IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PATRICK ESTEVEZ, on behalf of himself and all others similarly situated, Plaintiff, v. SIXT RENT A CAR, LLC., Defendant.	CASE NO. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Patrick Estevez ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against SIXT Rent a Car, LLC ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyber-attack against Defendant that allowed a third party to access Defendant's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to thousands of current and former employees of Defendant (the "Cyber-Attack").

2. As a result of the Cyber-Attack, Plaintiff and the members of the Class suffered ascertainable injury and damages in the form of the substantial and present risk of fraud and identity theft from their unlawfully accessed and compromised private and confidential information (including Social Security numbers, driver's license numbers, passport numbers, and bank account numbers), lost value of their private and confidential information, out-of-pocket

expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff's and, on information and belief, thousands of other Class members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack and subsequent data breach (the "Data Breach").

4. Information compromised in the Cyber-Attack includes at least full names, and a combination of at least some of the following: dates of birth, Social Security numbers, driver's license number, state identification numbers, passport numbers, financial account numbers, health insurance numbers, and health information (collectively the "Private Information").

5. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class members' Private Information that it collected and maintained.

6. Defendant maintained the Private Information in a reckless manner; in particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyber-attacks of this type.

7. Upon information and belief, the mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiff's and Class members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant failed to timely notify Plaintiff and the members of the Class of the Cyber-Attack.

9. The Cyber-Attack occurred between April 27, 2022 and May 1, 2022; however, Defendant failed to ascertain that Plaintiff's and Class members' Private Information was compromised until June 2, 2022, over one month after the Cyber-Attack.

10. Furthermore, Defendant failed to notify Plaintiff of the Cyber-Attack and the Data Breach until July 6, 2022, over two months after Defendant discovered the Cyber-Attack.

11. Plaintiff's and Class members' identities and financial health are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained is now in the hands of data thieves.

12. Had Defendant properly monitored its property and custodied information and timely notified Plaintiff and the members of the Class of the Cyber-Attack, Defendant would have discovered the extent of the intrusion sooner and would have allowed Plaintiff and the members of the Class to sooner mitigate the effects thereof.

13. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, using Class members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, obtaining driver's licenses in Class members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a further result of the Cyber-Attack and subsequent Data Breach, Plaintiff and the members of the Class have been exposed to a substantial and present risk of fraud and identity theft.

15. Plaintiff and the members of the Class must now and in the future closely monitor their financial accounts to guard against identity theft.

16. As an additional result of the Cyber-Attack and subsequent Data Breach, Plaintiff and the members of the Class may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach, Plaintiff and the members of the Class have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to: (i) take appropriate measures to avoid unauthorized and fraudulent charges; (ii) change their usernames and passwords on their accounts; (iii) investigate, correct, and resolve unauthorized debits; (iv) deal with spam messages and e-mails received subsequent to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiff and the members of the Class have likewise suffered and will continue to suffer invasions of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to and misuse of their Private Information from Defendant, and Plaintiff and the members of the Class will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

18. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed or removed from the network during the Cyber-Attack.

19. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, attorneys' fees and costs, and injunctive

relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

20. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct asserting claims for negligence, negligence per se, breach of implied contract, and violation of the consumer protection statutes invoked herein.

PARTIES

21. Plaintiff Patrick Estevez is an individual citizen of the State of Texas residing in Austin, Texas. From March 2017 to July 2018, Plaintiff was employed by Defendant as a Receivables Specialist at Defendant's Florida headquarters. Over the course of his initial training, his employment with Defendant, and the payment of his compensation and health benefits, Plaintiff was required to provide and did provide his Private Information to Defendant.

22. On or about July 6, 2022, Plaintiff received notice from Defendant that the Data Breach had occurred following "unauthorized activity in the company network" where "an unauthorized party obtained files stored on our file server," which included his Personal Information.

23. Defendant is a Delaware corporation with its principal place of business 1501 NW 49th St. Ste. 100, Fort Lauderdale, FL 33309.

24. Defendant is the American subsidiary of Sixt Group, which in turn is owned by the publicly traded German holding company Sixt SE.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of members of the Class is in the

thousands, many of whom have different citizenship from Defendant, including the named Plaintiff here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

26. This Court has jurisdiction over the Defendant because it is headquartered in this district, and the computer systems implicated in this Data Breach are likely based in this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because: 1) a substantial part of the events giving rise to this action occurred in this District; 2) Defendant is based in this District and maintains Class members' Private Information in the District; and 3) Defendant had caused harm to members of the Class residing in this District.

FACTUAL ALLEGATIONS

I. Defendant's business.

28. Defendant provides car rental services in the United States, and is headquartered in Fort Lauderdale, Florida.

29. Defendant offers vehicle rentals in over 30 locations throughout the United States.

30. In the ordinary course of doing business with Defendant, current and former employees provide Defendant with sensitive, personal, and private information such as their:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Passport number;

- Health information; and
- Financial account information for direct deposit of payment.

31. On information and belief, in the course of collecting Private Information from current and former employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for employee data through their applicable privacy policy and through other disclosures.

32. Plaintiff and the members of the Class, as current and former employees, relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

33. Due to its sensitive nature and the consequences to individuals resulting from its misappropriation, Plaintiff and the members of the Class demand security to safeguard their Private Information.

34. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and the members of the Class from involuntary disclosure to third parties.

II. The Cyber-Attack and Data Breach.

35. On or about July 6, 2022, Defendant began notifying current and former employees and state Attorneys General about a data breach that was discovered between April 27, 2022 and May 1, 2022.

36. According to the letter delivered to Plaintiff and the letters sent to state Attorneys General, Defendant "identified unusual network activity" sometime after May 1, 2022, and that "evidence showed that there was unauthorized activity in the company network[.] . . . During that time, an unauthorized party obtained files stored on our file server."

37. Defendant subsequently determined, on June 2, 2022, that Plaintiff's name, and a combination of his date of birth, Social Security number, driver's license number, state identification number, passport number, financial account number, health insurance number, and health information was compromised as a result of the Data Breach.

38. On July 6, 2022, Plaintiff was informed that his full name, and a combination of his date of birth, Social Security number, driver's license number, state identification number, passport number, financial account number, health insurance number, and health information was among the data obtained in the Data Breach.

39. Due to the severity of the Data Breach, Defendant offered recipients "one-year membership to Experian's® IdentityWorks^{SM} credit monitoring service."

40. Based on the letter he received, which informed Plaintiff that his Private Information was accessed and obtained on Defendant's network and computer systems, Plaintiff understands that his full name, and a combination of his date of birth, Social Security number, driver's license number, state identification number, passport number, financial account number, health insurance number, and health information was stolen from Defendant's network and potentially sold or published.

41. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and the members of the Class, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

42. Indeed, Defendant's own Privacy Policy warrants that it "respects your concerns about privacy" and states that it "maintain[s] administrative, technical and physical safeguards

designed to assist us in protecting the personal information we collect against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use."[1]

43. Plaintiff and the members of the Class provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

44. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and data breaches preceding the date of the breach.

45. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[2]

46. These data breach incidences continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[3]

47. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.[4] Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

---

1 https://www.sixt.com/privacy/ (last visited August 5, 2022).

2 Identity Theft Resource Center, *Identity Theft Resource Center®'s Annual End-of-Year Data Breach Report Reveals 17 Percent Increase in Breaches over 2018*, https://www.idtheftcenter.org/post/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/ (last visited August 5, 2022).

3 Bree Fowler, *Data breaches break record in 2021*, CNET, Jan. 24, 2022, https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited August 5, 2022).

4 *See, e.g.*, https://www.fbi.gov/investigate/cyber (last visited August 5, 2022).

III. Defendant failed to comply with FTC guidelines.

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

49. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[5]

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

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

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

---

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited August 5, 2022).

53. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

54. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

56. Defendant was at all times fully aware of its obligation to protect the Private Information of employees, former and prospective employees, customers and prospective customers, as well as the significant repercussions that would result from its failure to do so.

IV. Defendant failed to comply with industry standards.

57. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing and implementing Defendant's cybersecurity practices.

58. Best cybersecurity practices that are standard in industries that custody private and protected information include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

59. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the data breach.

V. Defendant breached its obligations to its current and former employees.

61. Defendant breached its obligations to Plaintiff and the members of the Class or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data.

62. Upon information and good faith belief, Defendant's unlawful conduct includes, but is not limited to, the following acts or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current and former employees' Private Information;

c. Failing to adequately protect Private Information of current and former employees' family members;

d. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to apply all available security updates;

f. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

j. Failing to properly train and supervise employees in the proper handling of inbound emails.

63. Because Defendant needed to upgrade its computer systems' security and its procedures for handling cybersecurity threats, and it did not do so, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class members' Private Information.

VI. Data breaches cause disruption and put victims at an increased risk of fraud and identity theft.

64. Defendant understood the Private Information it collected is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the cyber-criminals who perpetrated this Cyber-Attack.

65. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[6]

[6] *See* U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited August 5, 2022) ("GAO Report").

66. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[7]

67. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

68. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

69. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

70. A 2021 study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[8]

---

[7] *See* https://www.identitytheft.gov/Steps (last visited August 5, 2022).

[8] *See* Identity Theft Resource Center, *2021 ITRC Consumer Aftermath Responses: Non-Pandemic Related*, https://www.idtheftcenter.org/wp-content/uploads/2021/05/2021-ITRC-Consumer-Aftermath-Responses-Non-Pandemic-Related.pdf (last visited August 5, 2022).

Upon or after discovering the incident, did you experience any of the other following problems?		
	I was generally inconvenienced.	87.5%
	I lost time at work.	37.5%
	I missed time from school.	11.1%
	I lost my home/place of residence.	11.1%
	My utilities were cut off or I was denied new service.	12.5%
	I lost out on an employment opportunity.	16.7%
	I lost a job.	8.3%
	A lawsuit was filed against me.	8.3%
	Other.	25.0%

71. What's more, theft of Private Information is also gravely serious. Private Information is a valuable property right.[9]

72. The value of Private Information is axiomatic, considering the value of "Big Data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

[9] *See, e.g.*, John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

73. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report at 29.

74. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

75. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground internet websites.

76. Where the most private information belonging to Plaintiff and the members of the Class was accessed and removed from Defendant's network, there is a strong probability that the stolen information is yet to be dumped on the cyber black market, meaning Plaintiff and the members of the Class are at an increased and continued risk of fraud and identity theft for many years into the future.

77. Thus, Plaintiff and the members of the Class must vigilantly monitor their financial accounts for many years to come.

78. Sensitive information can sell for as much as $363 per file according to the Infosec Institute.[10]

79. Personally identifying information, or PII, is particularly valuable because criminals can use it to target victims with frauds and scams.

80. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

81. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web, with sensitive personal information varying in prices ranging from $8 to over $1,000.[11]

82. Social Security numbers are among the worst kind of personal information to have stolen because criminals may use Social Security numbers in a variety of fraudulent ways and Social Security numbers are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

83. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Thieves can also use stolen Social Security numbers to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An

---

[10] Infosec Institute, *Hackers Selling Healthcare Data in the Black Market*, July 27, 2015 https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited August 5, 2022).

[11] Jonathan Greig, *How much is your info worth on the Dark Web? For Americans, it's just $8*, TechRepublic, Feb. 8, 2021, https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/ (last visited August 5, 2022).

individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

84. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

85. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[13]

86. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached and strengthened their data systems accordingly.

87. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

---

[12] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 5, 2022).

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited August 5, 2022).

VII. Plaintiff's and Class members' damages.

88. To date, Defendant has not provided Plaintiff and the members of the Class with equitable relief for the damages they have suffered as a result of the Cyber-Attack and Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Cyber-Attack.

89. Specifically, Defendant has only offered 12 months of inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen) or to all persons whose data was compromised in the Cyber-Attack.

90. Moreover, the 12 months of credit monitoring offered to persons whose private information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

91. Defendant did not provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class members' Private Information.

92. Plaintiff and the members of the Class have been damaged by the compromise of their Private Information in the Cyber-Attack.

93. Moreover, Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

VIII. Plaintiff's Experience.

94. Plaintiff provided his Private Information to Defendant during the course of his employment with Defendant.

95. During the course of his employment with Defendant, Plaintiff also provided his Private Information to receive payment, as well as for the provision of his healthcare benefits. On or about July 6, 2022, Plaintiff received a letter from Defendant informing him that his full name,

and a combination of his date of birth, Social Security number, driver's license number, state identification number, passport number, financial account number, health insurance number, and health information was stolen by cyber-criminals in the Data Breach.

96. As a result of the Data Breach, Defendant directed Plaintiff to take certain steps to protect his Private Information and otherwise mitigate his damages.

97. As a result of the Data Breach and the information that he received in the notice letter, Plaintiff spent approximately 2-3 hours dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the notice letter, communicating with his bank, ensuring accounts are secure, investigating the need to open new accounts that were not compromised by the Data Breach, and exploring alternative credit monitoring options. Plaintiff anticipates spending additional hours in the future monitoring his accounts and addressing the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

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

99. Plaintiff stores any and all documents containing his Private Information in a secure location, and avoids the disclosure of any of his Private Information whenever possible. Moreover, he diligently chooses unique usernames and passwords for his various online accounts to maximize his digital security efforts.

100. Plaintiff suffered actual injury and damages due to Defendant's mismanagement of his Private Information before and throughout the Data Breach.

101. Plaintiff suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of providing him payroll and benefit services, which was compromised in and as a result of the Data Breach.

102. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered mental anguish, anxiety, and increased concerns for the theft of his privacy since he received the notice letter detailing the Cyber-Attack and Data Breach.

103. Plaintiff is especially concerned about the theft of his full name paired with his Social Security number, address, date of birth, and banking information.

104. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information, especially his Social Security number and banking information, being placed in the hands of unauthorized third parties and possibly criminals.

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

CLASS ACTION ALLEGATIONS

106. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

107. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

108. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

> All persons whose Private Information was compromised as a result of the Cyber-Attack on Sixt Rent a Car, LLC.

109. Excluded from the Class are Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns as well as any entities in which Defendant has a controlling interest. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

110. Plaintiff reserves the right to amend the definitions of the Class or add a class or subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

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

112. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of members of the Class is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of Defendant's current and former employees whose data was compromised in the Cyber-Attack and Data Breach.

113. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual members of the Class. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Private Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;

c) Whether Defendant's data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the Cyber-Attack were consistent with industry standards;

e) Whether Defendant owed a duty to members of the Class to safeguard their Private Information;

f) Whether Defendant breached its duty to members of the Class to safeguard their Private Information;

g) Whether computer hackers obtained Class members' Private Information in the Cyber-Attack;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and the members of the Class suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant's conduct was negligent;

k) Whether Defendant breach an implied contract between it and Plaintiff;

l) Whether Plaintiff and the members of the Class are entitled to damages, civil penalties, or injunctive relief.

114. Typicality. Plaintiff's claims are typical of those of other members of the Class because Plaintiff's information, like that of every other Class Member, was compromised in the Cyber-Attack.

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and has no interests antagonistic to those of other members of the Class .

116. Plaintiff's Counsel are competent and experienced in litigating data breach class actions.

117. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and the members of the Class, in that all the Plaintiff's and Class members' data was stored on the same computer systems and unlawfully accessed in the same way.

118. The common issues arising from Defendant's conduct affecting members of the Class set out above predominate over any individualized issues.

119. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

120. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy.

121. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation.

122. Absent a class action, most members of the Class would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy.

123. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class , which would establish incompatible standards of conduct for Defendant.

124. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE

126. Plaintiff re-alleges and incorporates by reference paragraphs 1-125 in this complaint as if fully alleged herein.

127. Defendant required Plaintiff and the members of the Class to submit and entrust to it non-public personal information during the course of their employment, to receive training, and to receive compensation or other employment-related benefits. Plaintiff and the Class did so submit and entrust to Defendant the Private Information with the understanding that it would be safeguarded from unauthorized access.

128. By collecting and storing this data in its computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff's and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

129. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

131. Defendant's duty of care to use reasonable security measures arose because Defendant alone was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to members of the Class from a data breach.

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

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff's and Class members' Private Information;

e. Failing to detect in a timely manner that Plaintiff's and Class members' Private Information had been compromised;

f. Failing to timely notify Plaintiff and members of the Class about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

134. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class members' Private Information would result in injury to Plaintiff and the members of the Class. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

135. It was therefore foreseeable that Defendant's failure to adequately safeguard Plaintiff's and Class members' Private Information would result in one or more types of injuries to members of the Class.

136. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

137. Plaintiff and the members of the Class are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

138. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's

actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face, entitling them to damages in an amount to be proven at trial.

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

COUNT II
NEGLIGENCE *PER SE*

140. Plaintiff re-alleges and incorporates by reference paragraphs 1-125 in this complaint as if fully alleged herein.

141. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

142. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect.

143. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

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

145. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

146. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

147. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

148. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

149. The injury and harm suffered by Plaintiff and the members of the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

150. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the members of the Class have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT

151. Plaintiff re-alleges and incorporates by reference paragraphs 1-125 in this complaint as if fully alleged herein.

152. Defendant required Plaintiff and the members of the Class to provide their personal information, including name, address, date of birth, and Social Security or other identifying number, during the course of their employment.

153. During the course of their employment with Defendant, and to receive payment of their compensation, Plaintiff and the members of the Class provided their Private Information.

154. In providing their Private Information, Plaintiff and the members of the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the members of the Class if their data had been breached and compromised or stolen.

155. Plaintiff and the members of the Class accepted Defendant's offer of employment by providing their Private Information to Defendant.

156. Plaintiff and the members of the Class fully performed their obligations under the implied contracts with Defendant.

157. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

158. Defendant breached the implied contracts it made with Plaintiff and the members of the Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the data breach.

159. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the members of the Class have suffered (and will continue to suffer)

ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm, entitling them to damages in an amount to be proven at trial.

160. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law, including attorneys' fees and costs.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

161. Plaintiff re-alleges and incorporates by reference paragraphs 1-125 in this complaint as if fully alleged herein.

162. During the course of their employment with Defendant, and to receive payment of their compensation, Plaintiff and the members of the Class provided their Private Information.

163. In providing their Private Information, Plaintiff and the members of the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the members of the Class if their data had been breached and compromised or stolen.

164. Defendant also required Plaintiff and the members of the Class to provide Defendant with their Private Information to receive employment, services, and training.

165. Plaintiff and the members of the members of the Class accepted Defendant's offer of employment by providing their Private Information to Defendant.

166. Plaintiff and the members of the Class fully performed their obligations under the implied contracts with Defendant.

167. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entered into the implied contracts.

168. Defendant represented to its employees, implicitly and otherwise, that their Private Information would be secure.

169. Plaintiff and the members of the proposed Class relied on such representations when they agreed to provide their Private Information to Defendant.

170. Plaintiff and the members of the Class would not have entrusted their Private Information to Defendant without such agreement with Defendant.

171. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

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

173. Defendant failed to advise Plaintiff and the members of the Class of the Data Breach promptly and sufficiently.

174. For example, Fla. Stat. § 501.171(4)(a) states: "A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, *but no later than 30 days after the determination of a breach or reason to believe a breach occurred* unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c)" (emphasis added).

175. Defendant did not provide Plaintiff with notice of the Data Breach within 30 days of its discovery of the scope of the breach.

176. Defendant's duty to safeguard Plaintiff's and the members of the Class's Private Information is inherent in and consistent with the contracts entered into by Defendant and Plaintiff and the members of the Class.

177. Defendant would not have suffered harm by enacting industry standard measures to safeguard Plaintiff's and the members of the Class's Private Information.

178. Defendant's failure to enact reasonable safeguards to protect the Private Information it collected resulted in harm to Plaintiff and the members of the Class and violated the covenant of good faith and fair dealing.

179. Similarly, Defendant's failure to timely discover the breach, to timely notify affected persons, and to fully detail the scope of the breach in its notice letter each suffices to demonstrate a breach of the covenant.

180. Plaintiff and the members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

181. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract of good faith and fair dealing, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law, including attorneys' fees and costs.

COUNT V
INVASION OF PRIVACY

182. Plaintiff re-alleges and incorporates by reference paragraphs 1-125 in this complaint as if fully alleged herein.

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

184. Defendant owed a duty to its current and former employees, including Plaintiff and the members of the Class, to keep this information confidential.

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

186. The intrusion at issue was into a place or thing which was private and entitled to be private.

187. Plaintiff and the members of the Class disclosed their sensitive and confidential information to Defendant as part of their training, employment, and to receive their compensation, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure.

188. Plaintiff and the members of the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

189. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

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

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

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

193. For example, Fla. Stat. § 501.171(4)(a) states: "A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time

necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, *but no later than 30 days after the determination of a breach or reason to believe a breach occurred* unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c)" (emphasis added).

194. Defendant did not provide Plaintiff with notice of the Data Breach within 30 days of its discovery of the scope of the breach.

195. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the members of the Class.

196. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the members of the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the members of the Class to suffer damages.

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

198. Plaintiff and the members of the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records.

199. A judgment for monetary damages alone will not end Defendant's inability to safeguard the Private Information of Plaintiff and the members of the Class.

200. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes

the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law, including attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

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

c) For equitable relief compelling Defendant to use appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Cyber-Attack;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiff and the members of the Class;

f) For an award of actual damages, compensatory damages, nominal damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: August 12, 2022.

Respectfully submitted,

/s/ Jonathan B. Cohen
Jonathan B. Cohen
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
(212) 594-5300 (phone)
jcohen@milberg.com

Gary M. Klinger (pro hac vice forthcoming)*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
Email: gklinger@milberg.com

Alex D. Kruzyk
Bryan A. Giribaldo (pro hac vice forthcoming)*
PARDELL, KRUZYK & GIRIBALDO, PLLC
501 Congress Avenue, Suite 150
Austin, Texas 78701
Tele: (561) 726-8444
akruzyk@pkglegal.com
bgiribaldo@pkglegal.com

Logan A. Pardell
PARDELL, KRUZYK & GIRIBALDO, PLLC
433 Plaza Real Suite 275
Boca Raton, FL 33432
Tele: (561) 726-8444
lpardell@pkglegal.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
