IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

CONNER MASCIOTRA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

VERTAFORE, INC., a Delaware corporation,

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Conner Masciotra ("Plaintiff"), individually and on behalf of all others similarly situated, asserts the following against Defendant Vertafore, Inc. ("Vertafore" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiff brings this Class Action Complaint on behalf of Texas drivers harmed as a result of Vertafore's failure to safeguard and protect their private and confidential information, including State of Texas driver's license numbers, names, dates of birth, addresses, and vehicle registration histories (collectively "personal information").

2. On November 10, 2020, Vertafore announced that it had stored Plaintiff's and Class members' personal information on an unsecured external server that was accessed by unauthorized third parties sometime between March 11, 2020 and August

1, 2020. As a result of Vertafore's conduct, approximately ***27.7 million*** Texas drivers' personal information were disclosed to and accessed by unknown third parties without authorization (the "Data Breach").

3. Vertafore failed to discover the Data Breach until mid-August and only confirmed publicly— ***nearly three months later***—that as a result of their negligence, the unsecured external server storing Plaintiff's and Class members' personal information was accessed by third parties without authorization. As a result of this delay, Plaintiff and Class members were not provided adequate notice that their personal information was compromised for several months and were unable to take steps to proactively mitigate the harm caused by the Data Breach.[1]

4. Vertafore acted negligently in failing to adopt reasonable security protocols to prevent and detect the Data Breach. Had Vertafore taken these measures, Plaintiff and Class members would not have been harmed.

5. Additionally, Vertafore's actions violate the federal Driver's Privacy Protection Act, 18 U.S.C. § 2721, *et seq.* ("DPPA"), which regulates obtaining and disclosing personal information gathered by state departments of motor vehicles. Under the DPPA, it is unlawful for an organization, like Vertafore, to knowingly disclose personal information contained in motor vehicle records for any purpose not specifically enumerated under 18 U.S.C. § 2721(b), none of which are applicable here.

[1] As Vertafore has failed to determine the exact date unauthorized third parties accessed Plaintiff's and Class members' personal information and has only narrowed it down to a window between March and August of this year, Plaintiff and Class members may not have received notice for nearly ***eight months*** since their personal information was compromised.

6. As Vertafore has admitted that unauthorized third parties have accessed Plaintiff's and Class members' personal information, Plaintiff and Class members have sustained immediate, tangible injury as a result of the Data Breach. Plaintiff and Class members have or will be required to expend significant effort, including, among other things, replacing driver's license numbers, installing identity theft protection, closely reviewing financial accounts, and placing "freezes" and "alerts" with credit reporting agencies to mitigate the effects of the Data Breach. This injury is ongoing as Plaintiff and Class members also face a significant and imminent risk of identity theft and fraud, as demonstrated by the fact that unauthorized third parties have already accessed their personal information from Vertafore's unsecured server.

7. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose personal information was stolen as a result of the Data Breach. Plaintiff and Class members seek remedies including reimbursement of losses due to identity theft and fraud and other out-of-pocket costs, including compensation for time spent in response to the Data Breach, credit monitoring and identity theft insurance, and injunctive relief requiring substantial improvements to Vertafore's security systems.

PARTIES

8. Plaintiff Conner Masciotra is a natural person and citizen of the State of Texas and a resident of Dallas County. Since approximately 2017, Plaintiff Masciotra has had a Texas driver's license.

9. Defendant Vertafore, Inc. is an insurance software provider, and is incorporated in Delaware with its principal place of business located in Denver, Colorado.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under the laws of the United States, namely the Driver's Privacy Protection Act, 18 U.S.C. § 2721, *et seq*.

11. The Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367(a), since Plaintiff's state law claims are so related to the claims in the action within the Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

12. The Court has personal jurisdiction over Defendant because: (1) Defendant maintains its principal places of business in Colorado; (2) Defendant conducts substantial business in and throughout Colorado; and (3) the wrongful acts alleged in the Complaint were committed largely in Colorado.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

A. Vertafore's Data Breach

14. Vertafore is an insurance software provider that offers an array of products and services, including "agency management, ratings, regulation, compliance, data and

analytics, and connectivity products" designed to "streamline workflows, improve efficiency and drive productivity."[2]

15. In connection with providing insurance ratings solutions to its clients, Vertafore has access to and stores the personal information of Texas drivers.

16. While Vertafore claims to "respect[] [individual's] privacy" [3] and take "data privacy and security very seriously," [4] it failed to take even the most rudimentary steps to protect this information. Specifically, Vertafore failed to properly train its employees in data security and adopt reasonable security measures designed to prevent and detect a data breach.

17. As a result of these deficiencies, Vertafore improperly stored Plaintiff's and Class members' personal information on an unprotected external server. Consequently, sometime between March 11, 2020 and August 1, 2020, unknown third parties acquired Plaintiff's and Class members' personal information without authorization.[5]

18. According to Vertafore, the files "included driver information for licenses issued before February 2019, contained Texas driver license numbers, as well as names, dates of birth, addresses and vehicle registration histories."[6]

---

[2] *Press Release*, *Vertafore Statement Regarding Data Event*, VERTAFORE (Nov. 10, 2020), https://www.vertafore.com/resources/press-releases/vertafore-statement-regarding-data-event (hereinafter "Press Release").
[3] *Privacy Statement*, VERTAFORE, https://www.vertafore.com/privacy-statement (last visited Dec. 8, 2020).
[4] *Press Release*, *supra* note 2.
[5] *Id.*
[6] *Id.*

19. The unauthorized third parties were ultimately able to acquire the personal information of approximately ***27.7 million individuals*** as a result of Vertafore's negligence.[7]

20. Even though the unauthorized third parties accessed Plaintiff's and Class members' personal information sometime between March 11, 2020 and August 1, 2020, Vertafore failed to discovery the Data Breach until at least mid-August of this year.

21. Furthermore, despite knowing of the Data Breach since mid-August, Vertafore failed to notify Plaintiff and Class members that their personal information had been compromised until November 10, 2020. As a result of this delay, Plaintiff and Class members had no notice whatsoever that their personal information had been compromised for months on end and were unable to take steps to proactively mitigate the harm caused by Vertafore's Data Breach.

22. Unlike credit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of information at stake here—unique Texas state driver's license numbers, as well as names, dates of birth, addresses and vehicle registration histories—are either irreplaceable or cannot be easily replaced.

23. For example, in the State of Texas, to replace a driver's license (and the driver's license number) that has been stolen or used by someone else, an individual must file a police report. They must then: (1) complete an application; (2) make an appointment at a local driver's license office; (3) provide documentation to a license and

[7] *Id.*

permit specialist, including forms of identification and the police report; (4) provide a thumbprint; (5) have a picture taken; and (6) pay the application fee. Even then, it is not guaranteed that the driver's license office will replace the driver's license number. Rather, the "driver license personnel will determine if it is necessary to issue a new number when reviewing [the individual's case]."[8] In this case, that would be ***27.7 million individual applications***.

24. Moreover, driver's license numbers are unique to a specific individual and extremely sensitive. As *Experian*, a globally recognized credit reporting agency, has explained, "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves."[9] This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the Department of Motor Vehicles, places of employment, doctor's offices, government agencies, and other entities.[10] For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud.

25. Since Vertafore has admitted that unauthorized third parties have accessed Plaintiff's and Class members' personal information, including driver's license numbers, Plaintiff and Class members have sustained immediate, tangible harm as a

---

[8] *How to replace your Driver License, Commercial Driver License or ID Card*, TEXAS DEPT' PUBLIC SAFETY, https://www.dps.texas.gov/driverlicense/replace.htm (last visited Dec. 8, 2020).
[9] Sue Poremba, *What Should I Do if My Driver's License Number is Stolen*, EXPERIAN, (Oct. 24, 2018), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Dec. 8, 2020).
[10] *Id.*

result of the Data Breach. Plaintiff and Class members have or will be required to expend considerable, time-consuming efforts to, among other things, replace their driver's license numbers, install identity theft protection and credit monitoring, review financial accounts, and place "freezes" and "alerts" with credit reporting agencies to mitigate the effects of the Data Breach.[11] Plaintiff and Class members are also at a substantial and imminent risk of identity theft and fraud, as demonstrated by the fact that unauthorized third parties have already had access to their personal information—possibly for months—without detection.

B. Vertafore Was on Notice of the Significant Risk of a Data Breach

26. Vertafore, a company that handles data "for more North American insurance professionals than any other provider—including more than 20,000 agencies, over 1,000 carriers, and 23 state governments" was—and at all relevant times has been—aware that the personal information that it obtains and processes, including driver's license numbers, is highly sensitive and could be used for nefarious purposes by unauthorized parties, such as perpetrating identity theft and making fraudulent purchases.

27. Vertafore also was—and at all relevant times has been—aware of the importance of safeguarding the personal information that it stores and of the

[11] Indeed, Experian recommends that if an individual's driver's license number is compromised, to sign up for credit monitoring and report to the state's department of motor vehicles that the number has been stolen. Poremba, *supra* note 9.

foreseeable consequences that would occur if its data security systems were breached, including the fraud losses and theft that would be imposed on Texas drivers.[12]

28. Vertafore's data security obligations were particularly important and well-known given the numerous data breaches concerning department of motor vehicle records, including two breaches in 2016 and 2018, where a vendor for Florida's Department of Highway Safety and Motor Vehicles improperly disclosed individuals' driving records. Perhaps most notably, the *Equifax* data breach disclosed in 2017 was particularly notorious in part because it involved the driver's license numbers of more than 10.9 million U.S. consumers.

29. Vertafore was also aware of the importance of properly configuring its servers to prevent unauthorized access. There have been dozens of reported data breaches this year alone resulting from misconfigured servers, like Vertafore's sever, including the *BlueKai* data breach which exposed billions of records as a result of an unsecured server.

30. Additionally, the FTC publishes guidelines that establish reasonable data security practices for businesses that put Vertafore on notice of the importance of adopting reasonable security measures. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved

[12] As Experience also notes, it is the obligation of the organization that stores driver's license numbers to "provide protection for the information that it stores." *Id.*

patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

31. These warnings and guidelines, among others, put Vertafore on notice that it may be susceptible to a data breach and of the importance of prioritizing data security to prevent a breach. Despite Vertafore's knowledge of the likelihood that personal information would be stolen without reasonable security measures, Vertafore failed to implement these measures which would have prevented the Data Breach.

C. Vertafore's Inadequate Data Security Practices

32. Vinay Sridhara, Chief Technology Officer of the leading data breach security firm *Balbix* explained in an article for the *Digital Journal* that the Vertafore Data Breach "is yet another example of a company leaving a server and critical information unsecured without any protection, an unfortunate trend that has been the cause of many recent breaches."[14]

33. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm *Aite Group* has stated: "'If

[13] The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.
[14] Tim Sandle, *Looking behind the Vertafore data breach*, DIGITAL JOURNAL (Nov. 21, 2020), http://www.digitaljournal.com/tech-and-science/technology/looking-behind-the-vertafore-data-breach/article/581178.

your data was stolen through a data breach that means you were somewhere out of compliance."[15]

34. Vertafore's Data Breach can be attributed to deficient data security, inadequate data storage practices, and lax employee training and policies.

35. Up to, and including, the period during which the Data Breach occurred, Vertafore breached its duties, obligations, and promises to Plaintiff and Class members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of unsecured data storage, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques unauthorized parties use to gain unauthorized access;

c. address well-known warnings that its unsecured servers were suspectable to a data breach;

d. implement certain protocols that would have prevented unauthorized access to Plaintiff's and Class members' personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data; and

f. adequately safeguard personal information and maintain an adequate data security environment to reduce the risk of a data breach.

[15] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017) https://www.reuters.com/article/us-chipotle-cyber/chipotle-says-hackers-hit-most-restaurants-in-data-breach-idUSKBN18M2BY.

D. The Data Breach Damages Plaintiff and Class Members

36. As a result of Vertafore's deficient security measures and failure to timely and adequately detect the Data Breach, Plaintiff and Class members have been harmed by the compromise of their personal information.

37. Plaintiff and Class members face a substantial and imminent risk of identity theft and fraud. Unauthorized individuals carried out the Data Breach and stole the personal information of Plaintiff and Class members with the intent to use it for fraudulent purposes and/or sell it to other cyber criminals. The risk of identity theft is particularly substantial as the personal information compromised, including driver's license numbers, are highly coveted pieces of information for cyber criminals because they are readily usable to perpetrate fraud or identity theft.

38. Moreover, identity thieves can combine the personal information stolen in the Data Breach with other information about Plaintiff and Class members gathered from underground sources, public sources, or even Plaintiff's and Class members' social media accounts to compile a "profile," of someone's personal information which they can then monetize for nefarious purposes. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class members to obtain more sensitive information. Thieves can also use the combined data, of which the personal information stolen in the Data Breach is a significant component, to commit potential crimes including, including but not limited to, opening new financial accounts in Plaintiff's and Class members' names, taking out loans in Plaintiff's and Class members'

names, using Plaintiff's and Class members' information to obtain government benefits, filing fraudulent tax returns using Plaintiff's and Class members' information, obtaining false driver's licenses in Plaintiff's and Class members' names but with another person's photograph, filing a false car insurance claim, improperly gaining title to a vehicle, and giving false information to police during an arrest.

39. Plaintiff and Class members have or will spend substantial amounts of time replacing their driver's license numbers, monitoring their accounts for identity theft and fraud, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

40. Also, many Class members will incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

41. Plaintiff and Class members also suffered a "loss of value" of their personal information in the Data Breach. A robust market exists for stolen personal information, which is sold on the "dark web" at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiff and Class members.

42. Class members who experience actual identity theft and fraud will also be harmed by the inability to use their information when their accounts are suspended or otherwise rendered unusable due to the fraudulent charges. To the extent Class members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class members will also be harmed by the loss of use of and access to their

account funds and credit lines or being limited in the amount of money they are permitted to obtain from their accounts. Class members will further be harmed by the loss of rewards points or airline mileage available on credit cards that they lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards. Adverse effects of the Data Breach may also include missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

43. The stolen sensitive personal information is a valuable commodity to identity thieves. Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[16] The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cyber criminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of

[16] *See* Attorney General William P. Barr Announces Indictment of Four Members of China's
Military for Hacking into Equifax, U.S. DEPT. OF JUSTICE (Feb. 10, 2020)
https://web.archive.org/web/20200304134007/https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."[17]

44. In the case of a data breach, merely reimbursing an individual for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[18]

45. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts *ad infinitum*.

CLASS ACTION ALLEGATIONS

46. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this class action individually and on behalf of the following Nationwide Class of individuals (the "Class"):

> All individuals in the United States whose personal information was compromised in the Data Breach made public by Vertafore on November 10, 2020.

---

[17] *See Legislator, security expert weigh in on Rutter's data breach*, ABC 27 NEWS, (last updated Feb. 17, 2020 8:47 AM), https://www.abc27.com/news/local/york/legislator-security-expert-weigh-in-on-rutters-data-breach/.

[18] *See* Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft*, 2012, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Dec. 2013), at 1.

47. Excluded from the Class is Vertafore and its subsidiaries and affiliates; all employees of Vertafore and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Class; government entities; and the Judge to whom this case is assigned, including his/her immediate family and Court staff.

48. Plaintiff reserves the right to modify, expand or amend the above Class definition or to seek certification of a Class or subclasses defined differently than above before any Court determines whether certification is appropriate following discovery.

49. Certification of Plaintiff's claims for Class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiff can prove the elements of his claims on a Class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

50. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are likely millions of members of the Class, the precise number of Class members is unknown to Plaintiff. However, Vertafore has admitted that the Data Breach has compromised the personal information of approximately 27.7 million people. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

51. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Vertafore engaged in the wrongful conduct alleged herein;

b. Whether Vertafore owed a duty to Plaintiff and Class members to safeguard their personal information;

c. Whether Vertafore breached its duty to Plaintiff and Class members to safeguard their personal information;

d. Whether unauthorized third parties obtained Plaintiff's and Class members' personal information in the Data Breach;

e. Whether Vertafore knew or should have known that its data security systems, employee protocols and training, and data security monitoring processes were deficient;

f. Whether Vertafore knowingly disclosed Plaintiff's and Class members' personal information for a purpose not permitted under the DPPA;

g. Whether Vertafore's failure to provide adequate data security proximately caused Plaintiff's and Class members' injuries; and

h. Whether Plaintiff and Class members are entitled to damages and equitable relief and, if so, in what nature and amount.

52. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class. Plaintiff's claims are typical of the claims of all Class members because Plaintiff, like other Class members, suffered theft of his personal information in the Data Breach.

53. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because he is a

member of the Class and his interests do not conflict with the interests of other Class members that he seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and his counsel, will fairly and adequately protect the Class's interests.

54. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Vertafore, so it would be impracticable for members of the Class to individually seek redress for Vertafore's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

55. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Vertafore has acted, or refused to act, on grounds generally applicable to the Class such that final declaratory or injunctive relief appropriate.

CAUSES OF ACTION

COUNT I
Negligence

56. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

57. Vertafore obtained Plaintiff's and Class members' personal information in connection with the insurance software products and services it provides to its clients.

58. By collecting and maintaining personal information, Vertafore had a duty of care to use reasonable means to secure and safeguard the personal information and to prevent disclosure of the information to unauthorized individuals. Vertafore's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

59. Vertafore owed a duty of care to Plaintiff and Class members to provide data security consistent with the various requirements and standards discussed above.

60. Vertafore's duty of care arose as a result of, among other things, the special relationship that existed between Vertafore and Texas driver's license holders whose information Vertafore stored. Vertafore was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to Plaintiff and the Class.

61. Vertafore's duty to use reasonable care in protecting personal information arose as a result of the common law, statutes, and standards described above.

62. Vertafore breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' personal information. Vertafore's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against unauthorized access on unsecured systems;

b. failure to comply with industry standards and best practices for data security;

c. failure to track and monitor access to its network and files;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

g. failure to recognize that unauthorized third parties were stealing personal information from its servers while the Data Breach was taking place; and

h. failure to timely notify Plaintiff and Class of the Data Breach.

63. It was foreseeable to Vertafore that a failure to use reasonable measures to protect Plaintiff's and Class member's personal information could result in injury to Plaintiff and the Class. Further, actual and attempted breaches of data security were reasonably foreseeable to Vertafore given the known frequency of data breaches and various warnings from industry experts.

64. Plaintiff and Class members suffered various types of damages as alleged above.

65. Vertafore's wrongful conduct was a proximate cause of Plaintiff's and Class members' damages.

66. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

67. Plaintiff and Class members are also entitled to injunctive relief requiring Vertafore to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) develop and implement sufficient security training and protocols; and (iv) provide several years of free credit monitoring and identity theft insurance protection to all Class members.

COUNT II
Violation of the Driver's Privacy Protection Act
18 U.S.C. § 2721, *et seq.*

68. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

69. DPPA, 18 U.S.C. § 2722(a) provides that "it shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of [the DPPA]."

70. The DPPA defines "person" to mean "an individual, organization or entity." 18 U.S.C. § 2725(2). Vertafore is a "person" under the DPPA.

71. The DPPA defines "motor vehicle record" to mean "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). The records that Vertafore obtains and stores from the Texas Department of

Motor Vehicles, containing Plaintiff's and Class members' personal information—including driver's license numbers motor vehicle registration histories, —constitute "motor vehicle records" under the DPPA.

72. The DPPA defines "personal information" to mean "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3). Plaintiff's and Class members' personal information, which includes driver's license numbers, names, and addresses falls within this definition.

73. Vertafore knew Plaintiff's and other Class members' personal information was obtained from the Texas Department of Motor Vehicles, as the files were provided so that Vertafore could offer insurance rating solutions and contained Texas driver information for approximately 27.7 million people.

74. In violation of the DPPA, Vertafore knowingly disclosed the personal information of Plaintiff and approximately 27.7 million other Class members by storing that information on unsecured external servers that was accessed by third parties.

75. Section 2721(b) of the DPPA provides for certain permissible uses of personal information. Vertafore's knowing disclosure of Plaintiff's and Class members' personal information to unauthorized third parties is not one of the permissible uses under Section § 2721(b). Therefore, Vertafore is in violation of 18 U.S.C. § 2722(a) of the DPPA.

76. Pursuant to 18 U.S.C. § 2724(b)(1)-(4), as a result of Vertafore's violation of the DPPA, Plaintiff and Class members are entitled to (1) actual damages, but not less than liquidated damages in the amount of $2,500, (2) punitive damages, (3) attorneys' fees and costs, and (4) such other preliminary and equitable relief as the Court determines to be appropriate.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Vertafore including the following:

A. Determining that this matter may proceed as a Class Action and certifying the Class asserted herein;

B. Appointing Plaintiff as Class Representative and appointing Plaintiff's counsel as Class Counsel;

C. An award to Plaintiff and the Class of compensatory, consequential, statutory, punitive, and liquidated damages as set forth above;

D. Ordering injunctive relief requiring Vertafore to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) develop and implement sufficient security training and protocols; and (iv) provide several years of free credit monitoring and identity theft insurance protection to all Class members;

E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Such other preliminary and equitable relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury as to all issues so triable.

Dated: December 8, 2020

Respectfully submitted,

/s/ Amanda Fiorilla
Amanda Fiorilla
Christian Levis
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: afiorilla@lowey.com
clevis@lowey.com

Anthony M. Christina
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

Counsel for Plaintiff Conner Masciotra and the Proposed Class

JS 44 (Rev. 10/20) District of Colorado

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

Conner Masciotra

(b) County of Residence of First Listed Plaintiff Dallas County, TX
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Amanda Fiorilla, Lowey Dannenberg, P.C., 44 South Broadway, Suite 1100, White Plains, NY 10601, 914-997-0500

DEFENDANTS

Vertafore, Inc.

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

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)***:
Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721, et seq.

☐ AP Docket

Brief description of cause:
Defendant improperly disclosed Plaintiff's and Class's driver's license information in violation of the DPPA

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Hon. George C. Hanks, Jr. (S.D. Tex.) DOCKET NUMBER 4:20-cv-04139

DATE 12/8/2020

SIGNATURE OF ATTORNEY OF RECORD /s/ Amanda Fiorilla

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 statue.

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 pending cases, if any. If there are related pending 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. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Colorado

Conner Masciotra, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

Vertafore, Inc., a Delaware corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Vertafore, Inc.
c/o Corporation Service Company
251 Little Falls Drive
Wilmington, DE 19808

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: Amanda Fiorilla, Esq.
Lowey Dannenberg, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
914-997-0500; afiorilla@lowey.com

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.

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:

Print Save As... Reset

ClassAction.org