Richard Lyon (Cal. Bar No. 229288)
rick@dovel.com
Simon Franzini (Cal. Bar No. 287631)
simon@dovel.com
DOVEL & LUNER, LLP
201 Santa Monica Blvd., Suite 600
Santa Monica, California 90401
Telephone: (310) 656-7066
Facsimile: (310) 656-7069

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

DAWN DAVIS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PROG LEASING, LLC (d/b/a PROGRESSIVE LEASING),

Defendant.

Case No. 5:23-cv-02327

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Table of Contents

I. Introduction.

1. Defendant Prog Leasing, LLC (d/b/a Progressive Leasing) ("Defendant" or "Progressive Leasing") is a provider of lease-to-own and rental programs in partnership with various retailers. Progressive Leasing was entrusted with personal information ("PI")[1] of their customers and potential customers (collectively, "Customers").

2. On or around September 11, 2023, Defendant was the target of a massive data breach in which approximately 193,055 U.S. Customers[2] were subject to an unauthorized access and exfiltration, theft, or disclosure of their PI ("Data Breach"). Outside parties accessed a trove of personal details about Defendant's Customers—such as names, dates of birth, addresses, email addresses, Social Security numbers, credit card or account information, income information, and financial account numbers—stored on Defendant's servers. Despite the highly sensitive nature of the PI, the data was maintained by Defendant in a form that was neither encrypted nor redacted.

3. The Data Breach violated the fundamental privacy rights of Plaintiff and Class Members. Because of the Data Breach, Plaintiff and Class Members face an increased risk of identity theft.

4. With the PI accessed in the Data Breach, outside parties can commit a variety of crimes against Plaintiff and Class Members, including 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' names to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

5. Plaintiff and Class Members will demonstrate that they have suffered ascertainable losses in out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

---

[1] As used herein, the term "PI" is intended to include the definition of personal information provided under Civil Code sections 1798.140(v)(1) and 1798.81.5, subparagraph (A) of paragraph (1) of subdivision (d).

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/84f4c920-079d-4928-896e-977e2bd8ac35.shtml

6. Plaintiff brings this lawsuit on behalf of Class Members whose PI was compromised as a result of the Data Breach and Defendant's failure to (i) implement and maintain reasonable security procedures and practices appropriate to the nature of the PI; (ii) disclose their inadequate security procedures and practices; (iii) effectively monitor their systems for security vulnerabilities; and (iv) timely detect, report, and disclose the Data Breach.

II. Parties.

7. At all relevant times, Plaintiff Dawn Davis was and is a citizen of California, residing in Riverside County. Plaintiff Davis is a customer of Defendant. She entrusted her PI to Defendant. Plaintiff Davis' PI was accessed and compromised as a result of the Data Breach. This resulted in an invasion of her privacy interests and has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

8. Defendant Prog Leasing, LLC is a Delaware limited liability company with its principal place of business in Draper, Utah.

III. Jurisdiction and Venue.

9. The 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 class members is well over 100. And the class members (including Plaintiff Dawn Davis) have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

10. This Court has personal jurisdiction over Defendant because it does business in this jurisdiction. The claims of Plaintiff and the Class arise out of Defendant's business activity in California and, at all times herein mentioned, Defendant was conducting business in California.

11. Venue is proper in this Court because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from

this District. Venue is also proper because it was within this District where Plaintiff and other Class Members entrusted their PI to Defendant.

12. This is a class action brought pursuant to Federal Rule of Civil Procedure 23.

IV. Factual Allegations.

A. The Data Breach

13. Defendant Prog Leasing, LLC is a provider of lease-to-own and rental programs in partnership with various retailers. Defendant offers its services at thousands of retail locations and has reached millions of customers.[3]

14. On or about September 11, 2023, Defendant experienced a cybersecurity incident in which an unauthorized third party obtained PI from or about customers. The data was stolen when it was left unsecured and unredacted.

15. Approximately 193,055 individual customers in the United States (a substantial percentage of which reside in California) had their PI stolen as a result of the Data Breach.

16. The Data Breach was not reported until September 18, 2023 when Defendant filed a Form 8-K Report with the SEC.[4]

17. The compromised PI of Plaintiff and the Class Members includes, without limitation, the following categories of highly sensitive information: (1) name; (2) date of birth; (3) address; (4) email address; (5) Social Security number; (6) credit card or account information; (7) income information; (8) financial account numbers.

18. The Data Breach subjected Plaintiff and the other Class Members to an unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted PI, including, but not limited to, PI that falls within the definition of subparagraph (A) of paragraph (1) of subdivision (d) of Civil Code section 1798.81.5.

---

[3] https://progleasing.com/about-us/

[4] https://investor.progholdings.com/static-files/f2cde36b-d0c3-4449-bce4-9c84fa3682de

19. The Data Breach resulted from Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PI.

B. Defendant failed to meet minimum cybersecurity standards.

20. In its privacy policy, Progressive Leasing touts that it is "commited to safeguarding, preserving, and respecting [] privacy rights" and "take[s] various reasonable organizational, administrative, and technical measures to protect [] personal information from unauthorized access, disclosure, alteration, or destruction."[5]

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PI, Progressive Leasing assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PI from disclosure.

22. Progressive Leasing was obligated by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PI confidential and to protect it from unauthorized access and disclosure.

23. Plaintiff and Class Members relied on Progressive Leasing to keep their PI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

24. On information and belief, Defendant breached the standard of care by failing to implement reasonable security procedures to adequately protect Class Members' PI—which was not password protected, redacted, or encrypted—from data breaches. Data breaches, such as this one, are commonly made possible through a vulnerability in a system or server.

25. Defendant could have prevented the Data Breach, which began no later than September 9, 2023, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PI.

---

[5] https://progleasing.com/privacy/

26. Several industry best practices have been identified that, at a minimum, should be implemented by businesses like Defendant, including but not limited to: educating employees; implementing strong passwords, multi-layer security (including firewalls, anti-virus, and antimalware software), encryption, and multi-factor authentication; making data unreadable without a key; backing up data; and limiting which employees can access sensitive data.

27. Upon information and belief, Defendant failed to follow some or all of these industry best practices.

28. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

29. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks, thus enabling unauthorized third-parties to access Plaintiff's and Class Members' PI and causing the Data Breach: 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 all established standards in reasonable cybersecurity readiness.

30. Defendant's negligence in safeguarding Plaintiff's and Class Members' PI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

31. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such

attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

32. As a result of Defendant's lax security, outside parties have accessed Plaintiff's and Class Members' PI in a readily usable form that is potentially of great value to them. Plaintiff and Class Members are thus exposed to criminals seeking to use the PI for nefarious and illegal activities, such as identity theft schemes. Given the sensitive nature of the PI, Plaintiff and Class Members face an imminent risk of identity theft.

33. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PI and of the foreseeable consequences that would occur if their data security system was breached.

C. Plaintiff was injured as a result of the Data Breach.

34. Plaintiff Davis is a citizen of Corona, California. Plaintiff has been a customer of Defendant for approximately 4 years and currently holds an active lease. During the relevant time period covered by this Complaint, she entrusted Defendant with her PI as a part of her business transactions.

35. Plaintiff Davis received a Notice of Data Breach letter from Defendant, dated October 23, 2023, informing her that her PI had been accessed and stolen during the Data Breach. The notice letter informed her that the stolen PI included her name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address.

36. Defendant has offered to provide Plaintiff and Class Members with complementary 12-month memberships to a credit monitoring services through Experian Identity Works as a result of the Data Breach. This offer is inadequate to compensate Plaintiff and Class Members for the harm the Data Breach has caused them.

37. Plaintiff and Class Members face substantial risk of out-of-pocket losses due to fraudulent activity resulting from the Data Breach, including loans opened in their

names, tax return fraud, credit card fraud, accounts opened in their names, and similar identity theft.

38. Plaintiff and Class Members face substantial risk of being targeted now and in the future, to phishing schemes, data intrusion, and other illegal activity because potential fraudsters could use their PI to implement such schemes more effectively against Plaintiff and Class Members.

39. Plaintiff and Class Members are likely to incur out-of-pocket costs for implementing protective measures for years, including credit monitoring fees, credit report fees, credit freeze fees, and other similar costs related to the Data Breach. They will also spend significant amounts of time (which has value) monitoring their financial accounts, credit scores, and personal accounts for indications of fraudulent activity.

40. Plaintiff and Class Members also suffered a loss of value of their PI when it was acquired by cyber thieves in the Data Breach. One's PI is among the most basic information that has value to an individual, and this value is dramatically decreased when it is in the hands of malicious actors, like the cyber thieves who stole their PI. Plaintiff and Class Members are also now forced to live with the anxiety that their PI may be publicly disclosed, which would subject them to embarrassment and deprive them of the basic right to privacy.

41. Plaintiff and Class Members have an interest in ensuring that their PI, which remains in the possession of Defendant, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is treated in accordance with best practices as discussed below.

42. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm because of the Data Breach.

43. Plaintiff would not have provided her PI to Defendant and/or would have switched to another lease and rental provider if she had been aware of Defendant's

inadequate computer and data security practices to safeguard its customers' personal and financial information from theft.

V. Class Allegations.

44. Plaintiff brings her claim individually and on behalf of the following class: all California residents whose PI was accessed or otherwise compromised in the Data Breach experienced by Defendant on or about September 11, 2023.

45. The following people are excluded from the class and the subclasses: (1) any Judge or Magistrate Judge presiding over this action and the members of their family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel, and their experts and consultants; and (6) the legal representatives, successors, and assignees of any excluded persons.

Numerosity

46. The proposed class contains members so numerous that separate joinder of each member of the class is impractical. There are tens or hundreds of thousands of proposed class members.

Commonality

47. This action involves questions of law and fact common to Class Members that predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

- When Defendant actually learned of the Data Breach;
- Whether Defendant adequately detected, disclosed and responded to the Data Breach;

- Whether Defendant owed a duty to the Class to exercise due care in collecting, encrypting, password protecting, storing, safeguarding and/or maintaining their PI;
- Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the PI;
- Whether Defendant breached the duty of care;
- Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PI secure and prevent loss or misuse of that PI;
- Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur; and,
- Whether Defendant violated the law by failing to promptly notify Class Members that their PI had been compromised.

Typicality

48. Plaintiff's claims are typical of the proposed class. Like the proposed class, Plaintiff had her PI accessed and compromised as a result of the Data Breach, due to Defendant's wrongful conduct, acts, or omissions.

Adequacy

49. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. There are no conflicts of interest between Plaintiff, her counsel and the class. Plaintiff is represented by attorneys who are competent and experienced in consumer class action litigation.

Predominance and Superiority

50. The prosecution of separate actions by individual members of the proposed class would create a risk of inconsistent or varying adjudication with respect to individual members, which would establish incompatible standards for the parties opposing the class. For example, individual adjudication would create a risk that Defendant's conduct is found wrongful for some consumer, but not other similarly-situated consumers.

51. Common questions of law and fact predominate over any questions affecting only individual members of the proposed class. These common legal and factual questions arise from central issues which do not vary from class member to class member, and which may be determined without reference to the individual circumstances of any particular class member. For example, a core liability question is common: whether Defendant maintained adequate computer safety and security procedures while in possession of customers' PI.

52. A class action is superior to all other available methods for the fair and efficient adjudication of this litigation because individual litigation of each claim is impractical. It would be unduly burdensome to separately litigate thousands of individual claims.

VI. Claims.

Count 1: Violation of the California Consumer Privacy Act ("CCPA")

Cal. Civil Code Sec. 1798.150, et seq.

(on behalf of Plaintiff and the Class)

53. Plaintiff incorporates the allegations contained in the foregoing paragraphs as though repeated here.

54. Plaintiff brings this cause of action on behalf of herself and the Class.

55. California Civil Code section 1798.150, subdivision (a)(1), provides,

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> > (B) Injunctive or declaratory relief.
> > (C) Any other relief the court deems proper.

56. On information and belief, Defendant took possession, retained, stored, and maintained the nonencrypted and nonredacted PI of Plaintiff and the Class. Defendant collects or receives such information and determines the purposes and means of the processing of such PI.

57. As a result of the Data Breach, nonredacted and nonencrypted PI of Plaintiff and Class Members that was stored on that server was compromised, accessed, and subject to exfiltration, theft or disclosure.

58. The Data Breach subjected Plaintiff and the other Class Members to an unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted PI, including, but not limited to, PI that falls within the definition of subparagraph (A) of paragraph (1) of subdivision (d) of Civil Code section 1798.81.5.

59. The Data Breach was a result of Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

60. Due to the Data Breach, Plaintiff and the Class Members are entitled to recover actual damages. Pursuant to California Civil Code § 1798.150, Plaintiff, on behalf of herself and all other members of the Class, seeks actual damages.

61. On Novmeber 13, 2023, Plaintiff provided written notice to Defendant, identifying the specific provisions of the CCPA that Plaintiff alleges have been or are being violated. If Defendant fails to cure this breach pursuant to §1798.150(b), Plaintiff may seek to amend this Complaint to also seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per Class Member.

VII. Prayer for Relief.

62. Plaintiff seeks the following relief individually and for the proposed class and subclasses:

- An order certifying the Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

- An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff and Class Members' PI;
- An award of actual damages pursuant to the CCPA;
- An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;
- Such other and further relief as this Court may deem just and proper.

VIII. Demand for Jury Trial.

63. Plaintiff demands the right to a jury trial on all claims so triable.

Dated: November 13, 2023

Respectfully submitted,

By: */s/ Richard Lyon*

Richard Lyon (Cal. Bar No. 229288)
rick@dovel.com
Simon Franzini (Cal. Bar No. 287631)
simon@dovel.com
DOVEL & LUNER, LLP
201 Santa Monica Blvd., Suite 600
Santa Monica, California 90401
Telephone: (310) 656-7066
Facsimile: (310) 656-7069

Attorneys for Plaintiff