UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

Amelia Yankovich and Joseph Allen, *on behalf of themselves and all others similarly situated*,	:	
Plaintiffs,	:	Civil Action No.
vs.	:	
	:	**CLASS ACTION COMPLAINT**
Applus Technologies, Inc.,	:	
Defendant.	:	

Plaintiffs, Amelia Yankovich and Joseph Allen, by undersigned counsel, bring the following Class Action Complaint against Applus Technologies, Inc., and allege, on their own behalf and on behalf of all those similarly situated, as follows:

INTRODUCTION

1. Plaintiffs and other Class Members are Connecticut residents who have registered their vehicles with the Connecticut Department of Motor Vehicles ("CT DMV") and who entrusted personally identifiable information ("PII") – their names, addresses, dates of birth, Personal Identification Number, Social Security Number, driver's license numbers, and license plate numbers – to Defendant Applus Technologies, Inc. ("Applus" or "Defendant"), a company that manages and provides vehicle inspections and emission testing and services to Connecticut drivers for the CT DMV.

2. Applus betrayed Plaintiffs' trust by failing to properly safeguard and protect their PII.

3. On or about March 30, 2021, Applus learned that it had been the victim of a malware attack (the "Data Breach") perpetuated by cybercriminals, which prompted Applus to shut down its vehicle emissions testing programs in eight states, including Connecticut.

Applus recommended that the public "monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual."[1]

4. Applus has not yet disclosed the specific type of malware used during the attack, but news reports note that "Applus was likely targeted by a ransomware attack" and "the ransomware operation likely stole data during the attack, which based on the type of company, could include information about vehicles and their owners."[2] One IT security expert explained that "in this case, you're talking about personally identifiable information. You've got financial data that belongs to the inspection stations. You've also got personal information for every single person that gets a sticker. So these databases have your vehicle identification number, they've got your license plate number, they've got your name and address, all information that would be valuable to someone."[3]

5. The confidential PII that was likely compromised and stolen in the Data Breach can be used to gain unlawful access to the users' online accounts, can be used to carry out identity theft or commit other fraud, can be disseminated on the internet and be available to those who broker and traffic in stolen PII.

6. The Data Breach was a direct result of Applus' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII, and could have been avoided through basic security measures, authentications, and training.

7. Because Applus failed to take reasonable steps to adequately protect the PII that Plaintiff and members of the Class entrusted with Applus, Plaintiffs' and Class

[1] https://www.ctpost.com/news/article/Monitor-your-financial-accounts-CT-DMV-16080894.php
[2] https://www.bleepingcomputer.com/news/security/malware-attack-is-preventing-car-inspections-in-eight-us-states/.
[3] https://www.wgbh.org/news/local-news/2021/04/14/tech-security-expert-ma-inspection-shutdown-cause-probably-some-form-of-ransomware

members' PII is now readily available on the internet for anyone to acquire, access, and use for unauthorized purposes for the foreseeable future. Indeed, Applus' failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiffs and Class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy.

8. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff and Defendant Applus are citizens of different states.

10. The Court has personal jurisdiction over Applus as it conducts substantial business in this State and in this District and because the conduct complained of herein occurred in this State.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) as a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, were directed to, and/or emanated from this District, and because Plaintiffs reside in this District.

PARTIES

12. Plaintiff Amelia Yankovich is, and at all times mentioned herein was, an adult individual residing in Cheshire, Connecticut. At all relevant times, Ms. Yankovich has had a Connecticut driver's license, registered her vehicle with the Connecticut Department of Motor Vehicles, had her vehicle inspected, and in so doing provided PII to Applus.

13. Plaintiff Joseph Allen is, and at all times mentioned herein was, an adult individual residing in Danbury, Connecticut. At all relevant times, Mr. Allen has had a Connecticut driver's license, registered his vehicle with the Connecticut Department of Motor Vehicles, had her vehicle inspected, and in so doing provided PII to Applus.

14. Defendant Applus Technologies, Inc. ("Applus") is a Delaware corporation with a principal place of business at 3225 Gateway Road, Suite 450, Brookfield, Wisconsin 53045.

FACTUAL ALLEGATIONS

15. At all pertinent times, Plaintiffs were Connecticut residents who had active driver's licenses issued by the CT DMV and owned personal motor vehicles registered with the CT DMV.

16. As part of the vehicle registration and inspection processes, the CT DMV required that Plaintiffs undergo vehicle inspection and emissions testing at facilities managed, maintained, and serviced by Applus.

17. In connection with their vehicle registrations and inspections with the CT DMV, Plaintiffs were each required to provide certain personal and financial information to Applus, including their name, address, date of birth, Personal Identification Number, Social Security Number, driver's license number, and license plate number.

18. On March 30, 2021, Applus contends that it learned that it had been the victim of a malware attack by cybercriminals (the Data Breach), which prompted Applus to shut down its vehicle inspection and emissions testing programs in Connecticut as well as several other states.

19. Applus announced that it had retained computer forensic experts to analyze the Data Breach and "determine the scope of the attack and whether or not any personal information has been compromised."[4]

20. Applus recommended that the public "monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual."[5]

21. Applus did not disclose the type of malware used during the attack, but news reports note that "Applus was likely targeted by a ransomware attack" and in such a scenario "the ransomware operation likely stole data during the attack, which based on the type of company, could include information about vehicles and their owners."[6]

22. Indeed, one IT security expert explained that "in this case, you're talking about personally identifiable information. You've got financial data that belongs to the inspection stations. You've also got personal information for every single person that gets a sticker. So these databases have your vehicle identification number, they've got your license plate number, they've got your name and address, all information that would be valuable to someone."[7]

---

[4] https://www.ctpost.com/news/article/Monitor-your-financial-accounts-CT-DMV-16080894.php
[5] *Id.*
[6] https://www.bleepingcomputer.com/news/security/malware-attack-is-preventing-car-inspections-in-eight-us-states/.
[7] https://www.wgbh.org/news/local-news/2021/04/14/tech-security-expert-ma-inspection-shutdown-cause-probably-some-form-of-ransomware

23. In an April 19, 2021 statement, Applus noted again that it had "engaged computer forensic experts to assist in analyzing the current attack to determine whether or not any personal information for motorists in Connecticut could potentially have been compromised."[8]

24. On April 27, 2021, vehicle inspection and emission testing programs in Connecticut resumed, but Applus reported that it was still investigating the scope of the malware attack.[9]

25. However, to date Applus has not disclosed the results of its investigation, nor has it disclosed the extent to which Connecticut vehicle owners' PII was impacted during the Data Breach.

26. During data breaches like the one at issue here, cybercriminals commonly engage in so-called "double extortion" where they both encrypt and lock up the victim's data and separately steal the data and threaten to make it public if the victim does not pay a ransom.[10]

27. Upon information and belief, and in light of the information Applus has publicly disclosed about the Data Breach to date, it is reasonably certain that the cybercriminals responsible for the malware attack on Applus deliberately stole PII during the Data Breach.

28. The PII impacted by the Data Breach is of great value to hackers and cyber criminals. The PII that was likely compromised in the Data Breach can be sold on the 'dark

[8] https://www.prnewswire.com/news-releases/ct-vehicle-emissions-to-be-restored-no-later-than-april-30-301271812.html
[9] https://portal.ct.gov/DMV/News-and-Publications/News-and-Publications/Emissions-Testing-Resumes-Today
[10] *See* https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html

web' to other criminals, and can be used in a variety of unlawful manners, for instance applying for credit cards, obtaining employment, obtaining a loan, filing false tax returns, obtaining medical care, stealing Social Security or other government benefits, or applying for a driver's license, birth certificate, or other public document.

29. Applus failed to maintain the confidentiality of the PII entrusted to it, failed to prevent cybercriminals from accessing and using the PII, failed to avoid accidental loss, disclosure, or unauthorized access to PII, failed to prevent unauthorized disclosure of PII, and failed to maintain security measures consistent with industry standards for the protection of PII.

30. The Data Breach was foreseeable in light of the publicized wave of data breaches in recent years. According to one recent report, in 2020 alone nearly 2,400 U.S.-based governments, healthcare facilities, and schools were the victims of ransomware, and one cyber insurance firm observed a 260% increase in ransomware attacks in the first half of year 2020.[11]

31. Thus, Applus knew that given the size and scope of the PII it collects, manages, and maintains, and given the prevalence of cyberattacks on similar entities, that Applus was the target of security threats, and understood or should have understood the risks posed by unsecure data security practices and systems.

32. Applus had a duty to Plaintiffs and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, and act reasonably to prevent foreseeable harm to Plaintiff and Class members. This duty arose as a

[11] https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

result of the special relationship that existed between Applus and Plaintiffs and the Class Members, because Plaintiff and members of the Class entrusted Applus with their PII as part of the vehicle registration and inspection processes and requirements in Connecticut. Moreover, Applus had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite Applus' obligation to protect PII.

33. Applus was at all times aware of its obligations to protect the PII of Connecticut vehicle owners and of the significant consequences that would result from its failure to do so.

34. However, Applus breached its duty owed to Plaintiffs and Class members and failed to maintain reasonable data security procedures and practices, resulting in the Data Breach.

35. Upon information and belief, as a result of the Data Breach, Plaintiff and Class Members' PII are now in the hands of unknown cybercriminal hackers who either have or will use the PII at a later date or resell it, and Plaintiffs and Class Members now and for the rest of their lives face an imminent, heightened, and substantial risk of identity theft and other fraud.

36. Accordingly, as a direct and proximate result of Applus' actions and inactions, Plaintiff and Class Members have been injured and damaged, including but not limited to the increased risk of identity theft and identity fraud, improper disclosure of PII, and the ensuing time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft resulting from the Data Breach.

CLASS ACTION ALLEGATIONS

A. The Class

37. Plaintiffs bring this case as a class action on behalf of the following class pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and/or 23(b)(3).

> **The Class:** All persons residing in Connecticut whose PII was compromised in the data breach initially disclosed by Applus on or about March 30, 2021

38. Applus and its employees or agents are excluded from the Class.

B. Numerosity

39. Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Applus and obtainable by Plaintiffs only through the discovery process, Plaintiffs believe, and on that basis allege, that the Class is comprised of potentially hundreds of thousands of individuals, if not more, whose PII was compromised in the Data Breach.

C. Common Questions of Law and Fact

40. There are questions of law and fact common to the Class that predominate over any questions affecting only individual Class members. These questions include:

a. Whether Applus had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs and Class members' PII;

b. Whether Applus breached its legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs and Class Members' PII;

c. Whether Applus' conduct, practices, actions, and omissions, resulted in or

were the proximate cause of the Data Breach;

d. Whether and when Applus knew or should have known that its computer systems were vulnerable to attack;

e. Whether Applus failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiffs' and Class Members' PII;

f. Whether Applus breached implied contracts with Plaintiffs and the Class by failing to maintain adequate data security measures despite promising to do so;

g. Whether Applus' conduct was negligent;

h. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Applus' conduct, including increased risk of identity theft; and

i. Whether Plaintiffs and Class members are entitled to relief, including damages and equitable relief.

D. Typicality

41. The Plaintiffs' claims are typical of the claims of the Class since Plaintiffs, like all members of the Class, are complaining about the same events and conduct and were injured by Applus' uniform misconduct described above and assert similar claims for relief. Indeed, Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all absent Class members.

E. Protecting the Interests of the Class Members

42. Plaintiffs will fairly and adequately protect the interests of the Class and have retained counsel experienced in handling class actions and claims involving unlawful business practices. Neither Plaintiffs nor their counsel has any interest which might cause them not to vigorously pursue this action.

F. Proceeding Via Class Action is Superior and Advisable

43. A class action is the superior method for the fair and efficient adjudication of this controversy. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records.

44. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

FIRST CAUSE OF ACTION
Negligence

45. Plaintiffs incorporate by reference all of the above paragraphs of this Complaint as though fully stated herein.

46. Applus required Plaintiffs and Class members to submit non-public, sensitive PII in connection with their vehicle registrations, inspections, and emissions testing performed by Applus.

47. Applus had, and continue to have, a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII. Applus also had, and continue to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the storage and protection of PII within Defendant's possession, custody, and control and that of its vendors.

48. Applus' duty to use reasonable security measures arose as a result of the special relationship that existed between Applus and Connecticut vehicle owners. Only Applus was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the Class members from a data breach.

49. Applus violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, including Plaintiffs' and Class members' PII.

50. It was reasonably foreseeable to Applus that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII.

51. Applus, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class members by, among

other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII within their possession, custody, and control.

52. Applus, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII.

53. But for Applus' negligent breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been released, disclosed, and disseminated without their authorization.

54. Upon information and belief, Plaintiffs' and Class members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Applus' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' PII.

55. As a direct and proximate result of Applus' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiffs and Class members have been injured and damaged, including but not limited to the ongoing, imminent and impending threat and increased risk of being the victim of identity theft crimes and identity fraud, improper disclosure of PII, and the ensuing time and expense necessary to mitigate, remediate, and sort out the increased risk and threat of identity theft resulting from the Data Breach.

56. Applus' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

SECOND CAUSE OF ACTION
Breach of Implied Contract

57. Plaintiffs incorporate by reference all of the above paragraphs of this Complaint as though fully stated herein.

58. Applus required Plaintiffs and Class members to provide PII as a condition of registering their vehicles with the CT DMV and undergoing vehicle emissions testing managed, serviced, and performed by Applus. In so doing, Plaintiffs and Class members entered into implied contracts with Applus by which Applus agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised, or stolen.

59. Plaintiffs and Class members fully performed their obligations under the implied contracts with Applus.

60. Applus breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect their PII.

61. As a direct and proximate result of Applus' breach of implied contract, Plaintiffs and Class members have been injured and damaged, including but not limited to the ongoing, imminent and impending threat and increased risk of being the victim of identity theft crimes and identity fraud, improper disclosure of PII, and the ensuing time and expense necessary to mitigate, remediate, and sort out the increased risk and threat of identity theft resulting from the Data Breach.

62. The above constitutes breach of implied contract by Applus.

DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendant as follows:

a. An order certifying the proposed Class, designating Plaintiffs as named representatives of the Class, and designating the undersigned as Class Counsel;

b. Awarding Plaintiffs and the Class members actual, compensatory, and consequential damages;

c. Awarding Plaintiffs and the Class members statutory damages and penalties, as allowed by law;

d. Awarding Plaintiffs and the Class members restitution and disgorgement;

e. Requiring Applus to provide appropriate credit monitoring services to Plaintiffs and the other class members;

f. Awarding Plaintiffs and the Class members punitive damages;

g. Entering injunctive and declaratory relief as appropriate under the applicable law;

h. Awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

i. Awarding reasonable attorneys' fees and costs as permitted by law; and

j. Entering such other and further relief as may be just and proper.

TRIAL BY JURY DEMANDED ON ALL COUNTS

Dated: May 26, 2021

Respectfully submitted,

By: */s/ Sergei Lemberg*
Sergei Lemberg, Esq.
43 Danbury Road
Wilton, CT 06897
Telephone: (203) 653-2250
Facsimile: (203) 653-3424
slemberg@lemberglaw.com
Attorneys for Plaintiff

ClassAction.org