IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

Aaron Mulvey, individually, and on behalf of himself and all others similarly situated individuals, Plaintiff, V. VERTAFORE INC., Defendant.	**CLASS ACTION COMPLAINT** JURY DEMAND

COMPLAINT—CLASS ACTION COMPLAINT

"In August 2019, Vertafore sent the department a letter stating Vertafore merged with QQ Solutions (the merger apparently occurred in 2015). David Richards provided guidance at the time that Vertafore needed to send in a new application, new contract, and new escrow deposit under the new name. In November 2019, VTR requested additional information from QQ Solutions regarding their use of motor vehicle data, since their account was still active. Due to QQ Solutions' failure to respond, QQ Solutions' account was suspended on 11/27/19 and terminated on 2/11/20…."

Dilip Kanuga || Program Specialist - Registration Services
Texas Department of Motor Vehicles Vehicle Titles and Registration
March 10, 2020

Joseph H. Malley (TX State Bar No. 12865900)
Law Offices of Joseph H. Malley P.C.
1045 North Zang Blvd
Dallas, Tx 75208
Telephone: (214) 943-6100
malleylaw@gmail.com

Counsel for Plaintiff Aaron Mulvey, individually, and on behalf of a class of similarly situated individuals.

COMES NOW, Plaintiff, Aaron Mulvey, ("Plaintiff")[1], individually, and on behalf of himself and all others similarly situated individuals, by and through his attorney, Joseph H. Malley, counsel for the Law Offices of Joseph H. Malley, P.C., move for as and for his complaint, and demanding trial by jury, allege as follows upon information and belief, based upon, *inter alia*, investigation conducted by and through his attorney, which are alleged upon knowledge, bring this legal action against Defendant Vertafore Inc., ("Defendant").[2] Plaintiff's allegations as to himself and his own actions, as set forth herein, are based upon his personal knowledge, upon information and belief as to those of others, and all other allegations are based upon information and belief pursuant to the investigations of counsel[3] Based upon such investigations, Plaintiff believes that substantial evidentiary support exists for the allegations herein, or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and discovery.

I.
NATURE OF ACTION

1. Plaintiff brings this consumer Class Action lawsuit pursuant to the Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), applicable, and (c)(4), on behalf of himself

[1] Plaintiff Aaron Mulvey will hereinafter be referred to as "Plaintiff" or "Plaintiff Mulvey" in succeeding references.

[2] Defendant Vertafore Inc. will hereinafter be referred individually to as "Defendant Vertafore" in succeeding references.

[3] Plaintiff's Counsel has experience involving DPPA litigation requiring research that includes open records requests from DMVs nationwide. On November 10, 2020, after receiving an alert concerning Defendant Vertafore's "alleged" Data Event. involving the entire database of TXDMV driver licenses and motor vehicle registration data, an immediate investigation determined QQ Solutions Inc, formerly a "Bulk Requestor" of TXDMV data, a merged entity that was dissolved when purchased by Defendant Vertafore in 2015, may still be acting as a "Reseller," although its contract with the TXDMV would have terminated upon its purchase. Since Defendant Vertafore was not cited with open records requests responses as a Bulk Requestor, litigation was delayed, and further investigation required. Documents related to Defendant Vertafore's contractual status with the TXDMV, or lack thereof, in January 2021.

and a proposed class of similarly situated individuals, ("Class members")[4], seeking redress for the unlawful and negligent obtainment, use, and redisclosure of millions of Texas resident's Personal Identifying Information ("PII")[5] and sensitive information,[6] a "Data Event"[7] that reportedly included the names, addresses, dates of birth, vehicle registrations, vehicle registration histories, and driver's license numbers issued before February 2019 involving 27.7 million Texas residents[8], in short, the *entire* database of the Texas Department of Motor Vehicles,[9] was compromised, reportedly the event beginning on March 11, 2020, the result of glaring weaknesses and vulnerabilities in Defendant Vertafore's data computing systems, described more fully in the following sections.

2. Specifically, on November 10, 2020, Defendant Vertafore announced publicly in a press release[10] that it was subject to one of the largest data events in Texas history, the severity

[4] Putative Class members of the Nationwide Class and the Nationwide Subclass shall hereinafter be referred to as "Class members" or the "Class" in succeeding references.

[5] As used throughout this Complaint, Personal Identifying Information ("PII") is defined as all information exposed by the Defendant Vertafore Data Event, including all or any part or combination of name, address, birth date, driver's license information (any part of license number, dates of issuance or expiration), driver's vehicle registration, or documents with personally identifying information.

[6] Tex. Bus. & Com. Code § 521.052 DEFINITIONS. (2) "Sensitive personal information" means, subject to Subsection (b)(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (ii) driver's license number or government-issued identification number

[7] Defendant Vertafore refers to the occurrence within its press release as a "Data Event", not a "Data Breach". The National Institute of Standards and Technology defines a "data event" as any *observable occurrence* in a system or network. The reason why Defendant Vertafore differentiated the reference to the occurrence will be described more fully in the following sections.

[8] Aravind Swaminathan, an attorney with Orrick, Herrington, & Sutcliffe, Defendant Vertafore's Counsel, submitted formal notice to the TXDMV on 11/10/20, first notice was a phone call on 10/16/20. The letter noted 27.7 million people, as well as 26.5 million lien holders and 45.9 million vehicle registration histories involved in the Data Event. Copy of the letter obtained by an open records request.

[9] Texas Department of Motor Vehicles ("TXDMV") maintains confidential personal information for all licensed drivers and vehicle owners in its Registration and Title System (RTS). An authorized entity may contract with the TXDMV and receive an electronic downloadable tile containing the confidential information in this system in totality, along with weekly updates, which keep the information current over time.

[10] "Vertafore Statement Regarding Data Event", (First accessed November 10, 2020), online: https://www.vertafore.com/resources/press-releases/vertafore-statement-regarding-data-event. Defendant Vertafore claimed that Social Security numbers or financial account information was not obtained, although 26.5 million lienholders records, information that could bear on a user's credit worthiness, was obtained. Such was noted because Defendant Vertafore acts as an integrated consumer reporting agency ("CRA") that prepares and furnishes consumer reports for credit and other purposes. As such, Defendant Vertafore Inc is both a "consumer reporting agencies" and "nationwide reporting agencies" as defined by the Fair Credit Reporting Act ("FCRA").

unprecedented, affecting most, if not all, of the Texas adult population. Reportedly, databases of PII involving Texas consumers were accessed, without authorization. The public concern being, using this information, identity thieves can then create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's insurance-worthiness—the very thing Defendant Vertafore exists to assess and report. And because some of their PII is not able to be replaced, such as driver license and vehicle registration numbers, thieves will be able to do so for years to come. On a scale of 1 to 10, in terms of risk to consumers, this data event was a 10.

3. Within its press release, Defendant Vertafore stated that in mid-August 2020 it was made aware of the "Data Event," by a "trusted third-party," refraining from disclosing the identity of the third-party. During this five (5) month period,[11] from the date of the breach to the initial notice of the breach, Defendant Vertafore claims to have failed to detect the unauthorized access of the massive amounts of data that were being exfiltrated from its computing system, reportedly delaying notice to involved consumers for 90 days to conduct an investigation while actively assisting law enforcement. A clarification of the actual events will be described more fully in the following sections.

4. This class action is brought by individuals throughout Texas whom suffered an invasion of a legally protected interest, and were victimized by these events, in order to redress the harm that they have suffered, and to obtain appropriate relief, risking that Defendant Vertafore will continue to obtain, use, and re-disclose motor vehicle records in its possession.

[11] *Coincidentally,* during this 5-month period, Defendant Vertafore was also finalizing its purchase by Roper Technologies Inc. for 5.3 billion dollars, the sale reportedly occurring on August 13, 2020, (hereinafter referred to as the "Quiet Period").

II.
PARTIES

5. Plaintiff Aaron Mulvey is a natural person, citizen of the State of Texas, residing in Dallas County, Texas. Plaintiff is a licensed and registered driver in the State of Texas. Plaintiff Mulvey's motor vehicle records were obtained by Defendant Vertafore Inc. and involved in the events, made the basis of this action.

6. Defendant Vertafore, a Delaware Corporation, headquartered in Colorado, doing business within this State during the Class Period. Defendant Vertafore can be served with process by serving its registered agent: Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware, 19808.

III.
JURISDICTION AND VENUE

1. As set forth herein, this Court has general jurisdiction over Defendant and original jurisdiction over Plaintiff's claims.

2. This Court has subject-matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

3. This Court has jurisdiction over the subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1331.

4. This Court has jurisdiction over Defendant, a Delaware corporation operating in the State of Colorado, doing business in Texas.

5. Plaintiff Mulvey is a citizen and resident of Dallas County, Texas, and asserts and claims on behalf of a proposed class whose members are domiciled within Texas. There is minimal diversity of citizenship between proposed Class members and Defendant .

6. This court has Federal question jurisdiction as the complaint alleges violations of the Violations of the Driver's Privacy Protection Act, 18 U.S.C.§2721, et. seq.

7. Subject-matter jurisdiction exists in this Court related to this action pursuant to 28 U.S.C. § 1332. The aggregate claims of Plaintiff and the proposed Class members exceed the sum or value of $5,000,000.00.

8. Venue is proper in this District, and vests jurisdiction in the State of Texas and Federal Courts in this district, under 28 U.S.C. §1391(b) and (c) against Defendant. A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred within this state, and within this district because: (1) 27.7 million Texas residents, the entire Class, reside and were harmed in the State of Texas; (2) A contract with the Texas Motor Vehicle Department to obtain the Plaintiff and Class member's motor vehicle records was consummated in Texas. (3) Defendant Vertafore obtained the database of Plaintiff and Class member's motor vehicle records involved in the Data Event from the Texas Motor Vehicle Department located in Texas. (4) Texas Motor Vehicle Department personnel involved with the Texas Motor Vehicle Department contract to obtain Plaintiff and Class member's personal information, fact witnesses, all reside in Texas; (5) Defendant conducts substantial business in and throughout Texas; and (6) the wrongful acts alleged in this complaint were committed largely in Texas. Thus, mandatory jurisdiction in this U.S. District Court vests for any Class Member, wherever they reside, which occurred within Texas.

9. Minimal diversity of citizenship exists in this action, providing jurisdiction as proper in the Court, since Defendant conducted activity within this state and in this district during the class period, and Plaintiff include citizens and residents of this state and district, and assert claims on behalf of a proposed class whose members; thus, there is minimal diversity of citizenship between proposed Class members and the Defendant .

10. This is the judicial district wherein the basis of the conduct complained of herein involving the Defendant was implemented, in whole or part. Motor vehicle motor vehicle records were obtained from this state and used within the state and district; therefore, evidence of conduct as alleged in this complaint is located in this judicial district.

IV.
FACTUAL BACKGROUND

A. Defendant Vertafore Collects, and Rediscloses PII for its Financial Gain

11. Defendant Vertafore plays a central role in the modern American economy, collecting and selling vast amounts of data about the most intricate details of consumers' financial lives, connecting every point within the insurance distribution channel.[12] The data—names, addresses, birthdates, social security numbers, drivers' license numbers, vehicle registration information, and more—contains the keys that unlock a consumer's identity,

[12] "Vertafore Honors Top Performing Insurance Agencies and Carriers at NetVU16" (Last accessed November 19, 2020), online: https://www.vertafore.com/resources/press-releases/vertafore-honors-top-performing-insurance-agencies-and-carriers-netvu1.

relied upon by third parties to make major financial decisions affecting almost all Texas consumers.

12. Defendant Vertafore reportedly provides a management system for data & analytics and distribution & compliance with integrated solutions for internal operations and information, including content management & workflow; rating & connectivity system to connect with partners across the insurance distribution chain, and as an insurance knowledge base. Its areas of expertise include agency and benefits management, connectivity and rating, content management and workflow, producer lifecycle management, and policy administration and billing.

13. Operating as an Insurance Software Solutions for Carriers, Agencies Brokers, MGAs, and MGUs, Defendant Vertafore reportedly develops software for more than 20,000 Insurance agencies, some 1,000 carriers, and managing general agents.[13] Defendant Vertafore's software involves an agency management and content management integration system that links agency management system domain entities (such as clients, policies, claims, vendors) to content management system content hierarchical structures (such as client files, policy folders, claims folders, vendor files). Because the extension of insurance relies on access to consumers' insurance files, the insurance industry has been referred to as the "linchpins" of the Texas financial system.

14. Defendant Vertafore recognized that the value of its company was inextricably tied to its massive trove of consumer data. For that reason, Defendant Vertafore has aggressively acquired companies with the goal of expanding into new markets and acquiring

[13] "Company Profile, Vertafore, Inc" (last accessed December 5, 2020), online: https://www.dnb.com/business-directory/companyprofiles.vertafore_inc.d1eb70eb5bfc5f7f00d2b395130f573f.html

proprietary data sources. One such acquisition, QQ Solutions Inc.,[14] headquartered in Deerfield Beach, FL. Defendant Vertafore became the surviving corporation of the merger, the separate existence of the subsidiary ceasing on August 31, 2015.[15]

15. QQ Solutions Inc., reportedly a leading provider of innovative and powerful agency management systems, offering software products that included QQCatalyst®, an agency management technology tool that incorporated enterprise grade databases, and QQ WebRater, reportedly, a comparative rater product to provide real-time quotes from over 150 carriers.

16. Defendant Vertafore's strategy of rapid expansion by adding new companies with additional data sources in order to increase profits came with one major caveat: an unwillingness to make corresponding investments in training of employees about cyber-security and data security to protect the highly sensitive information it continued to accumulate, including ignoring the legal implications of purchasing companies that had acquired restricted data. Defendant Vertafore's simple strategy: Gather as much personal data as possible and find new ways to sell it.

B. The Texas Department of Motor Vehicles determined Defendant Vertafore was not an "authorized recipient" to Obtain Plaintiff and Class member's motor vehicle records, pursuant to the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.

17. Defendant Vertafore's press release of November 10, 2020 refers only to a "Data Event" which originated between March 11, 2020 and August 2020, ("Data Event II.") Defendant Vertafore fails to provide notice as to "Data Event I," which involved Defendant

[14] On July 20, 2009, QuickQuote, Inc. changed its name to QQ Solutions Inc. See online: http://search.sunbiz.org/Inquiry/CorporationSearch/ConvertTiffToPDF?storagePath=COR%5C2009%5C0724%5C00166316.Tif&documentNumber=K33031, (last assessed January 6, 2021). QuickQuote Inc.had entered into a service contract for the purchase of Texas Motor vehicle Title and Registration (VTR) Database on December 23, 2004, the contract was subject to continuous automatic renewal.

[15] "Vertafore Acquires QQ Solutions (first assessed November 13, 2020), online: https://www.vertafore.com/resources/press-releases/vertafore-acquires-qq-solutions

Vertafore surreptitiously obtaining Plaintiff and Class member's motor vehicle records from the Texas Department of Motor Vehicles, accessing the records from the QQ Solutions Inc's SFTP portal, a continuous operation since 2015, an action without legal authority, violating the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.

18. The Texas Department of Motor Vehicle Department, in conjunction with the Office of the General Counsel for the Texas Department of Motor Vehicle Department conducted an extensive investigation[16] to determine if Defendant Vertafore was an "Authorized Recipient," qualified to obtain, use, and re-disclose motor vehicle records. The investigation included communications with representatives from Defendant Vertafore and encompassed the period from September 2018 to October 2020. *The investigation evidenced Defendant Vertafore was not an authorized recipient*, as such, any prior obtainment, use, or redisclosure of the motor vehicle records would involve a violation of the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq., (hereinafter referred to as "DPPA") including data involved in "Data Event II." The origin of such DPPA violations occurring on a continuous basis since August 31, 2015 when Defendant Vertafore acquired QQ Solutions, Inc.[17]

19. Defendant Vertafore's acquisition of QQ Solutions Inc. was premised upon its business model of aggregating vast amounts of data relating to consumers from various sources to create customer-concentric databases to facilitate its software, compiling that data in a usable format, and selling access to that information to those interested in making

[16] Coincidentally, this investigation included the period of Defendant Vertafore's "alleged" Data Event in March 2020, the same month representatives of the Texas Department of Motor Vehicles were in communication with Defendant Vertafore representatives related to the unauthorized access to Texas motor vehicle records, these communications continuing past August 2020 when Defendant Vertafore claims a "Trusted" Third-Party advised Defendant Vertafore of the Data Event.

[17] The DPPA does not have its own statute of limitations. Consequently, 28 U.S.C. § 1658(a)'s catchall statute of limitations applies. Subsection 1658(a) states the following: "Except as otherwise provided by law, a civil action arising under an Act of Congress . . . may not be commenced later than 4 years after the cause of action accrues." See; Foudy v. Miami-Dade County, 823 F.3d at 593.

insurance decisions, and other entities that use those reports to make decisions about individuals in a range of areas. One (1) source of data that fueled QQ Solutions Inc.'s technology, required for the actual continuous use of its software in order to maintain the integrity of the data, was the obtainment in bulk, and on a continuous basis, of motor vehicle records, (hereinafter referred to as "MVRs") held by State Department of Motor Vehicles, access and use of the data restricted by the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.[18]

20. Congress enacted the DPPA in order to restrict access to personal information contained within motor vehicle records[19]. One of the driving forces behind passage of the DPPA was when an obsessive fan of television star Rebecca Schaeffer that used her license plate number to obtain her address from the DMV and then gunned her down. *See* 140 CONG. REC. H2,518, 2,522, 2,526 (daily ed. April 20, 1994) (statements of Reps. Moran and Goss). Through the DPPA, certain entities' classes of data use are effectively "highly offensive" *per se.* Personal information, while legally available to state departments of motor vehicles, and authorized persons and entities, is to be held in trust by them, disclosable only for certain prescribed purposes. Disclosure to unauthorized recipients of this data is the trust which could be violated, subjecting persons to the risk that their data will be used against them. Further harm could take the form of something as mundanely annoying as junk mail or as serious as identity theft, stalking, or battery.

[18] 18 U.S.C. § 2721(a)-(c). Section 2721(a) is applicable to state departments of motor vehicles. *See id.* § 2721(a). Pursuant to section 2721(b), personal information may be disclosed to certain entities by a state department of motor vehicles. *See id.* § 2721(b). The Texas Motor Vehicle Records Disclosure Act (MVRDA) (Transportation Code, Chapter 730) was enacted by the 75th Texas Legislature, 1997, to implement the provisions of the federal Driver's Privacy Protection Act (DPPA) (18 U.S.C. Chapter 123).

[19] Generally, data released by the Texas Department of Motor vehicles to "Bulk Requestors," can include identification cards that are issued to *minor children.*

21. The DPPA's general prohibition on disclosure of personal information was subject to fourteen (14) exceptions[20]—the permissible purposes—which allowed for the limited disclosure of personal information contained within motor vehicle records. The DPPA also provided for liability for the obtain[ment], disclos[ure], or [use] of such records for unauthorized uses- a course of action, and a body of information, that was protected from improper access by state and federal law.[21] Without remedy for its negligent use, consumer's security and privacy would be violated by a multitude of companies — companies they have never heard of, companies they have no relationship with, and companies they would never choose to trust with their motor vehicle records, let alone their PII.

22. QQ Solutions Inc.[22] was a "Bulk Requestor" of motor vehicle records from the Texas Department of Motor Vehicles, referencing a person or entity that obtains the entire database, then periodic updates. The agreement[23] to obtain the motor vehicle records, the "SERVICE CONTRACT FOR THE PURCHASE OF TEXAS MOTOR VEHICLE TITLE AND REGISTRATION (VTR) DATABASE", included contact information, certification of use, restrictions, obligations,[24] and a Termination clause.[25] While the effect of termination

[20]One of the 14 exceptions is the Insurance Exception- "For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

[21] The Driver's Privacy Protection Act, 18 U.S.C. §2724(a) "sets forth the three elements giving rise to liability, i.e., that a defendant (1) knowingly obtained, disclosed or used personal information, (2) from a motor vehicle record, (3) for a purpose not permitted." See: Taylor v. Acxiom. Corp. 612 F.3d. 325. 5th Cir. 7/14/10. 5th Cir.

[22] In 2017, the Office of the General Counsel for the TXDMV responded to an open records request concerning all "Bulk Requestors" of MVRs for the previous 4 years, QQ Solutions was noted within the response as a bulk recipient of Texas Motor Vehicle records, this FOIA response re-accessed by Plaintiff Counsel on 11/10/2020.

[23] An open records request to the TXDMV for a copy of QQ Solutions Inc's evidenced none existed. Apparently QQ Solutions Inc. relied upon the continuous automatic renewal contract originally entered into on July 20, 2009 between QuickQuote, Inc. and the TXDMV.

[24] "The Purchaser shall immediately inform the State if the privacy protected personal information is redisclosed in violation of the DPPAs."

[25] "Automatic Termination. This contract will automatically terminate if the Purchaser ceases to conduct business, if the Purchaser substantially changes the nature of its business, if the Purchaser sells its business, if there is a significant change in the ownership of the Purchaser, of if the Purchaser dies. The Purchaser, its successor in interest, or its personal representative will immediately notify the State in writing of any change in status that would implicate this paragraph". Such then required the purchaser's successor in interest to apply for and execute a new contract.

permitted the Purchaser's successor in interest to be eligible to apply for obtainment of the MVRs, there were strict legal obligations required *prior to* purchasing a company which had previously acquired the motor vehicle record database. The Purchaser's successor would be required to give timely notice of the planned acquisition, permit the Texas Department of Motor Vehicles to determine if the successor had a DPPA permissible use to acquire the database of restricted consumer data,[26]rule out any non-permissible uses such as direct marketing. This would include an inquiry of RiskMatch™, one (1) of Defendant Vertafore's software products, and its use of the motor vehicle record database, due in part since the patent filing claimed, "Methods are disclosed for providing leads for insurance market participants."[27] Additional scrutiny would be also be applied by the Texas Department of Motor Vehicles towards Defendant Vertafore since it not only acts as a "Bulk Requestor", but also a "Bulk Re-Seller," of the motor vehicle records, referencing a person or entity that obtains the entire database of motor vehicle records, and periodic updates, from State Department of Motor Vehicles, then rediscloses such in bulk to "authorized recipients". Once the review was completed and approved, the parties would then need to execute a new purchase agreement, "Form VTR-275-K." Defendant Vertafore failed to properly comply

[26] States have a vested interested in protecting the sale of customer data when companies are purchased, reluctant to permit the sale of consumer data. See: "Attorney General Paxton Announces Agreement to Protect Consumer Privacy in RadioShack Case." (last assessed January 4, 2021), online: https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-announces-agreement-protect-consumer-privacy-radioshack-case.

[27] "Risk Match issued its 1st U.S. Patent" (last assessed January 6, 2021), U.S. Patent No: 8,666,788 B1, Abstract: "Methods are disclosed for providing leads for insurance market participants," online: https://www.vertafore.com/resources/press-releases/riskmatch-issued-its-1st-us-patent. Use of motor vehicle records, obtained from the State Department of Motor Vehicles, for direct marketing is strictly prohibited by the DPPA.

with the legal obligations to obtain the Texas motor vehicle records, a binding contract was never executed. [28]

23. On information and belief, Defendant Vertafore surreptitiously obtained the motor vehicle records for a period of about 5 years[29], knowingly accessing the QQ Solutions Inc's designated Secure File Transfer Program ("SFTP")[30] portal to download the data files provided by the Texas Department of Motor Vehicles to QQ Solutions Inc. Such unauthorized obtainment, use, and re-disclosure did not occur accidentally, nor inadvertently over a short period, but occurred knowingly over a period of many years. On September 5, 2018, Defendant Vertafore's Senior Vice President and General Counsel, Jayne Rothman, ("Rothman") sent initial notice to the Texas Department of Motor Vehicle concerning the purchase of QQ Solutions Inc., providing details that the acquisition had occurred on June 10, 2015, with a merger of QQ Solutions Inc. with and into Defendant Vertafore on September 1, 2015. Rothman then referenced the agreement between the Texas Department of Motor Vehicles and QQ Solution Inc.[31]

24. Defendant Vertafore's use of the QQ Solutions Inc's SFTP portal to obtain motor vehicle records intended for QQ Solutions Inc. was confirmed by an email dated March

[28] On January 6, 2021, the TXDMV General Counsel office responded to an open records request, submitted on November 13, 2020. The request concerned all authorized "Bulk Requestors" of MVRs for the previous 4 years. The document failed to list Defendant Vertafore.

[29] Defendant Vertafore's acquisition of QQ Solutions was effective August 31, 2015. The Texas Department of Motor Vehicles terminated QQ Solutions Inc's account was suspended on 11/27/19 and terminated on 2/11/20.

[30] Secure File Transfer Program ("SFTP") portal is a command-line interface client program to transfer files using the SSH File Transfer Protocol (SFTP), which runs inside the encrypted Secure Shell connection. It provides an interactive interface similar to that of traditional command-line FTP clients. The Texas Department of Motor Vehicles used such a program to transfer motor vehicle records, requiring the Bulk Requestor to provide network credentialing information, including an FTP address, User ID/Login, FTP Password, and an Encryption Key. The Bulk Requestor was then obligated to implement safety controls, restricting specific personnel's access to the SFTP in order to deter unauthorized access, to do otherwise would be negligent.

[31] Rothman's letter indicates a knowledge of contractual issues associated with the QQ Solutions Inc's contract with the Texas Department of Motor Vehicles occurring in 2018, however Defendant Vertafore continued to access QQ Solutions Inc's SFTP portal to obtain Plaintiff and Class member's motor vehicle records after this date, *emphasis added.*

6, 2020 from Dave Acker, ("Acker") Vice President & General Manager Information Solutions to Dilip Kanuga, ("Kanuga") program specialist-registration services, Texas Department of Motor Services, "*We have not been receiving the data from the SFTP site for quite a while…"* An additional email from Acker to Kanuga, dated March 11, 2020 [32] evidenced irregularities in the data processing process stated in part, "*over the past year we stopped getting the updates and we were told we needed to do a new contract."* Acker's statement evidenced that Defendant Vertafore's knowingly obtained the motor vehicle records from the Texas Department of Motor Vehicles, albeit accessing the QQ Solution's SFTP portal without authorization. Defendant Vertafore's obtainment ceased about February 2019.[33] Such statement acknowledged the period Defendant Vertafore was first placed on notice of irregularities in being able to access motor vehicle records from the Texas Department of Motor Vehicles, albeit unauthorized access, one (1) year before the date that Defendant Vertafore claimed was the initial occurrence of the "Data Event,"[34] and twenty-one (21) months before Defendant Vertafore provided actual notice to Texas consumers related to this occurrence.

25. On March 4, 2020, notice was provided to Defendant Vertafore concerning the termination of QQ Solutions Inc.'s access to Texas Motor Vehicle Records, sent to Defendant Vertafore's Senior Vice President and General Counsel, Jayne Rothman. Defendant Vertafore then *first* submitted a contract to legally obtain the motor vehicle records in bulk from the

[32] *Coincidentally*, the date of Acker's email to TXDMV, March 11, 2020, the date that Defendant Vertafore first claimed the "Data Event" occurred, is also the date that the Texas Department of Motor Vehicles terminated QQ Solution's account.

[33] *Coincidentally*, Defendant Vertafore's press release concerning the data event specified that the files, "included driver information for license issued before *February 2019.*"

[34] A data breach is defined by the Texas data breach notification law as "an unauthorized acquisition of computerized data," that compromises the "security, confidentiality, or integrity" of sensitive personal Information. Under the Texas data breach notification law, an entity must disclose any breach of system security, after discovering or receiving notification of the breach.

Texas Motor Vehicle Department. To date, Defendant Vertafore has not acquired a contract, but continues to use and re-disclose the motor vehicle records previously obtained. "Incident #00235104" was closed on March 9, 2020 by the Texas Department of Motor Vehicles, an internal email, sent from Kanuaga to David Richards ("Richards"), Texas Department of Motor Vehicles Associate General Counsel, provided the results of the internal investigation, "Vertafore submitted their 275-K on 2/18/20. QQ Solution Inc's access to Texas motor vehicle records was suspended on November 27, 2019, effectively terminated on February 11, 2020."

26. Defendant Vertafore's press release of November 10, 2020 discussed in detail the extent of the data accessed, and assurances that financial information had not been accessed, "The files, which 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. They did not contain any Social Security numbers or financial account information. No information misuse has been identified. No customer data nor any other data—including partner, vendor, or other supplier data—or systems hosted for them were impacted. Additionally, no Vertafore system vulnerabilities were identified." Omitted from this notice, aside from failing to quantify the amount of vehicle registration histories accessed as 45.9 million, is mention of 26.5 million lien holder records.[35]

27. The Texas Department of Motor Vehicles requires a contract to obtain lienholder data, titled "State of Texas Department of Motor Vehicles Electronic Lien and Title

[35] "Lienholders", online: https://www.txdmv.gov/lienholders (last accessed January 29, 2021). The Electronic Lien and Title Program (ELT) is a paperless method that allows TXDMV and a financial institution or lienholder to exchange vehicle title information electronically. The title record is sent electronically, and the lienholder stores the electronic record instead of a paper certificate of title. The electronic title is created and held by TXDMV in the state motor vehicle database.

Program Service Level Agreement."[36] There is a separate contract required, from that required to obtain the Plaintiff and Class member's motor vehicle records from the Texas Department of Motor Vehicles, with similar obligations.[37] This agreement, in the same accord as QQ Solutions Inc's agreement to obtain the motor vehicle records from the Texas Department of Motor Vehicles, is not assignable either in whole or in part, without the written consent of the department. "Financial Institution" is the reference identifier used within the lienholder's contract, the "Certified Lienholder Intake,"[38] requires financial institution information, the fact a lien is present is financial information. Defendant Vertafore's obtained the lienholder data from accessing a SFTP portal, see Texas Department of Motor Vehicles Electronic Lien and Title (ELT) Technical Specifications.[39]

B. Defendant Vertafore Knowingly "Re-Disclosed" Plaintiff and Class member's motor vehicle records, in violation of the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.

28. Defendant Vertafore's re-disclosed Plaintiff and Class member's motor vehicle records to its customers, the more than 20,000 Insurance agencies, some 1,000 carriers, and managing general agents[40], occurring over a period of almost five (5) years, and continuing to date. This redisclosure was in violation of the Driver's Privacy Protection Act, 18 U.S.C.

[36] "State of Texas Department of Motor Vehicles Electronic Lien and Title Program Service Level Agreement," online: https://www.txdmv.gov/sites/default/files/body-files/elt_sla.pdf, (last accessed January 29, 2021).

[37] "The Financial Institution agrees that this agreement is subject to the Motor Vehicle Records Disclosure Act, Transportation Code, Chapter 730, and the Driver's Privacy Protection Act, 18 U.S.C. Sec. 2721 et seq., hereinafter referred to as the "Acts", that all personal and vehicle information which would be considered privileged under the Acts, and is contained in any information forwarded to the Financial Institution under this Agreement, shall not be released by the Financial Institution to any individual or entity who would not otherwise have access to such information under the Acts".

[38] "Certified Lienholder Intake," online: https://www.txdmv.gov/sites/default/files/form_files/Intake_Form_0.pdf, (last accessed January 29, 2021).

[39] "Texas Department of Motor Vehicles Electronic Lien and Title (ELT) Technical Specifications," online: https://www.txdmv.gov/sites/default/files/body-files/elt_specifications.pdf, (last accessed January 29, 2021).

[40] "Company Profile, Vertafore, Inc" (last accessed December 5, 2020), online: https://www.dnb.com/business-directory/companyprofiles.vertafore_inc.d1eb70eb5bfc5f7f00d2b395130f573f.html

§2721 et seq. because Defendant Vertafore did not possess a legal right to obtain the Plaintiff and Class member's motor vehicle records. Additionally, permitting or otherwise authorizing the electronic transfer of 27.7 million motor vehicle records to an unsecured external storage server,[41] acts done knowingly, a "re-disclosure" of personal information that neither the text [of the DPPA], nor its legislative history permitted within the scope of any cited exemptions, and also a violation of the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq. Lastly, but most importantly, the unauthorized access to the Plaintiff and Class member's motor vehicle records, a redisclosure in and of itself, an occurrence acknowledged by Defendant's Vertafore's press release, "three data files were inadvertently stored in an unsecured external storage service that appears to have been accessed without authorization."

29. The term "disclose" is first used in subsection (a), in the statutory prohibition on initial disclosures, 18 U.S.C. §Section 2721(a), "shall not knowingly disclose or *otherwise make available* to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record." In that section, the statute forbids a state DMV from "knowingly disclos[ing] or otherwise mak[ing] available to any person or entity" protected personal information.[42] By attaching the terms "or otherwise make available" to the term "disclose" Congress intended to regulate the entire process of access to, and dissemination of, motor vehicle records. The statute's later use of the term "disclose," and

[41] Storage of commercial data using on premise storage means a company's server is hosted within their organization's infrastructure and, in many cases, physically onsite. The server is controlled, administered, maintained, procured, etc. by the company and its in-house IT team, or an IT partner. Data and other information are shared between computers through their local network, while cloud storage, an external server, uses an outside service provider to host data. The cloud provider procures, installs and maintains all hardware, software, and other supporting infrastructure in its data centers, permitting access to these services to manage the company's account via the internet from a PC, a web browser or a mobile app.

[42] Transportation Code, Title 7, Vehicles and Traffic, Subtitle J., Miscellaneous provisions, Motor Vehicle Records Disclosure Act., Section 730.003, defines "Disclose" to mean "to make available or make known personal information contained in a motor vehicle record about a person to another person, by any means of communication."

of "redisclose," is a short-handed reference back to subsection (a). Congress' employed broad language to define and regulate disclosures intended to include within the statute's reach the kind of re-disclosure of PII that occurred here, namely, the transfer of motor vehicle records from Defendant Vertafore to its customers, motor vehicle records not authorized to be obtained, and Defendant Vertafore permitting, or otherwise authorizing the electronic transfer of motor vehicle records, a redisclosure, to an unprotected external storage server.

30. The terms "disclose" or "re-disclose" are also not limited as to take the act of publication of protected information outside the statute's reach because no specific recipient was involved in the occurrence. Defendant Vertafore's action, re-disclosing the motor vehicle records to its customers, was an act of re-disclosure. Defendant Vertafore's action, permitting or otherwise authorizing the electronic transfer of motor vehicle records to an external storage server was an act of re-disclosure, tantamount to placing it in plain view on a public communication system, sufficient to come within the activity regulated by the statute, regardless of whether another person viewed the information or whether Defendant Vertafore intended it to be viewed only by its employees. The real effect of the placement of the motor vehicle records, without security protections, within the online ecosystem was to make available Plaintiff and Class Member's motor vehicle records to anyone online. This voluntary action, not knowledge of illegality or potential consequences, was sufficient to satisfy the mens rea element of the DPPA.[43]

31. The information re-disclosed by Defendant Vertafore's transfer of motor vehicle records to its customers was not permissible since defendant Vertafore had obtained the motor vehicle records in violation of the DPPA. The transfer of this data to an external storage

[43] See Pichler v. UNITE, 542 F.3d 380, 396–97 (3d Cir.2008) (discussing the term "knowingly" as it is used in the civil liability provisions of the DPPA and finding that knowledge of illegality or potential consequences is not an element).

server was not "[f]or use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in carrying out its functions with claims investigation activities, antifraud activities, rating or underwriting, 18 U.S.C. § 2721(b)(6). The words "[f]or use" perform a critical function in the statute and contain the necessary limiting principle that preserves the force of the general prohibition while permitting the re-disclosure compatible with that prohibition. Specifically, when the statutory language says that a disclosure is authorized that language means that the actual information re-disclosed—i.e., the re-disclosure as it existed in fact—must be information that is used for the identified purpose. When a particular piece of disclosed information is not used to effectuate that purpose, the exception provides no protection for the disclosing party. As such, Defendant Vertafore's re-disclosure, without safety protections, was not compatible with the purpose of the exception.

32. The DPPA requires entities re-disclosing the motor vehicle records to have adequate safeguards to protect access to the PII while being transferred and stored- storage, an incidental purpose to obtaining bulk data. Defendant Vertafore was on notice that it was obligated to protect motor vehicle records in its possession, transferring data, or storing the data, an obligation by any means of communication.[44]

33. The legal obligations imposed upon Defendant Vertafore to ensure that motor vehicle data that was re-disclosed would be protected from unauthorized access was required to assure compliance with the legislative intent of the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq., otherwise, the statute's purpose of safeguarding information for security

[44] Tex. Bus. & Com. Code § 521.052. BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

and safety reasons, contained in the general prohibition against re-disclosure, would be ignored. Defendant Vertafore could redisclose data on external storage servers without any considerations for privacy and security, leave it open to public access, without any obligation to protect the PII contained within the motor vehicle records, defeating the chief aim of the statute's privacy and security protection.

C. **Defendant Vertafore's "Data Event" - A Failure to Implement Safety Controls**

34. Defendant Vertafore's Data Event was the inevitable result of a top-down policy to prioritize growth and profits over data security, made possible because Defendant Vertafore adopted weak cybersecurity measures that failed to protect consumer data – a symptom of what appeared to be the low priority afforded cybersecurity by company leaders. The technical deficiencies and weaknesses that permitted unfettered access to Defendant Vertafore's systems demonstrate how little priority was given to even rudimentary data security protocols, despite Defendant Vertafore's role as one of the largest custodians of consumer data in the United States.

35. Reportedly, the Data Event occurred because sensitive data was being "*inadvertently stored in an unsecured external storage service*."[45] Defendant's Vertafore's own admission not only further exemplifies Defendant Vertafore's failure to secure consumer's data, but also evidences a failure to hire competent personnel, knowledgeable about data transfer, storage, and security. If that computing environment itself had been secured, rather than relying on the security mechanisms of the storage device or the perimeter around it (or lack thereof), then access to the data essentially would be useless to anybody trying to leverage the information. This style of data security protection, known as data-

[45] "Vertafore Statement Regarding data Event", (First accessed November 12, 2020), online: https://www.vertafore.com/resources/press-releases/vertafore-statement-regarding-data-event

centric security, includes methods such as tokenization, which replaces sensitive information with meaningless representational tokens. The best part is that data-centric security travels with the data, so even if it winds up in an unsecured location, as happened in the Defendant Vertafore Data Event, consumer's most sensitive PII would still have been protected.

36. Defendant Vertafore admitted within emails sent to representatives of the Texas Motor Vehicle Department that it was obtaining motor vehicle records in bulk, using the QQ Solutions Inc's SFTP, the data provided by the Texas Department of Motor Vehicles sent to a designated server, presumably an external storage server, used generally when storing large amounts of data such as in millions of motor vehicle records. The best security practices for enterprise-class external storage centers include data encryption and authentication. Authentication protects data by ensuring external storage resources are only available to authorized users and trusted networks. Encryption secures data at rest on the external storage server itself and end-to-end as data is transmitted between external storage and the computer system or mobile device accessing that information. Failure to provide these best security practices, not authenticating the network, encrypting the data, nor controlling unauthorized access to the computing systems, in and of itself negligent acts, exposes the data to individuals with nefarious purposes.

37. Defendant Vertafore publicly marketed its management system to the insurance industry as means to provide data security, warning that audit trails could track events, including login activity, and that it was imperative that data be secured. Defendant Vertafore, reportedly aware of the risks and techniques used by cyber-criminals, failed to implement policy protocols to monitor unauthorized activity inside its own network. Emphasizing within its marketing materials *"Your data is one of your most important assets – so it's imperative*

you secure it" [46]. Defendant Vertafore sought to assure customers that its data was protected from unauthorized access; however, Defendant Vertafore failed to satisfy the enormous responsibility required to protect the data it collected, nor fulfill its public assurances to protect Texans' confidential information. Instead, with continuing and absolute disregard for the privacy and security of 27.7 million Texas consumers, PII was exposed to third parties through lax and non-existent data security policies and protocols.

38. In addition to lacking the necessary safeguards to secure its most valuable "core" data, motor vehicle records, Defendant Vertafore did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration *after* it occurred, defending however within its press release its safety protocols by claiming no system vulnerabilities were identified, but in actuality, its system's infrastructure was compromised. Indeed, Defendant Vertafore Inc., like any company its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to tens of millions of consumer files. Unfortunately, Defendant Vertafore did not have these necessary data security protections in place prior to March 2020,[47] reportedly the initial period the Data Event originated, thereby permitting unauthorized parties the ability to covertly access and infiltrate the sensitive personal information of approximately 27.7 million Texas consumers.

39. By its own admission, stated within Defendant Vertafore's press release, Defendant Vertafore's computing systems were accessible on March 11, 2020, but it was not

[46] "Sagitta, powered by Vertafore", (last accessed November 20, 2020), online: https://www.vertafore.com/sites/default/files/files/2017-11/Sagitta-DataSheet 3.pdf

[47] Companies such as Defendant Vertafore that hold large amounts of sensitive data should have multiple layers of cybersecurity, including (1) frequently updated tools to prevent criminals from breaching their systems; (2) controls that limit criminals' ability to move throughout their systems in the event of an initial breach; (3) restrictions on criminals' ability to access sensitive data in the event of an initial breach; and (4) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible.

until August 2020, well over five (5) months later, that Defendant Vertafore was made aware of the Data Event, evidencing further its lack of security protections. Compounding this failure, Defendant Vertafore Inc's failed to even discover its own Data Event, the discovery reportedly discovered by a "trusted third-party'.

40. Defendant Vertafore is negligent by the redisclosure of Plaintiff and Class members' motor vehicle records to an unsecured external storage server, whether the server was a Cloud Provider, on the Defendant Vertafore's premise, or even on *QQ Solution Inc.'s premise*.[48] The Texas Department of Motor Vehicles sent motor vehicle records to Defendant Vertafore via FTP,[49] the process encrypted to control "packet-sniffing"[50] Acker's email of March 6, 2020 noted, "We have not been receiving the data from the SFTP site…" an indication that the files were "received" by an FTP server behind a corporate firewall then transferred to a STFP server for corporate use. The transfer of data via STFP requires an information security program with multiple existing safeguards, encryption protocols, and related policies that were designed to manage and restrict access. Defendant Vertafore's press release noted though that "someone" had transferred files to on "an unsecured external storage server," indicating that the transfer did not involve a SFTP transfer; moreover, access to the file to begin the transfer required access to the corporate database.

[48] On-premises storage means a company's server is hosted within their organization's infrastructure and, in many cases, physically onsite. The server is controlled, administered, maintained, procured, etc. by the company and its in-house IT team, or an IT partner. Data and other information are shared between computers through their local network, while cloud storage uses an outside service provider to host data. The cloud provider procures, installs and maintains all hardware, software, and other supporting infrastructure in its data centers, permitting access to these services to manage the company's account via the internet from a PC, a web browser or a mobile app.

[49] File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files from a server to a client on a computer network. The Texas Department of Motor Vehicle sends motor vehicle record data to Bulk Requestors via FTP, pursuant to the "SERVICE CONTRACT FOR THE PURCHASE OF TEXAS MOTOR VEHICLE TITLE AND REGISTRATION (VTR) DATABASE," and confirmed by a Texas Department of Motor Vehicles' Associate General Counsel in response to an open records request, "our weekly updates are provided via FTP." the response dated May 8, 2018.

[50] "Packet Sniffer," also referred to as a network analyzer, can intercept FTP packets in transit and extract data. See: Valentine, et al. v. NebuAd, Inc., No. 3:08-cv-05113, privacy litigation explaining packet sniffing.

41. Defendant Vertafore had a continuing obligation to comply with all federal and state laws, regulations, and security standards as enacted or revised over time, regarding Data Security, electronic data interchange, and restricted Permissible Uses of Plaintiff and Class member's motor vehicle records. Defendant Vertafore failed in this endeavor. This lack of basic safeguards on Defendant Vertafore's system and the company's failure to implement even minimal, industry-standard practices further highlights the glaring lack of care exercised by Defendant Vertafore in protecting its massive trove of consumer data. Clearly cybersecurity was not a priority at Defendant Vertafore ―even after warnings within the insurance industry it should have put Defendant Vertafore on notice that the data it was entrusted to safeguard was extremely vulnerable, likely the target of identity thieves. Given the amount of personal and sensitive data it compiles and stores, Defendant Vertafore was well aware it was a target, but nonetheless refused to implement best practices relating to data security—as demonstrated by its lack of security protections.

D. Defendant Vertafore's Delayed Public Notice-A Botched Response

42. Defendant Vertafore failed to notify Texas residents about the unauthorized access to Plaintiff and Class member's motor vehicle records in a timely manner. The public release on November 10, 2020, portrayed in the media as a "Data Breach," not as a data event, failed to discuss the totality of the unauthorized access to Texas residents' motor vehicle records, instead diverting attention to give notice only on the occurrence which began on March 11, 2020. In actuality, a "Data Breach" did occur, and it started in 2015, Plaintiff and Class members' privacy protected information being accessed by unauthorized parties for many years, namely, by Defendant Vertafore.

43. Defendant Vertafore had a duty to advise the Texas Department of Motor Vehicles in August 2015 about its proposed purchase of QQ Solutions which involved the

acquisition of a confidential database; moreover, enter a contract with the Texas Department of Motor Vehicles to obtain access to the motor vehicle record database. Defendant Vertafore failed to provide notice to Plaintiff and Class members concerning its unauthorized use of Plaintiff and Class member's motor vehicle records since 2015. Such acts are a violation of the Motor Vehicle Records Disclosure Act. Section 730.013, the state Driver Privacy Protection Act, [51] and the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq. Defendant Vertafore's failure to do so, while continuing to obtain, use, and redisclose the Texas motor vehicle record database was not an errant clerical error, nor the result of mismanagement by mid-level administrative personnel in the IT department, it was a top-down policy.

44. In February 2019, Defendant Vertafore reportedly first became aware of possible irregularities with accessing the database of motor vehicle records provided by the Texas Department of Motor Vehicles, albeit, an unauthorized access, failing at that time to provide notice to the Texas Department of Motor Vehicles about the irregularities. Since the Texas Department of Motor Vehicles had not ceased transferal of the database to QQ Solutions Inc., Acker's March 2020 emails indicate a possible third-party compromise beginning as early as February 2019. Defendant Vertafore failed to provide adequate notice to the Texas Department of Motor Vehicles, and the public, in March 2020.

45. From November 2019 until March 2020, representatives of Defendant Vertafore had an extensive exchange of emails with representatives of the Texas Department of Motor Vehicles related to its inability to access the motor vehicle record database, the access restricted, not due to a third-party compromise, but restricted by the Texas Department of

[51] Transportation Code, Title 7, Vehicles and Traffic, Subtitle J., Miscellaneous provisions, Motor Vehicle Records Disclosure Act. Section 730.013, Section D, "Resale and Re-disclosure" obligates the purchaser to "immediately inform the State if the privacy protected personal information provided to the Purchaser is disclosed in violation of the DPPAs.

Motor Vehicles. Defendant Vertafore's representatives being advised repeatedly that their company did not have a contract to obtain, use, or redisclose motor vehicle records from the Texas Department of Motor Vehicle. The actual dilemma, Defendant Vertafore had been doing so for almost 5 years.

46. On August 13, 2020, Roper Technologies, Inc. acquired Defendant Vertafore, and in mid-August 2020, Defendant Vertafore is first warned about suspicious network traffic from a "trusted third-party," yet Defendant Vertafore will delay public notice until November 10, 2020 via a press release published on the company's website. Defendant Vertafore's public notice, best described as cryptic and enigmatic, is vague: *"Although that firm did not find any evidence, to be considerate of all Texas driver license recipients and out of an abundance of caution, Defendant Vertafore is offering them one year of free insurance monitoring and identity restoration services in recognition that these services offer valuable protection in other contexts beyond this event," and* misleading claiming only three (3) data files had been compromised, omitting the previous five (5) years of compromise.

47. The notice, delayed in part, because Defendant Vertafore spent time re-building the trust of its customers for retention purposes – failing to be concerned with how consumers would be affected: "*No customer data nor any other data—including partner, vendor, or other supplier data—or systems hosted for them were impacted".* And while Defendant Vertafore stated publicly that data was "accessed," qualifying its comment as: "appears to have been accessed," the company refused to confirm that the data was exfiltrated – stolen – from their systems and downloaded by the criminals. By doing so, Defendant Vertafore was more focused on using the Data Event as a profitmaking opportunity for the company to defend its services, attempting to reassure its insurance customers about its data security, while withholding notice to affected consumers that would have permitted redress. Defendant

Vertafore intentionally failed to convey the seriousness of the Data Event, distorting the actual events, an effort to minimize the extent of the Data Event, seeking to control a PR nightmare. Defendant Vertafore's method of post-breach announcement was also inadequate, failing to provide notice to all potential parties affected by the Data Event. In possession of contact information of all affected Texas residents, data contained within its database, Defendant Vertafore could have provided direct notice by mail, choosing instead to merely post notice of the Data Event on its website page that few, if any, affected Texas residents had knowledge of, nor would have notice to access the site.

48. Defendant Vertafore reportedly informed the Texas Attorney General, Texas Department of Public Safety, Texas Department of Motor Vehicles and U.S. Federal law enforcement, FBI, and the U.S. Attorney's office, about the Data Event; however, initial notice to the Texas Department of Motor Vehicles didn't occur until sixty (60) days after first being advised of the data Event[52], although obligated by Transportation Code, Title 7, Vehicles and Traffic, Subtitle J., Miscellaneous provisions, Motor Vehicle Records Disclosure Act. Section 730.013, Section D, "Resale and Re-disclosure," Transportation Code, Chapter 730, the state Driver Privacy Protection Act, Tex. Bus. & Com. Code § 521.053(b), (d)), Texas Identity Theft Enforcement and Protection Act[53]., and the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.

[52] Defendant Vertafore's Counsel noted, within a November 10, 2020 letter to Tracey Beaver, General Counsel, Texas Department of Motor Vehicles, that the *first* call to the Texas Department of Motor Vehicles ("DMV") concerning the Data Event occurred October 16, 2020, a delay of 60 days, formal notice provided by the November 10, 2020 letter, a delay of ninety (90) days. Additionally, this letter notes that on October 16, 2020 the FBI and the U.S. Attorney's office requested that Vertafore delay providing notice until November 9, 2020. because that notice would compromise an ongoing investigation. The date law enforcement was first contacted by Defendant Vertafore regarding the Data Event, not provided in this letter.

[53]Texas Identity Theft Enforcement and Protection Act., effective January 1, 2021, breach notices must now be made to affected individuals and the Texas Attorney General within 60 days following the determination that a breach of system security had occurred.

49. While Defendant Vertafore was reportedly requested by law enforcement to temporarily delay notice in order to conduct a criminal investigation, discovery shall be required to determine the actual date Defendant Vertafore first notified law enforcement concerning the Data Event, a 90 days delay appears excessive, a period inclined to skepticism, since it is an inordinate amount of time required for law enforcement to implement a preliminary investigation, knowing 27.7 million people are at risk. Defendant Vertafore was negligent in providing adequate notice to consumers in a timely fashion. By waiting an inordinate period, consumers were deprived of an opportunity to take immediate precautionary measures to protect themselves from identity theft and fraud.

E. **Defendant Vertafore's Business Practices Harmed Plaintiff and Class members**

50. As a result of the Defendant Vertafore's business practices, Plaintiff and the Class have been harmed in several ways: (i) Defendant Vertafore knowingly *obtained, used, and redisclosed* Plaintiff and Class members' personal information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles without authorization, ("Data Event I"); (ii) Defendant Vertafore knowingly *redisclosed* Plaintiff and Class members' personal information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles without authorization,("Data Event II"); (iii) Plaintiff and Class members now know or should know that their PII was improperly accessed, and are concerned that it will be put up for sale on the dark web for purchase by malicious actors[54];

[54] A cyber black market exists in which criminals openly post and sell stolen information, and other Personal Information on Internet websites. Reportedly, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. The unauthorized disclosure of Vehicle Registration Numbers can be particularly damaging because Vehicle Registration Numbers cannot be replaced.

(iv) Plaintiff and Class members face an imminent and ongoing risk involving security[55], identity theft, and similar cybercrimes; (v) Plaintiff and Class members have expended and will continue to expend time and money to protect against cybercrimes; (vi) Plaintiff and Class members have lost property value in their personal identifying information; and (vii) Plaintiff and Class members did not receive the benefit of data privacy when they provided personal information to the Texas Department of Motor Vehicles due to Defendant Vertafore's actions.[56] Plaintiff and Class members will suffer such harm for many years to come.[57]

51. Defendant Vertafore's activities occurred throughout the State of Texas, knowingly *obtaining* the motor vehicle records of Plaintiff and the Class members from the Texas Motor Vehicle Department, accessing the QQ Solutions Inc/s SFTP portal- a course of action that was unauthorized, and a body of information that is protected from access and disclosure by federal law. These activities, "Data Event I", are undisputed by Defendant Vertafore's own admission. The heightened privacy and safety concerns generated by the obtain[ment], disclos[ure], or [use] of such records, without authorization, is apparent in U.S. law, creating restrictive consent standards. Plaintiff and the Class members have a relevant

[55]The DPPA prohibits disclosure of personal data to prevent injury before the fact. It would be odd for the court to require that a person whose information was unlawfully disclosed await such a grim result as what occurred to Actress Schaeffer before suing, to do otherwise would require the person wait until killed before their estate brought a case.

[56] Plaintiff and Class members had a legitimate expectation that the information would remain confidential while in the state's possession." See: https://www.leagle.com/decision/infdco20140512e10.

[57] Plaintiff and Class members will face a risk of injury due to the Data Event for years to come. Malicious actors often wait months or years to use the personal information obtained in Data Event, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cybercrimes stemming from a single Data Event. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims often do not know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Event is not used to harm them.

interest as individuals to control information contained within motor vehicle records concerning their person, the relevant harm if not protected, an invasion of their privacy. This intangible harm has a close relationship to a harm that traditionally provided a basis for suit in the Anglo-American legal system. In enacting the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq., Congress recognized the potential harm to privacy from the unauthorized access to drivers' personal information. This intangible harm associated with the violation of the DPPA's substantive protections is consonant with the common law tradition of lawsuits for invasion of privacy. Without remedy, Plaintiff' and Class members will continue to be violated by Defendant Vertafore.

52. Defendant Vertafore engaged in widespread commercial *usage*, knowingly using Plaintiff' and the Class Members' motor vehicle records, for its own benefit, without Plaintiff' and Class Members' knowledge, authorization, or consent, nor that of the Texas Department of Motor Vehicles. Defendant Vertafore used its software to create databases of Personal Information, derived in whole or part, from data contained in the motor vehicle records, data afforded special attention due to the consequences that may flow from its re-disclosure. Further, through its practices, Defendant was able to raise its profile with many companies, enabling Defendant to attract business, increase its prospective revenue, secure investment funding, and thereby profit from its conduct described herein.

53. Defendant Vertafore then knowingly *re-disclosed* Plaintiff and Class member's motor vehicle records within its software, knowingly redisclosing that data to more than 20,000 Insurance agencies, some 1,000 carriers, and managing general agents. Defendant Vertafore redisclosed Plaintiff and Class member's Personal Identifying Information within the agency management and content management integration system that links agency management system domain entities (such as clients, policies, claims, vendors) to content

management system. Such conduct constitutes a highly offensive and dangerous invasion of Plaintiff' and the Class Members' privacy.

54. Defendant Vertafore knowingly *re-disclosed* Plaintiff and Class members' motor vehicle records to an unsecured external storage server, "Date Event II," Acker's email of March 6, 2020 noted, "We have not been receiving the data from the SFTP site…" an indication that the files were "received" by an FTP server behind a corporate firewall then transferred to a STFP server for corporate use. The transfer of data via STFP requires an information security program with multiple existing safeguards, encryption protocols, designed to manage and restrict access. Defendant Vertafore's press release noted "human error", indicating that a representative of Defendant Vertafore was involved, accessing the database to transfer the data to the unsecured external storage server, this action was a redisclosure.

55. Defendant Vertafore knowingly *re-disclosed* Plaintiff and Class members' motor vehicle records to unauthorized persons by redisclosing data on external storage servers without any considerations for security, leaving it open to public access. Defendant Vertafore's action, permitting or otherwise authorizing the electronic transfer of motor vehicle records to an external storage server without adequate security protocols consistent with law and industry standards to protect consumers' Personal Information was an act of re-disclosure, tantamount to placing it in plain view on a public communication system, sufficient to come within the activity regulated by the statute, regardless of whether another person viewed the information.

56. Defendant Vertafore offered one (1) year of free credit monitoring and identity restoration services to Texas driver license recipients within its press release, providing a link

to a website,[58] an inadequate remedy. Contrary to the promises, the service fails to indicate whether information has been impacted—instead, it advises consumers that they "may" or "may not" have been compromised. This service, offered for only one (1) year, requires consumers to purchase the services after the expiration of the offer, a significant cost.[59]

57. Plaintiff and Class members face an imminent and ongoing risk of security, identity theft, including Synthetic ID theft[60], and similar cybercrimes, the victim of *targeting* for personal identifying information contained within motor vehicle records, used for nefarious purposes. The risk of identity theft to Plaintiff and Class members is imminent and ongoing because their Vehicle Identification Numbers (VIN) were obtained. The VIN is like a vehicle's Social Security number: it makes that vehicle unique against others of the same make and model. Thieves can use a single VIN to register dozens of vehicles. Unfortunately, consumers will not know this has happened unless they need to use the number; for example, if they move to another state or change insurance. Plaintiff Class member's driver's license numbers, aggregated with vehicle registration numbers, is data on file with places of employment, banks, stores, doctor's office, government agencies, and other entities. Having access to that one number, let alone both, can provide an identity thief with several pieces of information to commit fraud.

[58] "Vertafore Data Event," online: https://vertafore.kroll.com/ (First accessed November 10, 2020).

[59] "Most companies charge a $500 to a $1000 to get started and a monthly fee of $59-$120 starting the following month," remarks of Brad Young, a credit monitoring & credit repair expert from Texas discussing the significant costs of credit monitoring, online: https://landmarkcredit.com/faq/#1443755370403-827684dc-626c. (last accessed January 29, 2021).

[60] Synthetic identity theft is reportedly the "fastest growing type of ID fraud," representing 80-to-85% of all current identity fraud, according to the U.S. Federal Trade Commission. Synthetic ID fraud artists merge real and fake personal consumer data to create a fresh identity, which they can use to commit financial fraud. For instance, synthetic fraudsters can steal a driver's license or vehicle registration number and create a new identity by merging those numbers with a different—but real—name, address and phone number. Once that task is accomplished, synthetic identity thieves can apply for and get credit cards, mobile devices, and other credit accounts.

58. *"We are also not aware of any way this information could be used to commit fraud,"* a statement issued by a representative of Defendant Vertafore to Dave Lieber, ("Lieber")[61] an investigative reporter, in *October 2020*,[62] after he confronted the company about known identity theft involving Texas Driver licenses, linked to Defendant Vertafore, reported to him by members of his "Watchdog" group as early as *September 2020*:

> *"When I informed them later that they were right, Perry said, "Well, well. My reaction is I'm not the least bit surprised. No wonder I had no idea about it until I was alerted to it being on the dark web. I knew eventually you'd find out something because when I called the police to report it, and they told me five or six other people had called the same day about the same thing, I knew that's not just a coincidence."*

59. Defendant Vertafore has admitted that unauthorized third parties have accessed Plaintiff and Class member's PII. The targeting of Plaintiff and Class member's personal information contained within motor vehicle records, obtained from the Texas Department of Motor Vehicle Department for the purpose of misuse in cyberattacks, along with the fact that the identity theft has occurred makes the threatened injuries, "sufficiently imminent," a substantial and imminent risk involving the reasonable likelihood that their PII would be the subject of use.

[61] Dave Lieber is an award-winning investigative journalist for the Dallas Morning News, founder of the "Watchdog Nation," https://watchdognation.com/, a consumer protection group that investigates scams and fraud by corporations, author of 8 books, and a playwright: https://amonplay.com/.

[62] "The Watchdog: Your Texas driver's license, vehicle information and lien holder were stolen in a huge data theft," online: https://dentonrc.com/news/the_watchdog/the-watchdog-your-texas-driver-s-license-vehicle-information-and-lien-holder-were-stolen-in/article_550fff85-0b5b-5989-8ad2-23c2f2c73fba.html, (last accessed January 20, 2021).

VIII.
CLASS ALLEGATIONS

60. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), applicable, Plaintiff brings this action on behalf of himself and a proposed class of similarly situated individuals. Plaintiff seeks certification of the following nationwide class (the "Nationwide Class," or the "Nationwide Subclass" (the "Classes"):

NATIONWIDE CLASS

All natural persons nationwide who, on or after, four (4) years prior to the date of this filed complaint, through the final disposition of this or any related actions (the Nationwide "Class Period"), had Defendant Vertafore obtain their motor vehicle records from the Texas Department of Motor Vehicles, to use and re-disclose, without authorization, and seek liquidated damages in the amount of $2500 each, pursuant to 18 U.S.C. §2724(b)(1) et seq.

NATIONWIDE SUBCLASS

All natural persons nationwide who, prior to the date of this filed complaint, through the final disposition of this or any related actions (the Nationwide Subclass "Class Period"), whose Personal Information was compromised as a result of the Data Event announced by Defendant Vertafore on or about November 10, 2020, as identified by Defendant Vertafore's records relating to that Data Event.

61. Plaintiff reserves the right to revise these definitions of the classes based on facts they learn as litigation progresses.

62. Excluded from the class are the Defendant, its employees, officers, directors, agent, legal representatives, heirs, assigns, successors, individual or corporate entities acting within a partnership, joint venture, trust, association, union, subsidiaries, whether wholly or partially owned, divisions, whether incorporated or not, affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which Defendant exercises supervision or control, or group of individuals associated in fact, although not a

legal entity, or other legal entity, in addition to Plaintiff's legal counsel, employees, and his immediate family, the judicial officers and his immediate family, and associated court staff assigned to this case, and all persons within the third degree of consanguinity, to any such persons.

63. Certification of a class under Fed. R. Civ. P. 23 is appropriate because Plaintiff and the putative Class members have satisfied Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), questions of law and fact that are common to the Class that predominate over any questions affecting only individual members of the Class, and a class action is superior to all other available methods for fair and efficient adjudication of this controversy in fact, the wrongs suffered and remedies sought by Plaintiff and the other members of the Class are premised upon the same evidence.

64. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiff is informed and believes—based upon Defendant Vertafore's press releases— that there are approximately 27,7 million class members. Those individuals' names and addresses identified in the Class definition are identifiable from the information and records in the custody of the Defendant and the State Motor Vehicle Department which provided motor vehicle records to Defendant, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

65. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)**. As to the Class, this action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including:

1. whether Defendant Vertafore obtained, used, and re-disclosed Plaintiff and Class member's personal information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles,

2. whether Defendant Vertafore acted knowingly when it obtained, used, and re-disclosed Plaintiff and Class member's personal information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles; pursuant to a contract between QQ Solutions Inc. and the Texas department of Motor Vehicles,

3. whether Defendant Vertafore had a DPPA permissible use to obtain, use, and re-disclose, Plaintiff and Class member's personal information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles,

4. whether Defendant Vertafore's electronic transfer of 27.7 million motor vehicle records to an unsecured external storage server, without adequate security protections, was a knowing "re-disclosure" of personal information,

5. whether Defendant Vertafore's conduct described herein violates the Driver's Privacy Protection Act, 18 U.S.C. §2721,

6. Whether Defendant Vertafore possessed a legal duty to properly design, adopt, implement, control, manage and monitor its data security processes, control, policies, procedures, and/or protocols, complying with industry standards, to protect Plaintiff and Class member's Personal Information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles from a Data Event; and if so, whether Defendant Vertafore negligently failed in this obligation,

7. Whether Defendant Vertafore's breach of a legal duty caused its computing systems to be compromised, resulting in the loss and/or potential loss of Plaintiff and Class member's Personal Information contained within motor vehicle records obtained from the Texas Department of Motor Vehicles,

8. Whether Defendant Vertafore possessed a legal duty to timely and adequately investigate the Data Event, take reasonable remedial actions in response to the Data Event, and inform Plaintiff and Class members of the Data Event; and if so, whether Defendant Vertafore negligently failed in this obligation,

9. the nature, and extent of Plaintiff' and Class members damages,

10. the nature, and extent of all statutory penalties, including liquidated damages of $2500.00, and/or damages for which Defendant Vertafore is liable for, and legally obligated to, Plaintiff and Class members,

11. whether Plaintiff and Class members are entitled to appropriate injunctive relief against Defendant Vertafore; and

12. whether punitive damages are appropriate.

66. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Classes, Plaintiff' claims are typical of other Class members' claims because Plaintiff and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

67. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate class representative because his interests do not conflict with the interests of Class members who he seeks to represent, Plaintiff has retained counsel competent and experienced in complex class action litigation, including numerous Driver Privacy Protection Act Class Actions filed in Federal Courts, and Plaintiff intend to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and his counsel.

68. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** Defendant Vertafore's conduct, as complained of herein, is generally applicable to the Classes, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Classes as a whole. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for

Defendant Vertafore. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant Vertafore has acted and/or refused to act on grounds generally applicable to the Classes, making final injunctive relief or corresponding declaratory relief appropriate.

69. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** 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 Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant Vertafore, so it would be impracticable for Class members to individually seek redress for Defendant Vertafore's wrongful conduct. Even if Class members could afford 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.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violations of the Driver's Privacy Protection Act, § 18 U.S.C. § 2721. et. seq.

(On Behalf of the Plaintiff and members of the proposed Nationwide Class and Nationwide Subclass against Defendant.)

70. Plaintiff realleges, and incorporates by reference, all preceding allegations as if fully set forth herein.

71. As set forth herein, Defendant violated the Driver's Privacy Protection Act, 18 U.S.C. § 2721. et. seq. by engaging in the acts alleged in this complaint.

72. Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq., "Prohibition on release and use of certain personal information from State motor vehicle records", regulates persons or entities' obtainment and re-disclosure of personal information gathered by State Departments of Motor Vehicles. Driver's Privacy Protection Act creates a private cause of action for a "person" whose personal information was knowingly obtained, disclosed, or used, from a motor vehicle report, "for a purpose not permitted under this chapter," 18 U.S.C. § 2724(a).

73. Driver's Privacy Protection Act regulates representations made to State Department of Motor Vehicles by persons or entities requesting access to motor vehicle records, " FALSE REPRESENTATION.—It shall be unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record", a violation of 18 U.S.C. §2722 (b).

74. Driver's Privacy Protection Act 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). Defendant Vertafore obtained motor vehicle records from the Texas Department of Motor Vehicles, records admittingly involved in the Data Event. Plaintiff and Class members' motor vehicle records, involved in the Data Event, and constitute "motor vehicle record[s]" as defined by the Driver's Privacy Protection Act.

75. Driver's Privacy Protection Act defines "person" to mean "an individual, organization or entity," 18 U.S.C. §2725(2). Defendant Vertafore is an organization. Plaintiff and Class members are "person[s]" as defined by the Driver's Privacy Protection Act.

76. Driver's Privacy Protection Act 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 and Class members' motor vehicle records were obtained by Defendant Vertafore, involved in the Data Event, and constitute "personal information" as defined by the Driver's Privacy Protection Act.

77. Defendant violated the Driver's Privacy Protection Act, § 18 U.S.C. §2721 et seq., by making false representations to the Texas Motor Vehicle Department, as set forth below, knowingly obtaining, using, and re-disclosing 27,7 million motor vehicle records of the Plaintiff and Class members, motor vehicle records involved in the Data Event, a violation of 18 U.S.C. §2722 (b).

78. Driver's Privacy Protection Act, § 18 U.S.C. § 2721 et seq. authorized State Motor Vehicle Departments to disclose personal information contained in the department's motor vehicle records, in accordance with that Act, Motor Vehicle Records Disclosure Act, Chapter 730, implementing Driver's Privacy Protection Act, § 18 U.S.C. § 2721. The Texas Department of Motor Vehicles, pursuant to Transportation Code, Chapters 501, 502, and 504 established that the State was responsible for administering and retaining Texas motor vehicle title and registration database records (MVRs), Chapter 730, authorized the State to contract with 'authorized recipients" in accordance with the Driver's Privacy Protection Act, § 18 U.S.C. § 2721 et seq.

79. In accordance with provisions of the Transportation Code, Chapter 730, the state Driver Privacy Protection Act, QQ Solutions Inc. contracted with the Texas Department of Motor Vehicles to obtain motor vehicle records. Pursuant to the agreement, Section 11, "Termination," the contract automatically terminates if the Purchaser ceased to conduct

business, substantially changed the nature of its business, sold its business, or if there was a significant change in the ownership. Defendant Vertafore failed to notify the Texas Department of Motor Vehicles concerning the purchase of QQ Solutions Inc. in 2015, failed to permit the Texas Department of Motor Vehicles to determine if Defendant Vertafore was an "authorized recipient," of motor vehicle records, and failed to contract directly with the Texas Department of Motor Vehicles immediately after the QQ Solutions Inc. purchase.

80. Defendant Vertafore continued to knowingly obtain, use, and re-disclose the motor vehicle records from the Texas Department of Motor Vehicles, motor vehicle records involved in the Data Event, falsely representing to the Texas Department of Motor Vehicles it was an "authorized recipient," a violation of 18 U.S.C. §2722 (b).

81. Defendant Vertafore's electronic transfer of 27.7 million motor vehicle records to an unsecured external storage server, without adequate security protections, was a knowing "re-disclosure" of personal information, as set forth below, a violation of the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq.

82. Driver's Privacy Protection Act describes the term "disclose" in subsection (a), statutory prohibition on initial disclosures, "shall not knowingly disclose or *otherwise make available* to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record," 18 U.S.C. §Section 2721(a). The statute's later use of the term "disclose," and of "redisclose," is a reference back to subsection (a). Nondisclosure of personal information is the default rule. See 18 U.S.C. § 2721(a) (In general, the DPPA never explicitly listed any prohibited uses; rather, it prohibited disclosure of personal information except the fourteen permissible uses enumerated in section 2721(b)).

83. Defendant Vertafore certified one (1) permissible use when it contracted to obtain motor vehicle records from State Motor Vehicle Departments, specifically, "[f]or use

by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in carrying out its functions with claims investigation activities, antifraud activities, rating or underwriting, 18 U.S.C. § 2721(b)(6). Defendant Vertafore then knowingly re-disclosed the motor vehicle records to an unsecure external storage server without adequate security protections, a knowing re-disclosure for an impermissible use. Defendant Vertafore knew, or should have known, that failing to design and implement adequate security precautions—such as encryption end-to-end, internal firewalls, password protections, and intrusion detection protocols, while storing PII on Internet-connected external storage servers, could permit that data to be accessible by the public and cyber threat actors, individuals with nefarious interests and purposes, as occurred in this Data Event, a violation of the Driver's Privacy Protection Act, § 18 U.S.C. §2721 et seq.

84. Plaintiff and the Classes have suffered damages, as alleged herein, and pursuant to 18 U.S.C. § 2724(b)(1), are entitled to actual damages, but not less than liquidated damages in the amount of $2,500 each.

85. Plaintiff and the Classes, pursuant to 18 U.S.C. § 2724(b)(1), are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of money, actual and punitive damages, reasonable attorneys' fees, and Defendant's profits obtained from the above-described violations. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate him for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. § 2724(b)(1).

86. As a direct and proximate result of the aforesaid acts and activities of Defendant, Plaintiff, and each of them, have been caused to sustain harm.

87. All of the acts and activities of Defendant, as heretofore set out, were performed knowingly.

88. Plaintiff and Class members were damaged thereby, and seek redress thereof.

SECOND CAUSE OF ACTION

NEGLIGENCE
(On Behalf of the Plaintiff and members of the proposed Nationwide Subclass against Defendant.)

89. Plaintiff realleges, and incorporates by reference, all preceding allegations as if fully set forth herein.

90. Defendant Vertafore owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, disclosing their Personal Information in its possession from being accessed by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant Vertafore's security systems to ensure that Plaintiff' and Class members' Personal Information in Defendant Vertafore's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

91. Defendant Vertafore's duty to use reasonable care to protect Plaintiff and Class member's personal information arose from common law and state statutes and several additional sources, including but not limited to, those described below.

92. Defendant Vertafore had a common law duty of care to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable

that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information because individuals routinely attempt to steal such information and use it for nefarious purposes, Defendant Vertafore knew that it was more likely than not Plaintiff and other Class members would be harmed.

93. Defendant Vertafore's duty of care also arose under the Driver's Privacy Protection Act, § 18 U.S.C. § 2721 et seq., which prohibits "A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: **(1)** personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section;" as interpreted and enforced by the Office of the U.S. Attorney General, Department of Justice.

94. Defendant Vertafore's duty of care also arose from Section 730.002 of the Motor Vehicle Records Disclosure Act, ("MVDA") which prohibits "the disclosure and the use of personal information contained in a motor vehicle record, except as authorized by the individual or by law," as interpreted and enforced by the Texas Attorney General.

95. Defendant Vertafore undertakes its collection of highly personal information generally without the knowledge or consent of consumers and consumers that cannot "opt out" of the collection and disclosure by the State Department of Motor Vehicles of their Personal Information contained within motor vehicle records.

96. Defendant Vertafore also had a duty to safeguard the Personal Information of Plaintiff and Class members and to promptly notify them of a breach because of federal and state laws that require Defendant Vertafore to reasonably safeguard sensitive Personal Information, as detailed herein. Timely notification was required, appropriate and necessary

so that, among other things, Plaintiff and Class members could take steps to mitigate or ameliorate the damages caused by Defendant Vertafore's misconduct.

97. Defendant Vertafore breached the duties it owed to Plaintiff and Class members described above and thus was negligent. Defendant Vertafore breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) timely disclose that Plaintiff' and the Class members' Personal Information in Defendant Vertafore's possession had been or was reasonably believed to have been, stolen or compromised.

98. But for Defendant Vertafore's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

99. As a direct and proximate result of Defendant Vertafore's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiff' and Class members' injuries include: (1) theft of their Personal Information; (2) costs associated with the detection and prevention of identity theft and unauthorized use of their Personal Information; (3) costs associated with purchasing credit monitoring and identity theft protection services after one (1) year; (4) unauthorized use of their Personal Information, and adverse effects on their financial accounts and credit; (5) lowered credit scores resulting from credit monitoring inquiries; (6) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Vertafore Data Event ; (7) the

imminent and certainly impending injury, including privacy and security concerns flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals; (8) damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to Defendant Vertafore with the mutual understanding that Defendant Vertafore would safeguard Plaintiff' and Class members' data against theft and not allow access and misuse of their data by others; (9) continued risk of exposure to hackers and thieves of their Personal Information, which remains in Defendant Vertafore's possession and is subject to further breaches so long as Defendant Vertafore fails to undertake appropriate and adequate measures to protect Plaintiff and Class members; and (10) costs associated with time spent and the loss of productivity from taking time for Plaintiff and Class members to provide their Personal Information to the Texas Department of Motor Vehicles, a legal obligation, with the understanding and agreement that their Personal Information would remain confidential, but now obligated to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Vertafore Data Event.

100. Plaintiff and the Classes, pursuant to 18 U.S.C. § 2724(b)(1), are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of money, actual and punitive damages, reasonable attorneys' fees, and Defendant's profits obtained from the above-described violations. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff remedy at law is not adequate to compensate him for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. § 2724(b)(1).

101. As a direct and proximate result of the aforesaid acts and activities of Defendant, Plaintiff, and each of them, have been caused to sustain harm.

102. All of the acts and activities of Defendant, as heretofore set out, were performed knowingly.

THIRD CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf of the Plaintiff and members of the proposed Nationwide Class and Nationwide Subclass against Defendant.)

103. Plaintiff and Class members were damaged thereby, and seek redress thereof.

104. Plaintiff realleges, and incorporates by reference, all preceding allegations as if fully set forth herein.

105. Transportation Code, Chapters 501, 502, and 504 established that the State was responsible for administering and retaining the Texas motor vehicle title and registration database records (MVRs). Transportation Code, Title 7, Vehicles and Traffic, Subtitle J, Miscellaneous, provisions, Chapter 730, Motor Vehicle Records Disclosure Act, ("MVDA") authorized the Texas Department of Motor Vehicles, ("TXDMV") to disclose personal information contained in the department's motor vehicle records, in accordance with that the Driver's Privacy Protection Act, § 18 U.S.C. § 2721 et seq.

106. Section 730.002 of the Motor Vehicle Records Disclosure Act, ("MVDA") prohibits "the disclosure and the use of personal information contained in a motor vehicle record, except as authorized by the individual or by law." including, as interpreted and enforced by the State of Texas, acting by and through the Texas Department of Motor Vehicles. ("TXDMV"), the unfair act or practice by companies such as Defendant Vertafore of failing to use reasonable security measures to protect Personal Information contained within motor vehicle records.

107. Defendant Vertafore violated Section 730. 001 of the MVDA by failing to use reasonable security measures to protect Personal Information contained in motor vehicle records and not complying with industry standards. Defendant Vertafore's conduct was particularly unreasonable given the nature and amount of Personal Information contained within motor vehicle records it obtained and stored and the foreseeable consequences of a Data Event.

108. Defendant Vertafore's violation of Section 730. 001 of the MVDA constitutes negligence *per se*.

109. Plaintiff and Class members are "Person(s)" within the class of individuals Section 730. 001 of the MVDA was intended to protect.

110. Moreover, the harm that has occurred is the type of harm the MVDA was intended to guard against.

111. Indeed, the State of Texas has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiff and the Classes.

112. As a direct and proximate result of Defendant Vertafore's negligence, Plaintiff and Class members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION

DECLARATORY JUDGMENT
(On Behalf of the Plaintiff and members of the proposed nationwide Class and Nationwide Subclass against Defendant.)

113. Plaintiff realleges, and incorporates by reference, all preceding allegations as if fully set forth herein.

114. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

115. An actual controversy has arisen in the wake of the Defendant Vertafore Data Event regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant Vertafore is currently maintaining data security measures adequate to protect Plaintiff and Class members from further Data Events that compromise their Personal Information. Plaintiff alleges that Defendant Vertafore's data security measures remain inadequate. Defendant Vertafore denies these allegations. Furthermore, Plaintiff and Class members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

116. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (1) Defendant Vertafore continues to owe a legal duty to secure Plaintiff and Class Member's Personal Information and to timely notify consumers of a Data Event under the common law, (2) Section 730. 001 of the MVDA Act, and the Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq. require Defendant Vertafore to possess a contract to obtain motor vehicle records, Defendant Vertafore failed to obtain a contract. This court should require Defendant Vertafore to cease using these records and either destroy the records or return the records to the Texas Department of Motor Vehicles; **(3)** Vertafore continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

117. The Court also should issue corresponding prospective injunctive relief requiring Defendant Vertafore to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

118. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another Data Event involving Defendant Vertafore. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant Vertafore occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

119. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant Vertafore if an injunction is issued. Among other things, if another massive Data Event occurs at Defendant Vertafore, Plaintiff and Class members will likely be subjected to additional identify theft and other damages. On the other hand, the cost to Defendant Vertafore of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant Vertafore has a pre-existing legal obligation to employ such measures.

120. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another Data Event involving Defendant Vertafore, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully prays for judgment against Defendant as follows:

a) For an order certifying that this action may be maintained as a class action under Fed. R. Civ. P. 23(a) and (b)(1)(a), (b)(2), and (b)(3),

b) For an order designating Plaintiff and his counsel as representatives of the Classes,

c) For a declaration that Defendant's actions violated the Federal Driver's Privacy Protection Act, 18 U.S.C. §2721, and for all actual damages, statutory damages, penalties, and remedies available as a result of Defendant's violations of the DPPA, but not less than liquidated damages in the amount of $2,500 for each Plaintiff and each member of the Classes,

d) As applicable to the Class mutatis mutandis, awarding injunctive and equitable relief including, inter alia: (i) prohibiting Defendant from engaging in the acts alleged above; (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiff and the other Class members motor vehicle records, or to whomever the Court deems appropriate; (iii) requiring Defendant to delete all motor vehicle records collected through the acts alleged above; (iv) awarding Plaintiff and Class members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged herein; and (v) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant,

e) For a preliminary and permanent injunction restraining Defendant, its officers, agents, servants, employees, and attorneys, and those in active concert or participation with any of them from:

1. Obtaining, directly or indirectly, Plaintiff and Class members' Motor Vehicle Records, without express consent, from the State Motor Vehicle Department, for purposes that violate the Driver's Privacy Protection Act,

2. Re-disclosing Plaintiff and Class members' motor vehicle records for purposes that violate the DPPA,

3. Reselling Plaintiff and Class members' motor vehicle records for purposes that violate DPPA,

f) A permanent injunction enjoining and restraining Defendant, and all persons or entities acting in concert with them during the pendency of this action and thereafter perpetually, from,

1. Obtaining, directly or indirectly, Plaintiff and Class members' Motor Vehicle Records, derived in whole or part, from data maintained by the Texas Motor Vehicle Department, for purposes that violate the Driver's Privacy Protection Act,

2. Using, processing, and disseminating, Plaintiff and Class members' motor vehicle records for purposes that violate the DPPA,

3. Re-disclosing Plaintiff and Class members' motor vehicle records for purposes that violate DPPA,

g) For an award to Plaintiff and the Classes of costs and expenses of this litigation,

h) For an award to Plaintiff and the Classes for his reasonable attorneys' fees,

i) An award to Class members of damages, including but not limited to compensatory, statutory, exemplary, aggravated, and punitive damages, as permitted by law and in such amounts to be proven at trial,

j) For pre-and post-judgment interest as allowed by law, and

k) For such other relief as the Court may deem just and proper.

Dated: January 31, 2021

Respectfully submitted,

By: /s/ Joseph H. Malley
Law Office of Joseph H. Malley P.C.
1045 North Zang Blvd
Dallas, TX 75208
Telephone: 214.943.6100
malleylaw@gmail.com

Counsel for Plaintiff Aaron Mulvey, individually, and on behalf of a class of similarly situated individuals.