UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RALPH NGUYEN, individually and on behalf of all others similarly situated, Plaintiff, v. CHRISTIAN DIOR, INC., Defendant.	Case No. **CLASS ACTION** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Ralph Nguyen brings this class action against Defendant Christian Dior, Inc., and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("Private Information") of Plaintiff and the Class members, including, without limitation: names, dates of birth, home addresses, phone numbers, driver's license number and/or passport numbers.

2. In the course of its operations, Defendant was entrusted with an extensive amount of Plaintiff's and the Class Private Information.

3. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed non-delegable legal and equitable duties to Plaintiff and the Class members.

4. On or about May 7, 2025, learned that intruder gained entry to Defendant's network, accessed Plaintiff's and the Class members' Private Information, and exfiltrated information (the "Data Breach Incident").

5. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach Incident is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

6. Defendant did not notify Plaintiff and the Class members of the incident until on or about July 18, 2025.

7. Plaintiff's and the Class members' Private Information that was acquired in the Data Breach Incident can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and the Class members face a lifetime risk of identity theft.

8. Plaintiff's and the Class members' Private Information was compromised due to Defendant's negligent acts and omissions and the failure to protect Plaintiff's and the Class members' Private Information.

9. Plaintiff and Class members continue to be at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Defendant disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure their Private Information 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 in the possession

of its vendor. As a result, the Private Information of Plaintiff and Class members was compromised through access to and exfiltration by an unknown and unauthorized third party.

11. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect their Private Information; (ii) warn of Defendant's inadequate information security practices; (iii) effectively oversee, supervise, and secure equipment and the database containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents; and (iv) adequately supervise and oversee its vendor with whom it shared Plaintiff's and the Class members' Private Information.

12. Plaintiff and Class members have suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach Incident; (d) invasion of privacy; (e) the emotional distress and anguish, stress, and annoyance of responding to, and resulting from, the Data Breach Incident; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' Private Information against theft and not allow access and misuse of their personal data by others; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate

measures to protect Plaintiff's and Class members' Private Information, and, at the very least, are entitled to nominal damages.

13. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

14. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Florida.

15. Plaintiff provided his Private Information to Defendant.

16. Plaintiff greatly values his privacy and Private Information. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his Private Information. Plaintiff would not have agreed to provide his Private Information to Defendant or used Defendant's product had Plaintiff known that Defendant would not safeguard his Private Information from unauthorized access.

17. Plaintiff is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

18. Plaintiff received a letter dated July 18, 2025, from Defendant concerning the Data Breach Incident. The letter stated that unauthorized actors gained access to files on Defendant's network. The compromised files contained Plaintiff's names, dates of birth, home addresses, phone numbers, passport and/or driver's license number.

19. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff faces, Defendant offered him a two-year subscription to a credit monitoring service. Plaintiff has not signed up for the program as he does not trust Defendant's chosen vendor with

his Private Information. Additionally, Plaintiff does not believe this is sufficient to protect his identity from the ongoing risks of theft he faces.

20. Since learning of the Data Breach and in an attempt to prevent the misuse of his Private Information, Plaintiff has spent additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts.

21. Plaintiff plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity. Indeed, Defendant's notice directs Plaintiff to take such steps.

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

23. Defendant is, and at all times relevant hereto was, a domestic corporation with its principal place of business located in New York, New York.

JURISDICTION AND VENUE

24. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a putative class action involving thousands of Class members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, many absent Class members and Defendant are citizens of different states.

25. This Court has general personal jurisdiction over Defendant because Defendant is headquartered in this jurisdiction.

26. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district.

FACTS

27. At the time of the Data Breach Incident, Defendant maintained Plaintiff's and the Class members Private Information utilizing a database and software.

28. By obtaining, collecting, and storing Plaintiff's and Class members' Private Information, Defendant assumed non-delegable legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

29. Plaintiff and Class members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that any vendor with whom Defendant shared the information was properly supervised and had the proper procedures in place to protect their Private Information.

30. Defendant had a non-delegable duty to adopt reasonable measures to protect Plaintiff's and Class members' Private Information, including any Private Information Defendant shared with any of its vendors, from involuntary disclosure to third parties.

31. Prior to the Data Breach Incident, Defendant should have ensured that it had adequate monitoring software in place to detect intrusions or the transfer of large volumes of data to third party networks, that it implemented multi-factor authentication to verify the credentials of individuals attempting to access Private Information, that it limited access to Private Information to only necessary employees, that it encrypted or tokenized Private Information in internet

accessible locations, and that it deleted or redacted Private Information that it was no longer required to maintain. By failing to implement these reasonable and industry standard data security measures, Defendant left Plaintiff's and Class members' Private Information in a condition vulnerable to unauthorized access.

32. On or about May 7, 2025, an intruder gained entry to Defendant's database, Defendant mailed Plaintiff and the Class members a form notice attempting to minimize the Data Breach Event, while admitting that sensitive Private Information had been compromised and stolen.

33. Defendant did not notify Plaintiff of the breach until on or about July 28, 2025.

34. Contrary to the self-serving narrative in Defendant's form notice, Plaintiff's and Class members' unencrypted information has been compromised and will end up for sale on the dark web and/or fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval.

35. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and the Class members.

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

37. Defendant's negligence in safeguarding Plaintiff's and the Class members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

38. Defendant knew that it was a prime target for hackers given the significant amount of sensitive personal information in its possession, custody and/or control related to its customers and others. Defendant's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

39. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. 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. 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.

40. Despite knowing the prevalence of data breaches, Defendant failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Defendant could have prevented the Data Breach by encrypting and/or redacting sensitive data, limiting access to Private Information to only necessary employees, monitoring their network for signs of intrusion or the transfer of large volumes of data, and employing multi-factor authentication to ensure that only authorized individuals are granted access to sensitive data.

41. Despite the prevalence of public announcements and knowledge of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class members from being compromised.

42. The Private Information of Plaintiff and the Class members was stolen to engage in identity theft and/or to sell it to criminals who will purchase the Private Information for that purpose.

43. The Private Information exposed by Defendant as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

44. Indeed, stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

45. 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.

46. 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.[1]

47. 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.

---

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

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

49. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

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

51. The injuries to Plaintiff and the Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Plaintiff's and the Class members' Private Information.

52. Plaintiff has suffered and will continue to suffer a substantial risk of imminent identity, financial, fraud and theft; emotional anguish and distress resulting from the Data Breach Incident, including emotional stress and damages about the years of identity fraud Plaintiff faces; and increased time spent reviewing financial statements and credit reports to determine whether there has been fraudulent activity on any of his accounts.

53. Plaintiff 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 ALLEGATIONS

PROPOSED CLASS

54. Plaintiff brings this lawsuit as a class action on behalf of himself individually and on behalf of all other similarly situated persons as a class action pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and 23(c)(5). The "Class" that Plaintiff seeks to represent is defined as:

> **Class: All persons in the United States whose Private Information was accessed and/or exfiltrated during the Data Breach Incident.**

55. Defendant and its employees or agents are excluded from the Class.

NUMEROSITY

56. The Data Breach Incident has impacted several thousand individuals. The members of the Class, therefore, are so numerous that joinder of all members is impracticable.

57. Identification of the Class members is a matter capable of ministerial determination from Defendant's records.

COMMON QUESTIONS OF LAW AND FACT

58. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are: [1] Whether and to what extent Defendant had a non-delegable duty to protect the Private Information Plaintiff and Class members, including

Private Information Defendant shared with its vendor; [2] Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members; [3] When Defendant actually learned of the Data Incident; [4] Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their Private Information had been compromised; [4] 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 Incident; [5] Whether Defendant adequately addressed and supervised the vulnerabilities which permitted the Data Breach Incident to occur; [6] Whether Plaintiff and the Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; [7] Whether Plaintiff and the Class members are entitled to restitution as a result of Defendant's wrongful conduct; and [8] Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach Incident.

59. The common questions in this case are capable of having common answers. Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

60. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

61. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

62. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

63. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

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

64. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

65. Plaintiff bring this claim on behalf of himself and the Class.

Foreseeability

66. Prior to the Data Breach Incident, each Defendant knew that threat attackers were targeting companies such as Defendant in an effort to obtain personally identifiable information and misuse it to commit fraud and identity theft, particularly when stored in an internet-accessible environment, in at least the following respects:

(a) Defendant was aware of previous data breaches, including breaches that affected information of their competitors;

(b) Hackers are known to routinely attempt to steal such information and use it for nefarious purposes; and

(c) Publicly available industry warnings regarding threat attackers' efforts to obtain such information for ransom or misuse were widely and readily available to Defendant.

Duty, Breach, and Causation

67. Prior to the Data Breach, Defendant knowingly and intentionally acquired the Private Information of Plaintiff and the Class members.

68. In knowingly and intentionally acquiring the Private Information of Plaintiff and Class members, Defendant assumed a duty to use reasonable care, including implementing reasonable security practices and procedures, to safeguard the Private Information of Plaintiff and Class members against unauthorized access, acquisition, and misuse.

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

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

71. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of doing business with Defendant.

72. Defendant failed to use reasonable care by storing the Private Information of Plaintiff and Class members in an internet-accessible environment under the following circumstances:

(a) The Private Information of Plaintiff and Class members was not encrypted.

(b) The Private Information of Plaintiff and Class members that Defendant had no reasonable need to store in an internet-accessible environment, including the Private Information of Plaintiff and Class members with whom Defendant had not had a relationship for years, was not removed from Defendant's network.

(c) The movement of the Private Information of Plaintiff and Class members from Defendant's network to the internet was not monitored and detected in real time.

73. Defendant was negligent in that it failed to ensure that it had adequate monitoring software in place to detect intrusions or the transfer of large volumes of data to third party networks, that it implemented multi-factor authentication to verify the credentials of individuals attempting to access Private Information, that it limited access to Private Information to only necessary employees, that it encrypted or tokenized Private Information in internet accessible locations, and that it deleted or redacted Private Information that it was no longer required to maintain. By failing to implement these reasonable and industry standard data security measures, Defendant left Plaintiff's and Class members' Private Information in a condition vulnerable to unauthorized access.

Damages

74. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, including unauthorized charges; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information, including the exposure of their Private Information on the dark web and the substantial risk of future harm; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach Incident, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continuing risk to their Private Information, which remains 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 current and former customers' Private Information in their continued possession; (viii) damages consisting of the cost of identity theft protection services for the remainder of the lives of Plaintiff and Class members; and (ix) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of Private Information resulting from the Data Breach for the remainder of the lives of Plaintiff and Class members.

75. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risk of exposure of their Private

Information, which remains 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 in their continued possession.

76. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are now at an increased risk of identity theft or fraud.

77. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

a) An order certifying this case as a class action on behalf of the Class as defined above, and appointing Plaintiff as the representative of the Class and Plaintiff's counsel as Class Counsel;

b) Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

c) Injunctive relief, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order: (1) requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws; (2)

requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members; (3) requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Member's personal identifying information; (4) prohibiting Defendant from maintaining Plaintiff's and Class members' personal identifying information on a cloud-based database; (5) requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; (6) requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring; (7) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (8) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; (9) requiring Defendant to conduct regular database scanning and securing checks; (10) requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be

provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members; (11) requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (12) requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information; (13) requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; (14) requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; (15) requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and (16) for a period of 10 years, appointing a qualified and independent third party assessor to conduct attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to

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

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

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

f) For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demand a trial by jury.

DATED: July 30, 2025

Respectfully submitted,

/s/ Zane C. Hedaya
ZANE C. HEDAYA, ESQ.
New York Bar No.: 6135339
E-mail: zane@jibraellaw.com
The Law Offices of Jibrael S. Hindi
1515 NE 26th Street
Wilton Manors, FL 33305
Phone: 813-340-8838

HIRALDO P.A.
Manuel S. Hiraldo, Esq.
Florida Bar No. 030380
Pro Hac Vice to be Submitted
401 E. Las Olas Boulevard
Suite 1400
Ft. Lauderdale, Florida 33301
Email: mhiraldo@hiraldolaw.com
Telephone: 954.400.4713