UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MARY STERNER, on behalf of herself and all others similarly situated, Plaintiff, v. **NOVO NORDISK INC.** and **NOVO NORDISK A/S**, Defendants.	Case No. 3:26-cv-7353 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Mary Sterner ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Novo Nordisk Inc. and Novo Nordisk A/S ("Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. Defendants are global pharmaceutical companies.

3. As such, Defendants stores a litany of highly sensitive personal identifiable information ("PII/PHI") and protected health information ("PHI")—together "PII/PHI"—about their current and former patients and employees. But Defendants lost control over that data when cybercriminals infiltrated their insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendants' network before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of their systems—thereby allowing cybercriminals unrestricted access to their current and former patients and employees' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendants' failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim. She brings this class action on behalf of herself, and all others harmed by Defendants' misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, their current and former patients and employees' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff Mary Sterner is a natural person and a citizen of Florida. She is domiciled in Florida (where she intends to remain).

9. Defendant Novo Nordisk Inc. is a corporation incorporated in Delaware and with its principal place of business at 800 Scudders Mill Road, Plainsboro, New Jersey 08536.

10. Defendant Novo Nordisk A/S is a public limited liability company formed under the laws of Denmark and with its principal place of business at Novo Alle 1 2880, Bagsværd Denmark.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Novo Nordisk A/S are citizens of different states. And there are over 100 putative Class Members.

12. This Court has personal jurisdiction over Defendants because Novo Nordisk Inc. is headquartered in New Jersey, and because both Defendants regularly conduct business in New Jersey and have sufficient minimum contacts in New Jersey.

13. Venue is proper in this Court because Novo Nordisk Inc.'s principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendants Collected and Stored the PII/PHI of Plaintiff and the Class

14. Defendants are global pharmaceutical companies.

15. As part of their business, Defendants receives and maintains the PII/PHI of thousands of their current and former patients and employees.

16. In collecting and maintaining the PII/PHI, Defendants agreed it would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

17. Under state and federal law, businesses like Defendants have duties to protect their current and former patients and employees' PII/PHI and to notify them about breaches.

Defendants' Data Breach

18. In or around June 2026, Defendants were hacked by the notorious cybercriminal

group FulcrumSec who exfiltrated approximately "1.3 terabytes and around 700,000 files" from Defendants.[1]

19. On information and belief, FulcrumSec acquired the PII/PHI of the current and former patients and employees of Defendants.

20. So far, Novo Nordisk has confirmed that the exposed data included at least "patient IDs, sex, year of birth, biomarkers, health and immunogenicity data, and lifestyle factors like BMI and smoking status."[2]

21. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendants' custody and control. And upon information and belief, the putative class is over one hundred members—as it includes their current and former patients and employees.

22. Defendants failed their duties when their inadequate security practices caused the Data Breach. In other words, Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendants caused widespread injury and damages.

23. Because of Defendants' Data Breach, the sensitive PII/PHI of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

24. As explained by the global cybersecurity firm BlackFog, the *modus operandi* of cybercriminals like FulcrumSec is to exfiltrate private information through a data breach and then

[1] Ransomnews Research Team, *Novo Nordisk hit by FulcrumSec: the stealer logs saw it coming*, RANSOM NEWS (June 17, 2026) https://ransomnews.com/novo-nordisk-fulcrumsec-breach-2026/.
[2] *Id*.

"post it on forums on the Dark Web where it will be sold for profit."[3]

25. Indeed, the Federal Trade Commission has explained that "data stolen from businesses ends up on the dark web where criminals buy and sell it to commit fraud, get fake identity documents, or fund their criminal organizations."[4]

26. Thus, on information and belief, the PII/PHI of Plaintiff and the Class has already been leaked or sold by cybercriminals FulcrumSec on the Dark Web or will be leaked or sold imminently by cybercriminals FulcrumSec on the Dark Web.

Plaintiff's Experiences and Injuries

27. Plaintiff Mary Sterner is a patient of Defendants.

28. As a condition of receiving products and services, Defendants required that Plaintiff disclose her PII/PHI to them.

29. Thus, Defendants obtained and maintained Plaintiff's PII/PHI.

30. As a result, Plaintiff was injured by Defendants' Data Breach.

31. Plaintiff is very careful about the privacy and security of her PII/PHI. She does not knowingly transmit her PII/PHI over the internet in an unsafe manner. She is careful to store any documents containing her PII/PHI in a secure location.

32. As a condition of receiving products and services with Defendant, Plaintiff provided Defendants with her PII/PHI. Defendants used that PII/PHI to facilitate their products and services to Plaintiff.

33. Plaintiff provided her PII/PHI to Defendants and trusted the company would use

---

[3] Brenda Robb, *After the Data Breach – What Happens to Your Data*, BLACKFOG (July 27, 2025) https://www.blackfog.com/after-the-data-breach-what-happens-to-your-data/.

[4] John Krebs, *The dark web: What your business needs to know*, FED. TRADE COMM. (Oct. 17, 2017) https://www.ftc.gov/business-guidance/blog/2017/10/dark-web-what-your-business-needs-know.

reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

34. Plaintiff reasonably understood that a portion of the funds derived from her payments would be used to pay for adequate cybersecurity and protection of PII/PHI.

35. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

36. Through their Data Breach, Defendants compromised Plaintiff's PII/PHI.

37. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendants directed Plaintiff to take those steps in their breach notice.

38. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam phone calls.

39. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

40. Because of Defendants' Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

41. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

42. Plaintiff suffered actual injury in the form of damages to and diminution in the

value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendants was required to adequately protect.

43. As a patient, Plaintiff suffered actual injury and lost the "benefit of the bargain" when Plaintiff provided payments to Defendants in exchange for both payment and reasonable data security for her PII/PHI. After all, if Defendants was transparent about its deficient data security, then Plaintiff would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.[5]

44. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

45. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

46. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Consumers Prioritize Data Security

47. In 2024, the technology and communications conglomerate Cisco published the

[5] Economics has long recognized that "[w]orkers choose a job and receive in return a bundle consisting of income and a probability of [] injury" and that "jobs with disagreeable characteristics command higher wages[.]" Jeff E. Biddle & Gary A. Zarkin, *Worker Preference and Market Compensation for Job Risk*, 70(4) REV. ECON. & STAT. (MIT PRESS) 660, 660–61 (1988); Robert S. Smith, *Compensating Wage Differentials and Public Policy: A Review*, 32 INDUS. & LABOR REL. REV. (CORNELL UNIV.) 339 (1979); Greg J. Duncan & Bertil Holmlund, *Was Adam Smith Right After All? Another Test of the Theory of Compensating Wage Differentials*, 1 J. LABOR ECON. (UNIV. CHICAGO PRESS) 336, 336–37 (1983).

results of its multi-year "Consumer Privacy Survey."[6] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[7]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[8]

c. 89% of consumers stated that "I care about data privacy."[9]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[10]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[11]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[12]

Plaintiff and the Proposed Class Suffered Common Injuries and Damages

48. Because of Defendants' failure to prevent the Data Breach, Plaintiff and Class

[6] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited June 18, 2026).
[7] *Id*. at 3.
[8] *Id*.
[9] *Id*. at 9.
[10] *Id*.
[11] *Id*.
[12] *Id*. at 11.

Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII/PHI.

Substantially Increased Risk of Identity Theft and Fraud

49. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

50. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

51. 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

"[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

52. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the Dark Web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

53. The "Dark Web" is an unindexed layer of the internet that requires special software or authentication to access.[13] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[14] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

54. The unencrypted PII/PHI of Plaintiff and Class Members has or will end up for sale on the Dark Web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII/PHI may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII/PHI.

55. Theft of Social Security numbers also creates a particularly alarming situation for

[13] *What Is the Dark Web?*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited June 18, 2026).
[14] *Id*.

victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

56. In particular, the theft of Social Security numbers—in combination with other PII/PHI (e.g., name, address, date of birth)—provides cybercriminals with a "skeleton key" to commit rampant fraud and identity theft.

57. For example, cybersecurity expert Jim Stickley explained to Time Magazine that "[i]f I have your name and your Social Security number, and you haven't gotten a credit freeze yet, you're easy pickings . . . With that, you can do whatever you want . . . You can become that person."[15] For context, Jim Stickley is a "penetration tester" who is employed by businesses "to infiltrate their systems in order to find flaws they can fix before the bad guys exploit them."[16]

58. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

59. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to

[15] Patrick L. Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME MAGAZINE (Aug. 5, 2019) https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[16] *Id*.

learn that information.[17]

60. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

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

62. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

63. Identity thieves can also use an individual's personal data and PII/PHI to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even

[17] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. SYSTEMICS, CYBERNETICS & INFORMATICS 9 (2019) http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[18]

64. One example of criminals piecing together bits and pieces of compromised PII/PHI to create comprehensive dossiers on individuals is called "Fullz" packages.[19] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen PII/PHI, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

65. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals

[18] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited June 18, 2026).

[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 those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

(such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

66. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[20]

67. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Yet, Defendant failed to rapidly report to Plaintiff and the Class that their PII/PHI was stolen. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injuries by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

68. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

69. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII/PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor

[20] *2019 Internet Crime Report* (Feb. 11, 2020) FED. BUREAU INTELLIGENCE, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited June 18, 2026).

their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

70. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII/PHI. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

71. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

72. In 2024, a record 3,158 data breaches occurred—exposing approximately 1,350,835,988 sensitive records (i.e., 211% increase year over year).[21]

73. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[22]

74. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendant.

Defendants Could Have Prevented the Data Breach

75. Data breaches are preventable.[23] Indeed, the American Bar Association published

---

[21] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.
[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[23] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (2012).

a treatise titled the *Data Breach and Encryption Handbook* wherein the author explained that:

a. "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[24]

b. "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[25]

c. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [26]

Defendants Failed to Follow FTC Guidelines

76. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

77. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices

[24] *Id.* at 17.
[25] *Id.* at 28.
[26] *Id.*

businesses must use.[27] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

78. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

79. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

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

[27] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

81. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to their current and former patients and employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

82. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

83. Other industry standard best practices 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; and training staff regarding critical points.

84. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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 frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby

causing the Data Breach.

Defendants Violated HIPAA

86. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[28]

87. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[29]

88. The Data Breach resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of

[28] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[29] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

89. Simply put, the Data Breach resulted from a combination of insufficiencies that

demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

90. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach that impacted Defendants in or around June 2026, including all those individuals who received notice of the breach.

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

92. Plaintiff reserves the right to amend the class definition.

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

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

95. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least one thousand members.

96. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

97. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

98. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

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

c. if Defendants were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendants breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or

injunctive relief.

99. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

101. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to Defendants on the premise and with the understanding that Defendants would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

102. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendants' failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

103. Defendants has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

104. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiff and Class Members' PII/PHI.

105. Defendants owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in their care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

106. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

107. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

108. Defendants knew or reasonably should have known that the failure to exercise due

care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

109. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendants with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

110. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendants hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII/PHI —whether by malware or otherwise.

111. PII/PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

112. Defendants improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendants breached these duties as evidenced by the Data Breach.

114. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in their employ who were responsible for making that

happen.

115. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

116. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

117. Defendants has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

118. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

119. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

120. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

122. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII/PHI.

123. Section 5 of the FTC Act 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 the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the Class Members' sensitive PII/PHI.

124. Defendants breached their respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

125. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

126. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

127. But for Defendants' wrongful and negligent breach of their duties owed, Plaintiff and Class Members would not have been injured.

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

129. Similarly, under HIPAA, Defendants had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

130. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of PHI that Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

131. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

132. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

133. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

134. Plaintiff and Class Members (or their third-party agents) were required to provide their PII/PHI to Defendants as a condition of receiving services and/or employment provided by

Defendant. Plaintiff and Class Members (or their third-party agents) provided their PII/PHI to Defendants or their third-party agents in exchange for Defendants' services and/or employment.

135. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid and/or derived from their labor would be used to pay for adequate cybersecurity measures.

136. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

137. Plaintiff and the Class Members (or their third-party agents) accepted Defendants' offers by disclosing their PII/PHI to Defendants or their third-party agents in exchange for services and/or employment.

138. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII/PHI to unauthorized persons.

139. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

140. After all, Plaintiff and Class Members (or their third-party agents) would not have entrusted their PII/PHI to Defendants (or their third-party agents) in the absence of such an agreement with Defendant.

141. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

142. The covenant of good faith and fair dealing is an element of every contract. Thus,

parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

143. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

144. Defendants materially breached the contracts it entered with Plaintiff and Class Members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into their computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendants created, received, maintained, and transmitted.

145. In these and other ways, Defendants violated their duty of good faith and fair dealing.

146. Defendants' material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

147. And, on information and belief, Plaintiff's PII/PHI has already been published—or

will be published imminently—by cybercriminals on the Dark Web.

148. Plaintiff and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

149. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

150. This claim is pleaded in the alternative to the breach of implied contract claim.

151. Plaintiff and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendants benefitted from (1) using their PII/PHI to provide services and/or facilitate employment, and (2) accepting payment and/or using their labor to derive profit.

152. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

153. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

154. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI.

155. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

156. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII/PHI and (2) employment and/or payment because Defendants failed to adequately protect their PII/PHI.

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

158. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of their misconduct.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

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

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

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

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

F. Awarding attorneys' fees and costs, as allowed by law;

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

H. Granting Plaintiff 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.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: June 18, 2026

Respectfully submitted,

By: /s/ *Mark K. Svensson*

Mark K. Svensson
MILBERG, PLLC
405 East 50th Street
New York, New York 10022
Phone: (202) 975-0468
Email: msvensson@milberg.com

Attorneys for Plaintiff and Proposed Class

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MARY STERNER, on behalf of herself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Out of State
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Mark K. Svensson, MILBERG, PLLC
405 East 50th Street, New York, New York 10022
Phone: (202) 975-0468

DEFENDANTS

NOVO NORDISK, INC. and NOVO NORDISK A/S

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. Georgette Castner DOCKET NUMBER 3:26-cv-07280-GC-JBD

DATE
Jun 18, 2026

SIGNATURE OF ATTORNEY OF RECORD
/s/ Mark K. Svensson

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of New Jersey

MARY STERNER, on behalf of herself and all others similarly situated,

Plaintiff

v.

NOVO NORDISK INC. and NOVO NORDISK A/S,

Defendant

Civil Action No. 3:26-cv-7353

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* NOVO NORDISK INC. and NOVO NORDISK A/S

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Mark K. Svensson
MILBERG, PLLC
405 East 50th Street
New York, New York 10022

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:26-cv-7353

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

.

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: