaintiff Toikach made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Toikach has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Toikach otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

127. Subsequent to the Data Breach, Plaintiff Toikach has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 29 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 30 of 64

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

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

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

131. Plaintiff Toikach has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Beata Toikach's Experiences

132. Plaintiff Beata Toikach is a customer of Defendant's.

133. Upon information and belief, as a condition of buying product(s), Plaintiff Toikach was required to provide her Private Information to Defendant.

134. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Toikach's Private Information in its system.

135. Plaintiff Toikach is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 31 of 64

136. Plaintiff Toikach provided her Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

137. Plaintiff Toikach reasonably understood that in exchange for providing Defendant with her Private Information, Defendant would employ adequate cybersecurity measures and protect her Private Information.

138. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated July 18, 2025. According to the Notice Letter, Plaintiff Toikach's Private Information was improperly accessed and obtained by unauthorized third parties.

139. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Toikach made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Toikach has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Toikach otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Subsequent to the Data Breach, Plaintiff Toikach has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third

parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

143. Plaintiff Toikach has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Raveen Bhatt's Experiences

144. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Bhatt's Private Information in its system.

145. Plaintiff Bhatt is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

146. Plaintiff Bhatt provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 32 of 64

147. Plaintiff Bhatt reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

148. As a result of the Data Breach, Plaintiff Bhatt made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Bhatt has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Bhatt otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Subsequent to the Data Breach, Plaintiff Bhatt has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 33 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 34 of 64

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

152. Plaintiff Bhatt has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Portia Marie Smithson's Experiences

153. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Smithson's Private Information in its system.

154. Plaintiff Smithson is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

155. Plaintiff Smithson provided her Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

156. Plaintiff Smithson reasonably understood that in exchange for providing Defendant with her Private Information, Defendant would employ adequate cybersecurity measures and protect her Private Information.

157. As a result of the Data Breach, Plaintiff Smithson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Smithson has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Smithson otherwise would have spent on other activities,

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 35 of 64

including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

158. Subsequent to the Data Breach, Plaintiff Smithson has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

161. Plaintiff Smithson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Scott Holland's Experiences

162. Plaintiff Holland is a customer of Defendant's.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 36 of 64

163. Upon information and belief, as a condition of buying product(s), Plaintiff Holland was required to provide his Private Information to Defendant.

164. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Holland's Private Information in its system.

165. Plaintiff Holland is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

166. Plaintiff Holland provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

167. Plaintiff Holland reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

168. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated July 18, 2025. According to the Notice Letter, Plaintiff Holland's Private Information was improperly accessed and obtained by unauthorized third parties.

169. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Holland made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Holland has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Holland otherwise would

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 37 of 64

have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

170. Subsequent to the Data Breach, Plaintiff Holland has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

173. Plaintiff Holland has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ralph Nguyen's Experiences

174. Plaintiff Nguyen provided his Private Information to Defendant.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 38 of 64

175. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Nguyen's Private Information in its system.

176. Plaintiff Nguyen is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

177. Plaintiff Nguyen's provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

178. Plaintiff Nguyen's reasonably understood that in exchange for providing Defendant his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

179. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated July 18, 2025. According to the Notice Letter, Plaintiff Nguyen's Private Information was improperly accessed and obtained by unauthorized third parties.

180. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Nguyen made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Nguyen has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Nguyen otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 39 of 64

181. Subsequent to the Data Breach, Plaintiff Nguyen has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

184. Plaintiff Nguyen has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Andy Ansryan's Experiences

185. Plaintiff Ansryan is a customer of Defendant's.

186. Upon information and belief, as a condition of buying product(s), Plaintiff Ansryan was required to provide his Private Information to Defendant.

187. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Ansryan's Private Information in its system.

188. Plaintiff Ansryan is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

189. Plaintiff Ansryan provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

190. Plaintiff Ansryan reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

191. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, on or around July 19, 2025. According to the Notice Letter, Plaintiff Ansryan's Private Information was improperly accessed and obtained by unauthorized third parties.

192. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Ansryan made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Ansryan has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Ansryan otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 40 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 41 of 64

193. Subsequent to the Data Breach, Plaintiff Ansryan has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

196. Plaintiff Ansryan has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

197. Plaintiffs bring this class action, under Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including those who received notice of the Data Breach (the "Class").

198. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

199. Plaintiffs reserve the right to amend the class definition.

200. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

201. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

202. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 42 of 64

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

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

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

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

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

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

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

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 43 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 44 of 64

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

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

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

207. Superiority and Manageability. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually

afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 45 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 46 of 64

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

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

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

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard Plaintiffs' and Class Members' Private Information; and,

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 47 of 64

CAUSES OF ACTION

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

214. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 213, as if fully set forth herein.

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

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

217. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 48 of 64

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

222. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of purchasing Defendant's products.

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

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

225. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Plaintiffs' and Class Members' Private Information they were no longer required to retain pursuant to regulations.

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

227. Defendant had and continue to has a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent,

mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

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

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

b. Allowing unauthorized access to Class Members' Private Information;

c. Failing to remove Plaintiffs' and Class Members' Private Information it was no longer required to retain pursuant to regulations, and;

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

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 49 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 50 of 64

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

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

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

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

236. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, and the critical importance of providing adequate security of that Private Information.

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 51 of 64

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

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

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

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

244. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 52 of 64

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

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

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

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

248. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 53 of 64

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

250. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 213, as if fully set forth herein.

251. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

252. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant obtained and stored and the foreseeable consequences of a data breach.

253. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

254. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

255. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 54 of 64

256. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

257. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

258. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 213, as if fully set forth herein.

259. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information and payment and/or labor. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 55 of 64

260. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the payment and/or labor and the Private Information entrusted to it. Defendant profited from Plaintiffs' payment and/or labor and retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

261. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

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

263. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information at Defendant.

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

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 56 of 64

267. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 57 of 64

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

270. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 213, as if fully set forth herein.

271. Plaintiffs and the Class entrusted their Private Information to Defendant as a condition of purchasing products. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

272. At the time Defendant acquired the Private Information of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

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

274. Plaintiffs and the Class would not have entrusted their Private Information to Defendant had they known that Defendant would make not adequately protect the Private Information entrusted to it.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 58 of 64

275. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

276. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

277. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

278. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

279. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 213, as if fully set forth herein.

280. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

281. Defendant owed a duty to Plaintiffs and Class Members to keep this information confidential.

282. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' Private Information is highly offensive to a reasonable person.

283. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

285. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

286. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

287. Acting with knowledge, Defendant had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 59 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 60 of 64

288. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

289. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

290. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

291. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

292. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding prejudgment and post-judgment interest, as provided by law;

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

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

JURY TRIAL DEMANDED

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

Dated: December 9, 2025

Respectfully submitted,

By: */s/ Jeff Ostrow*
Jeff Ostrow, FBN 121452
KOPELOWITZ OSTROW P.A.
1 W Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 61 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 62 of 64

ostrow@kolawyers.com

Mariya Weekes, FBN 56299
MILBERG PLLC
333 SE 2nd Avenue
Suite 2000 Miami, FL, 33131
Tel: (786) 206-9057
Fax: (786) 879-7520
Email: mweekes@milberg.com

Manuel S. Hiraldo, FBN 030380
HIRALDO P.A.
401 E. Las Olas Boulevard, Suite 1400
Fort Lauderdale, FL 33301
Tel: 954.400.4713
mhiraldo@hiraldolaw.com

Amber L. Schubert (pro hac vice forthcoming)
SCHUBERT JONCKHEER & KOLBE LLP 2001 Union St., Ste. 200
San Francisco, CA 94123
Tel: 415-788-4220
aschubert@sjk.law

Nicholas A. Migliaccio (pro hac vice forthcoming)
Jason Rathod (pro hac vice forthcoming)
MIGLIACCIO & RATHOD, LLP
412 H Street NE, Suite 302
Washington, D.C. 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Jason P. Sultzer
SULTZER & LIPARI, PLLC
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Tel: (845) 483-7100
sultzerj@thesultzerlawgroup.com

Attorney for Plaintiffs and Proposed Class

EXHIBIT A

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 63 of 64

Unique Code : CAA-FAA-BCABB-JDGCFAGC-BEEDICG-H Page 64 of 64

Return Mail Processing
PO Box 999
Suwanee, GA 30024

DIOR

[redacted]AUTO**ALL FOR AADC 331
[redacted]

NOTICE OF DATA BREACH

July 18, 2025

Dear Michael Tokach,

[redacted]

What happened? On May 7, 2025, we identified a [redacted] promptly conducted an investigation, supported by leading [redacted] investigation determined that an unauthorized party was able to gain [redacted] that contained information about Dior clients on January 26, 2025. [redacted] contain the incident, and we have no evidence of subsequent [redacted]

What information was involved? The Dior database [redacted] first and last name, contact information, address, date of birth, and [redacted] have provided to Dior, such as a passport or government ID number. [redacted] information, including bank account or payment card information, was [redacted] database accessed.

What are we doing? We have conducted an investigation with the support of leading third-party cybersecurity experts and notified law enforcement. We have taken steps designed to enhance our network security and help prevent future incidents. The third-party cybersecurity experts have verified that the incident is contained, and that there is no evidence that the unauthorized third-party was able to access Dior systems except on January 26, 2025.

To help [redacted] Experian IdentityWorks℠ [redacted] fraud resolution services, and [redacted] offer, please follow the steps in the [redacted]

What can you do? We recommend you remain vigilant for [redacted] We also recommend that you continue to review your financial accounts, [redacted] free credit reports for any suspicious activity. Attachment A to this letter contains [redacted] information about steps you can take to protect yourself against potential fraud and identity theft.

For more information: We remain committed to maintaining the security of your personal information. For any questions or concerns about this letter or support with enrollment in the Experian IdentityWorks℠ monitoring, please contact 1-[redacted].

CHRISTIAN DIOR COUTURE
30, avenue Montaigne, 75008 Paris – Tél. 33 (0) 1 40 73 54 44 – www.dior.com

Engagement # B147873

Public court record.

This copy was downloaded from https://cw.simpluris.com/docs/public/downloads/CTC/COMPLAINT on 2026-11-02 and is hosted, unaltered, for reference at https://chimo.ai/class-action/christian-dior

Court: Circuit Court for Broward County, Florida
Case number: CACE 25-18776
Filed: 2025-12-09

Chimo hosts public court records for readers' reference; documents are unaltered copies from the court docket or the court-approved settlement website.